Universitatea
Transilvania
din Brașov

ȘCOALA DOCTORALĂ INTERDISCIPLINARĂ
Facultatea: INGINERIE ELECTRICĂ ȘI ȘTIINȚA CALCULATOARELOR

Florin OGÎGĂU-NEAMȚIU

CERCETĂRI PRIVIND SECURIZAREA INFORMAȚIEI ÎN SISTEMELE CLOUD COMPUTING

CONTRIBUTIONS ON INFORMATION SECURITY IN CLOUD COMPUTING SYSTEMS

REZUMAT / ABSTRACT

Conducător ştiințific
Prof.dr.ing. Sorin-Aurel MORARU

BRAȘOV, 2018

Universitatea Transilvania din Braşov

D-lui (D-nei)

.....

COMPONENȚA

Comisiei de doctorat

Numită prin ordinul Rectorului Universității Transilvania din Braşov

Nr. ..... din .....

Conf.dr.ing. Delia UNGUREANU	Preşedinte, Universitatea Transilvania din Brasov
Prof.dr.ing. Sorin-Aurel MORARU	Conducător ştiinţific, Universitatea Transilvania din Braşov
Prof.dr.ing. Theodor BORANGIU	Referent oficial, Universitatea Politehnica din Bucureşti
Prof.dr.ing. Cezar SCARLAT	Referent oficial, Universitatea Politehnica din Bucureşti
Conf.dr.ing. Liviu PERNIU	Referent oficial, Universitatea Transilvania din Braşov

Data, ora şi locul susținerii publice a tezei de doctorat: 14.09.2018, ora ....., sala .....

Eventualele aprecieri sau observații asupra conținutului lucrării vă rog să le transmiteți electronic, în timp util, pe adresa fogigau@crmra.ro.

Totodată, vă invităm să luați parte la şedința publică de susținere a tezei de doctorat.

Vă mulțumim.

CUPRINS

	Pg. teza	Pg. rezumat
Lista de abrevieri	5	7
Lista de figuri	7	-
Listă de tabele	8	-
1.Introducere	9	8
1.1 Importanța și actualitatea temei	9	8
1.2 Obiectivele tezei	11	9
1.3 Prezentarea capitolelor tezei	13	10
2 Stadiul actual al cercetării în domeniu	15	11
2.1 Specificul mediului cloud computing	15	11
2.2 Modele de implementare	19	13
2.3 Modele de livrare a serviciilor	22	15
2.4 Managementul riscului în sistemele cloud computing	26	17
2.5 Riscuri de securitate ale arhitecturii cloud computing	27	17
2.5.1 Accesul la servere și date	28	18
2.5.2 Securizarea virtualizării	31	18
2.5.3 Securitatea rețelei	33	19
2.5.4 Securitatea datelor	34	20
2.5.5 Segregarea datelor	42	23
2.5.6 Standardizarea	43	23
2.5.7 Transferul datelor	44	24
2.5.8 Managementul actualizărilor de securitate	45	24
2.5.9 Acordul de furnizare a serviciilor	46	25
2.5.10 Interoperabilitate	48	25
2.6 Concluzii	49	25
3 Strategia de protecție a datelor în platformele cloud computing	51	26
3.1 Importanța securizării informației	51	26
3.2 Securitate prin niveluri	52	26
3.3 Apărarea în adâncime	54	26
3.4 Provocări de securitate specifice mediului tehnologic actual	60	28
3.4.1 Tehnologia ca serviciu	60	29
3.4.2 Internetul obiectelor - *Internet of Things*	62	29
3.4.3 Cantități mari de date - *Big Data*	63	29
3.4.4 Modificarea profilului infractorului cibernetic	65	30
3.4.5 Modificarea strategiilor de atac	67	30
3.4.6 IT ca bun de larg consum - *IT Consumerization*	69	31
3.4.7 Rețele definite software - *Software Defined Networks*	71	31
3.5 Studiu de caz	72	32
3.6 Analiza viabilității strategiilor clasice	76	33
3.7 Propuneri	79	35
3.8 Concluzii	82	36
4 Token-izarea ca tehnică de securizare a informației	84	37
4.1 Studiu privind metodele actuale de obscurizare a informației	84	37
4.1.1 Criptarea datelor	84	37
4.1.2 Mascarea datelor	85	38
4.1.3 Token-izarea	87	38

4.2 Analiză comparativă a tehnicilor de obscurizare a datelor	88	39
4.2.1 Capabilități de securizare a datelor	89	39
4.2.2 Costuri în investiții hardware și software	91	40
4.2.3 Impactul asupra proceselor organizaționale	92	41
4.3 Potențialul de utilizare a token-izării	95	42
4.4 Concluzii	97	43
5. Automatizarea obscurizării datelor în sisteme de prelucrare a informațiilor bazate pe tehnologii cloud computing	99	44
5.1 Obscurizarea datelor în mediul clasic actual	99	44
5.1.1 Importanța clasificării datelor	100	44
5.1.2 Limitări ale sistemelor actuale	100	45
5.2 Prelucrarea automată a datelor	103	46
5.2.1 Analiza și identificarea informației	103	46
5.2.2 Măsuri de bază pentru regăsirea informației	103	46
5.2.3 Metode de identificare a informației	106	46
5.2.4 Procesarea limbajului natural – natural language processing (NLP)	110	47
5.3 Învățarea automată	113	48
5.3.1 Învățarea supervizată	114	48
5.3.2 Învățarea nesupervizată	114	49
5.3.3 Învățarea cu întărire	115	49
5.4 Prezentarea modelului propus	116	49
5.4.1 Modulul de clasificare a datelor	117	50
5.4.2 Modulul de obscurizare a datelor	120	51
5.4.3 Implementarea modelului	120	52
5.4.4 Dezvoltarea interfeței cu utilizatorul	122	53
5.4.5 Testarea funcționalității sistemului	122	54
5.5 Analiza de oportunitate a sistemului	124	55
5.5.1 Analiza de cost	125	55
5.5.2 Analiza de risc	130	58
5.6 Beneficiile modelului propus	132	59
5.7 Concluzii	134	60
6. Concluzii generale, realizări și contribuții originale, direcții viitoare de cercetare și diseminare	136	61
6.1 Concluzii generale	136	61
6.2 Contribuții originale	138	62
6.3 Direcții viitoare de cercetare	139	63
6.4 Diseminarea rezultatelor prin lucrări elaborate pe durata pregătirii doctoratului	140	64
Bibliografie selectivă	143	65
Scurt rezumat (română /engleză)	151	67
CV	153	68

TABLE OF CONTENTS

	Pg. teza	Pg. rezumat
List of abreviations	5	7
List of figures	7	-
List of tabels	8	-

1.Introduction	9	8
1.1 The importance and actuality of the subject	9	8
1.2 Objectives of the thesis	11	9
1.3 Presentation of the chapters	13	10
2 Current state of the research	15	11
2.1 The cloud computing environmental specificity	15	11
2.2 Implementation models	19	13
2.3 Service delivery models	22	15
2.4 Risk management in cloud computing	26	17
2.5 Security risks in cloud computing environments	27	17
2.5.1 Access to servers and data	28	18
2.5.2 Virtualization security	31	18
2.5.3 Network security	33	19
2.5.4 Data security	34	20
2.5.5 Data segregation	42	23
2.5.6 Standardization	43	23
2.5.7 Data transfer	44	24
2.5.8 Security updates management	45	24
2.5.9 Service level agreements	46	25
2.5.10 Interoperability	48	25
2.6 Conclusions	49	25
3 Data protection strategy in cloud computing platforms	51	26
3.1 The importance of securing information	51	26
3.2 Security through levels	52	26
3.3 Defense in depth	54	26
3.4 Security challenges specific to the current technological environment	60	28
3.4.1 Technology as a service	60	29
3.4.2 Internet of Things	62	29
3.4.3 Big Data	63	29
3.4.4 Modern cyber criminal profile	65	30
3.4.5 Modern cyber attack strategies	67	30
3.4.6 IT Consumerization	69	31
3.4.7 Software Defined Networks	71	31
3.5 Case Study	72	32
3.6 Classical strategies viability analysis	76	33
3.7 Recommended techniques	79	35
3.8 Conclusions	82	36
4 Tokenization as a technique for securing information	84	37
4.1 Study on current information obscuring techniques	84	37
4.1.1 Encrypting data	84	37
4.1.2 Data masking	85	38
4.1.3 Tokenization	87	38
4.2 Comparative analysis of data obscuration techniques	88	39
4.2.1 Data security capabilities	89	39
4.2.2 Costs of hardware and software investments	91	40
4.2.3 Impact upon organizational processes	92	41
4.3 Tokenization utilization potential	95	42
4.4 Conclusions	97	43

5. Automating data obfuscation in cloud computing based technological systems	99	44
5.1 Obfuscating data in the current classical environment	99	44
5.1.1 The importance of data classification	100	44
5.1.2 Limitations of the current systems	100	45
5.2 Automated data processing	103	46
5.2.1 Information analysis and identification	103	46
5.2.2 Information retrieval	103	46
5.2.3 Information identification	106	46
5.2.4 Natural language processing (NLP)	110	47
5.3 Automatic learning	113	48
5.3.1 Supervised learning	114	48
5.3.2 Unsupervised learning	114	49
5.3.3 Reinforcement learning	115	49
5.4 Presentation of the proposed model	116	49
5.4.1 Data classification module	117	50
5.4.2 Data obfuscation module	120	51
5.4.3 Model implementation	120	52
5.4.4 User interface development	122	53
5.4.5 Testing system functionality	122	54
5.5 System Opportunity Analysis	124	55
5.5.1 Cost analysis	125	55
5.5.2 Risk analysis	130	58
5.6 Advantages of the proposed model	132	59
5.7 Conclusions	134	60
6 General conclusions, achievements and original contributions, future directions for research and dissemination	136	61
6.1 General conclusions	136	61
6.2 Original contributions	138	62
6.3 Future directions for research	139	63
6.4 Dissemination of results	140	64
Bibliography	143	65
Abstract	151	67
CV	153	68

Listă de abrevieri

ACL – Access Control List
AD – Active Directory
API – Application Programming Interface
APT – Advanced Persistent Threat
ARPANET – Advanced Research Projects Agency Network
AWS – Amazon Web Services
BYOD - Bring Your Own Device
CAPEX – Capital Expenditures
CDMI – Cloud Data Management Interface
CIA – Confidentiality, Integrity, Availability
CNP – Cod Numeric Personal
COPPA –Children's Online Privacy Protection Act
CRM – Content Resource Management
DARPA – Defense Advanced Research Projects Agency
DHCP – Dynamic Host Configuration Protocol
DNS – Domain Name System
DMZ – Demilitarized Zone
FACTA – Fair and Accurate Credit Transactions Act
FISMA – Federal Information Security Management Act
FTPS –File Transfer Protocol with SSL Security
GDPR – General Data Protection Regulation
HDFS – Hadoop Distributed File System
HIPAA –Health Insurance Portability and Accountability Act
HSBC – The Hongkong and Shanghai Banking Corporation
HTTP – Hypertext Transfer Protocol
HTTPS –Hypertext Transfer Protocol Secure
IaaS – Infrastructure as a Service
INFOSEC – Information Security
IoT – Internet of Things
ISO – International Organization for Standardization
IP – Internet Protocol
IT – Information Technology
LDAP – Lightweight Directory Access Protocol
LSG – Loss of Strength Gradient
NAT – Network address translations
NLP – Natural Language Processing
OCCI – Open Cloud Computing Interface
OSI – Open Systems Interconnection
OVF – Open Virtualization Format
PaaS – Platform as a Service
PAN – Primary Account Number
PCI/DSS – Payment Card Industry Data Security Standard
PKI – Public Key Infrastructure
SaaS – Software as a Service
SDN – Software Defined Networks
SSH – Secure Shell
SSL – Secure Sockets Layer
TCO – Total Cost of Ownership

1. Introducere

1.1 Importanța și actualitatea temei

Domeniul cloud computing a cunoscut o dezvoltare fulminantă în ultimul deceniu incitând interesul unor importante comunități de specialiști din domeniul tehnologiei informației, dar și din partea a numeroase persoane care activează în alte domenii de activitate. Caracteristica definitorie a acestei tehnologii este aceea de a propune oferirea resurselor informaționale sub forma unor servicii de care beneficiarii se pot folosi la momentul, sub forma, în cantitatea și calitatea de care aceștia au nevoie, din orice locație geografică. Numeroasele avantaje ale modelului de prelucrare a datelor propus (Armbrust, 2009) a determinat ca o mare parte a comunității oamenilor de știință și de afaceri să depună eforturi pentru dezvoltarea și integrarea masivă a acestuia în organizații, în vederea optimizării cheltuielilor în domeniul tehnologiei informației.

În acest domeniu se unifică două mari tendințe prezente în mediul informațional al zilelor noastre: necesitatea optimizării utilizării resurselor - care în domeniul tehnologiei informației se transpune prin utilizarea unor tehnologii și arhitecturi organizaționale capabile să exploateze capabilitățile tehnologice concomitent cu minimizarea cheltuielilor / maximizarea competitivității organizației și dinamica înaltă a mediului de afaceri – în care accesul la informație, prelucrarea acesteia și livrarea rezultatelor necesită întrunirea unor parametri înalți de performanță (rapiditate, adaptabilitate, mobilitate, complexitate etc.) care nu ar putea fi atinși fără utilizarea instrumentelor din aria tehnologiei informației.

În comparație cu tehnologiile clasice, utilizarea cloud computing-ului oferă beneficiarilor avantaje precum instalare rapidă, investiții de capital limitate - capital expenditures (CAPEX), plata în funcție de utilizare, scalabilitate ridicată, provizionare rapidă, elasticitate avansată, acces la resurse din orice locației la orice oră, reziliență ridicată, soluții de back-up și repunere în funcțiune cu costuri minime, repunere rapidă a serviciilor în funcțiune etc. Astfel s-a constat (International Data Group, 2016) că organizațiile au identificat avantajele acestui mod de lucru și aproximativ 70% dintre ele au configurată și utilizează cel puțin o aplicație în cloud. Totuși, același studiu a relevat faptul că principala îngrijorare care limitează migrarea organizațiilor către tehnologia cloud computing este problematica securizării datelor în acest mediu.

Cloud computing-ul a introdus în spectrul utilizării resurselor specifice tehnologiei informației un nou model de manipulare al datelor. Acest model ridică numeroase provocări strategiei clasice principale de protecție a datelor – „apărarea în adâncime” – făcând ca instrumentele utilizate în momentul de față la nivel strategic, operațional și tactic pentru securizarea datelor în mediile clasice să nu mai poată fi utilizate sau să aibă eficiență redusă în noul mediu.

Dacă în mediile clasice securitatea datelor era asigurată prin utilizarea unor echipamente aflate în administrarea organizației și sub strictul control al unor echipe direct loiale organizației, în arhitectura cloud computing manipularea datelor se face utilizând echipamente ale altor organizații, la care au acces un număr mare de alți clienți iar managementul acestora este executat de către echipe care nu sunt cunoscute de organizație. Manipularea informațiilor în medii externe, de către entități cu factor redus de încredere și utilizând echipamente în afara controlului organizației modifică radical spectrul clasic al factorilor de risc al securității informațiilor.

Rata de utilizare a unei tehnologii depinde de avantajele și riscurile utilizării acesteia, iar ezitările organizațiilor cu privire la nivelul de acceptanță al unei tehnologii în general și al cloud computing-ului în particular depinde de încrederea pe care acestea o au în capabilitățile tehnologiei. Abilitatea tehnologiei informației de a se alinia la nevoile de business ale organizației și de a aduce avantaje prin integrarea sa în procesele interne este un factor principal care condiționează organizațiile moderne în procesul de atragere a tehnologiei. Studiul (Securelink, 2016) a relevat faptul că organizațiile care prelucrează informații cu grad redus de reglementare, au integrat cloud computing-ul la nivel ridicat, în schimb, cele care operează cu

informații cu un nivel de reglementare ridicat, au abordat adopția tehnologiei cu mai multă prudență. Se poate trage astfel concluzia că securitatea datelor în sistemele cloud computing încă are provocări majore și numeroase elemente nu sunt clare.

"Complexitatea este inamicul securității" (Geer Jr, 2008) iar cloud computing-ul aduce în cadrul organizațiilor un nivel adițional de abstractizare și utilizare a resurselor care ridică nivelul de complexitate.

Securitatea în general și securitatea datelor în particular nu este un produs, ci mai degrabă o stare către care tinde un sistem informațional. Se impune deci implementarea unor instrumente adecvate de management al riscurilor pentru identificarea elementelor care pot modifica starea de securitate a datelor, de cuantificare a gradului de influență. De asemenea deciziile managerilor privind strategiile de urmat trebuie aliniate cu politica de management a riscului specifică organizației.

Organizațiile moderne operează într-un mediu concurențial extrem de dinamic în care optimizarea utilizării tuturor resurselor este un element critic pentru succesul acestora. Tehnologia informațională a ajuns în momentul de față la posibilitatea de a oferi organizațiilor capabilități de neegalat în domeniul managementului datelor, care pot fi utilizate pentru obținerea de avantaje competiționale. Integrată corespunzător în procesele organizaționale, tehnologia informațională este un element care poate potența activitățile desfășurate și crește eficiența acestora. Valoarea pe care o aduce acest domeniu în cadrul unei organizații necesită reconsiderarea acesteia dintr-o resursă cu caracter de suport al altor activități în una de nivel strategic, necesitând abordări corespunzătoare din partea decidenților de nivel superior. Cloud computing-ul este un exemplu elocvent al acestei categorii de resurse organizaționale, implementarea acestuia la nivelul organizațiilor aducând numeroase beneficii concretizate în avantaje economice. Domeniul introduce paradigme și arhitecturi noi de procesare și manipulare a datelor care măresc nivelul de expunere a acestora și necesită analize comprehensive ale riscurilor de securitate înainte de luarea deciziei strategice de angajare a organizației pe această direcție.

1.2 Obiectivele tezei

În cadrul acestei teze de doctorat autorul își propune următoarele obiective:

O1. Primul obiectiv specific constă în realizarea unei analize a stadiului actual tehnologic în domeniul cloud computing focusată pe implicațiile pe care le are tehnologia asupra securității datelor. În cadrul acestei analize o componentă importantă este identificarea riscurilor de securitate și a implicațiilor pe care le au acestea asupra managementului securității în aceste medii.

O2. Al doilea obiectiv specific are în vedere analiza eficacității strategiilor actuale utilizate în securizarea activelor specifice tehnologiei informaționale în mediul cloud computing. Creșterea rapidă a incidentelor de securitate și impactul major al acestor acțiuni distructive asupra organizațiilor moderne ridică semne de întrebare, asupra capacității strategiei clasice de apărare, de a face față acestor provocări. Obiectivul presupune de asemenea realizarea unei analize a mediului de securitate din sistemul informatic bazat pe tehnologii cloud computing din cadrul Institutului de Cercetare, Dezvoltare și Inovare – Produse High-Tech pentru Dezvoltare Durabilă (ICDT-Pro-DD) – al Universităţii Transilvania din Braşov și a modului în care strategia clasică poate răspunde nevoilor mediului informațional actual.

O3. Al treilea obiectiv constă în identificarea uneia sau a mai multor strategii noi care să suplinească sau să înlocuiască strategia clasică a apărării în adâncime. Caracteristicile focusate pe dinamism, flexibilitate, viteză, impactul strategic al tehnologiei, cantități mari de date prelucrate specifice mediului tehnologic actual determină necesitatea identificării unor strategii noi de operare care să facă față într-un mod sustenabil acestor provocări.

O4. Metodele cele mai utilizate de obscurizare a datelor (criptarea si mascarea) au limitări care determină ineficiențe amplificate de specificul mediilor informaționale moderne. Al patrulea obiectiv specific constă în studierea token-izării ca metodă de obscurizare a informației

și identificarea capabilităților pe care această tehnologie le-ar putea oferi organizațiilor care adoptă arhitecturi cloud computing.

O5. Al cincilea obiectiv specific stabilit constă în studierea procesului de obscurizare a datelor în mediile cloud computing, al identificării limitărilor care există în momentul de față și propunerea unui model îmbunătățit de obscurizare a acestora. În cadrul acestui obiectiv se intenționează realizarea unei aplicații de automatizare a obscurizării informațiilor și identificarea posibilităților de utilizare a acesteia.

O6. Al șaselea obiectiv constă în analizarea sustenabilității modelului de obscurizare automată a informațiilor propus anterior și a capacității acestuia de a oferi organizațiilor capabilități îmbunătățite de management a securității datelor. Obiectivul presupune desfășurarea unei analize a modelului bazată pe evaluarea investițiilor în securitate și a managementului riscurilor de securitate în cadrul noii arhitecturi de management al datelor propusă.

1.3 Prezentarea capitolelor tezei

Securizarea datelor în sistemele informatice este considerată, de o lungă perioadă de timp, ca fiind un element auxiliar care introduce limitări și are costuri nejustificate.

În cadrul acestei teze am încercat să demonstrez că securitatea datelor este un element critic pentru organizațiile care activează în mediile moderne, bazate pe tehnologii cloud computing. Dependența ridicată a organizațiilor moderne și a persoanelor de aceste tehnologii face ca modificările acestora să constituie elemente puternic perturbatoare la nivelul mediului operațional organizațional clasic. Securizarea activelor de tehnologia informației se constituie astfel, ca un element care condiționează performanța sistemelor tehnologice și implicit capacitatea acestora de a răspunde nevoilor organizației.

O altă dimensiune esențială a unui plan strategic de protecție a datelor unei organizații este reprezentată de sustenabilitatea economică a investițiilor în securitate. Strategiile aplicate trebuie să răspundă riscurilor cu care se confruntă organizația, dar în același timp este necesară dimensionarea și calibrarea lor în funcție de posibilitățile de alocare a resurselor. În acest context, automatizarea mecanismelor de securitate oferă posibilitatea organizațiilor de a răspunde eficient provocărilor de securitate. Această abordare răspunde într-un mod sustenabil economic dinamismului ridicat specific mediului cloud computing, într-un cadru corespunzător de management al riscurilor de securitate.

În capitolul I am făcut o introducere în domeniu prin prezentarea rolului pe care îl are tehnologia în mediile organizaționale actuale și a importanței măsurilor de securizare a activelor informaționale. Am făcut o prezentare a obiectivelor de cercetare stabilite și a capitolelor tezei.

În capitolul II am făcut un studiu a stadiului tehnologic actual al tipurilor de sisteme cloud computing, a modelelor de oferire a serviciilor, precum și o analiză comprehensivă a riscurilor de securitate specifice acestor sisteme. Acest capitol răspunde obiectivului specific numărul 1.

În capitolul III am făcut o analiză a strategiilor de securizare a mediului informațional din organizațiile clasice. Caracteristicile specifice mediului informațional modern datorate tehnologiilor cloud computing precum complexitatea, diversitatea, flexibilitatea, caracterul globalizator, precum și impactul marcant pe care datele îl au asupra organizațiilor și persoanelor au determinat o modificare a profilului infractorului informatic și a strategiilor folosite de acesta. În acest capitol am desfășurat o analiză cu scopul de a determina capacitatea strategiilor clasice de a face față provocărilor de securitate specifice mediilor cloud computing. Analiza a scos în evidență o serie de riscuri pe care strategia clasică nu le poate administra corespunzător, asigurarea securizării datelor în acest mediu necesitând o nouă abordare de nivel strategic care impune dezvoltarea unor alte mecanisme de protecție. În acest sens am propus un număr de inițiative strategice, adaptate mediilor cloud computing, care asigură un cadru de lucru multivalent, concertat, sustenabil economic, bazat pe managementul riscului și maximizarea eficacității instrumentelor de nivel tactic și operativ folosite în securizarea activelor informaționale. Prin abordarea inovatoare, holistică asupra tehnicilor de securizare a datelor

utilizate în aceste sisteme am încercat să unific și să completez inițiativele individuale făcute de diferite entități. Acest capitol răspunde obiectivelor de cercetare specifice 2 și 3.

În capitolul IV am analizat principalele tehnici de obscurizare a datelor (criptarea, mascare și token-izarea) identificând avantajele și limitările fiecăreia dintre ele. La momentul actual token-izarea este folosită în principal în industria plăților electronice, dar analiza a scos în evidență faptul că tehnologia este subevaluată. De asemenea, datorită avantajelor sale față de alte tehnici de obscurizare, ea oferă capabilități superioare pentru mediile de lucru bazate pe tehnologii cloud computing.

Analiza depășește nivelul simplei comparații a capacităților tehnice și prezintă impactul acestor tehnologii asupra unei organizații. Ea poate fi utilizată de către factorii de decizie în eforturile lor de a proiecta și implementa o strategie viabilă de protecție a datelor pentru organizarea lor, încercând în același timp să minimizeze costurile IT din punctul de vedere al consumului de resurse și al perturbării proceselor interne de afaceri. Acest capitol răspunde obiectivului specific numărul 4.

Capitolul V dezvoltă conceptul de automatizare a procesului de obscurizare a informațiilor propus. Astfel, limitările actuale ale procesului de obscurizare utilizat în organizații, pot fi depășite prin utilizarea unor algoritmi automatizați de selecție, procesare și obscurizare. În acest capitol este prezentat în detaliu modelul teoretic al acestui sistem precum și o variantă de implementare practică bazată pe serviciile platformei IBM Bluemix. De asemenea, pentru fundamentarea modelului, am realizat o analiză de oportunitate a acestui sistem din perspectiva costurilor necesare și a managementului riscului. Acest capitol răspunde obiectivelor de cercetare specifice 5 și 6.

În capitolul VI sunt prezentate concluziile generale ale acestei cercetări, contribuțiile originale aduse, lucrările în care au fost diseminate rezultatele cercetărilor efectuate și o scurtă prezentare a viitoarelor direcții de cercetare.

2. Stadiul actual al cercetării in domeniu

2.1 Specificul mediului cloud computing

Evoluțiile tehnologice din domeniul hardware-ului din ultimele decenii au condus la situația în care este posibilă preluarea, transmiterea, stocarea, procesarea și manipularea unor cantități foarte mari de date. Aceste capabilități specifice mediului informațional modern necesită performanțe computaționale care depășesc posibilitățile unui computer personal făcându-le inaccesibile utilizatorilor obișnuiți. Totuși, datorită avantajelor oferite de accesul la aceste cantități importante de date industria de profil a încercat diferite soluții pentru a face disponibile aceste resurse consumatorilor, la costuri sustenabile.

Soluția centralizării puterii de calcul, a capacităților de stocare, de procesare a datelor și oferirea resurselor informatice clienților sub formă de servicii s-a profilat în ultimele decenii ca o soluție de succes oferind capabilități informaționale, cu costuri optimizate, care se adaptează rapid la dinamica extinsă a mediului în care performează organizațiile moderne.

În ultimele două decenii s-au depus eforturi constante pentru dezvoltarea de soluții la aceste probleme rezultând tehnologii precum „grid computing” sau arhitecturi „peer – to – peer”. Acestea au format bazele pe care s-au dezvoltat aplicații care au schimbat modul în care interacționăm astăzi cu tehnologia: Napster – punerea în comun a datelor, Google – motoare de căutare, Facebook – rețele de socializare, Dropbox – stocare date în rețea etc. Deși, până nu demult, domeniul a atras doar interesul unui număr limitat de organizații (companii din domeniul tehnologic, oameni de știință, cercetători etc.) în ultimul deceniu s-a dezvoltat o largă piață de consum tehnologiile fiind integrate într-un spectru din ce în ce mai larg de activități, atât la nivelul companiilor cât și al persoanelor fizice deopotrivă. Această paradigmă nouă de lucru și de management al tehnologiei informaționale este cunoscută sub numele de “cloud computing”.

Noutatea acestui domeniu se manifestă și la nivel conceptual, astfel că însuși definirea lui este un lucru încă disputat între specialiști. Tehnologia a cunoscut o evoluție fulminantă, dezvoltarea ei făcându-se necoordonat, fără un cadru bine stabilit, în funcție de interesele și inițiativele diferiților actori din domeniu. Însăși denumirea "cloud computing" asignată acestui domeniu permite crearea acestui cadru larg de dezvoltare și utilizare fără a direcționa sau limita pe o anumită direcție eforturile celor care o utilizează. Datorită acestor particularități, încercările de definire a acesteia au anumite caracteristici particulare și spectre largi de manifestare reflectând, de cele mai multe ori, domeniul de interes al entității care a încercat promovarea acelei definiții. Una dintre cele mai comprehensive definiții este cea dată de Institutul National de Standarde și Tehnologii, SUA astfel: "Cloud computing-ul este un model pentru asigurarea ubicuă, convenabilă, la cerere a serviciilor de acces la un fond comun de resurse computaționale configurabile (ex. rețele, servere, stocare, aplicații și servicii) care pot fi rapid date în funcțiune și eliberate, cu minim efort administrativ sau interacțiune a furnizorului" (Mell P., 2011).

Din punctul de vedere al consumatorului, cloud computing-ul permite accesul, într-un timp foarte scurt, cu costuri optimizate, la o cantitate considerabilă de resurse computaționale, acestea având, capacitatea de a fi integrate rapidă în procesele organizaționale pe care le desfășoară.

Cloud computing-ul poate fi considerat ca următoarea generație de sisteme de calcul, oferind consumatorilor servicii rapide cu un grad mare de personalizare prin intermediul rețelelor de calculatoare. Acesta poate furniza capabilități de accesare și prelucrare a datelor utilizând active computaționale într-o arhitectură bazată pe punerea în comun și distribuția de resurse.

Dinamica extinsă a mediului de lucru în care operează organizațiile moderne necesită un suport informațional pe măsură bazat pe flexibilitate, dinamică, adaptabilitate, eficientizare, scalabilitate, reziliență etc. iar cloud computing-ul oferă, în temeni de configurații hardware și software, o alternativă optimă financiar la soluția clasică de creare a infrastructurii specifice prelucrării informației.

Utilizarea echipamentului unei alte entități pentru procesarea, stocarea și transmiterea datelor ridică totuși numeroase semne de îngrijorare referitoare la păstrarea securității datelor în acest mediu modern de manipulare. Externalizarea serviciilor de tehnologia informației către terți contractori adaugă cadrului clasic de management al datelor riscuri suplimentare precum: managementul autorității, acorduri privind cantitatea și calitatea serviciilor, evitarea blocării la un singur furnizor, integrarea cu sistemele clasice existente etc. care trebuie să fie tratate cu atenție sporită de către organizație înainte de a se angaja pe drumul migrării către cloud computing.

Securizarea datelor în mediul cloud computing este o provocare actuală majoră și a fost identificată ca fiind principalul element care descurajează organizațiile să se angajeze mai puternic în adoptarea ei (Securelink, 2016). Studiul făcut de Securelink în 2016 a identificat următoarele elemente ca fiind principalele obstacole ale acceptării acestei tehnologii în mediul guvernamental și privat:

Probleme de securitatea datelor: 86%;
Probleme de conformitate: 86%;
Confidențialitate: 79%
Retenție și distrugere: 79%
Locația datelor: 75%

Studiul a evidențiat de asemenea faptul că rata de acceptanță a noii tehnologii pentru organizațiile private este mai mare decât pentru organizațiile guvernamentale sau cele care operează în domenii cu un nivel înalt de reglementare (bănci, sănătate, securitate etc.). Astfel, organizațiile care operează în medii guvernamentale sau cu un nivel înalt de reglementare prezintă un nivel redus de atragere a tehnologiilor cloud computing și de migrare a capabilităților computaționale către servere publice. Motivația din spatele acestui ritm redus rezidă în riscurile sporite asociate noului mediu de procesare a datelor precum și a provocărilor complexe determinate de asigurarea unui mediu corespunzător de protecție a datelor. Drept urmare,

organizațiile care operează în domenii cu un nivel sporit de reglementare sunt ezitante în introducerea tehnologiilor specifice cloud-ului ca formă de inovare tehnologică și au posibilități limitate de a profita de capabilitățile deosebite ale noului mediu de lucru.

Noul mediu de manipulare ridică probleme complexe privind securizarea datelor, atât în domeniul asigurării unei arhitecturi sigure de prelucrare la nivelul proceselor tehnologice care se desfășoară în interiorul cloud-ului, cât și la nivelul managerial. Instrumentele și politicile specifice mediilor clasice au, în momentul utilizării în mediile cloud, limitări considerabile în asigurarea unui cadru optim de control al datelor și transparentizare a operațiunilor care le afectează.

O altă provocare este direct legată de educarea consumatorilor pentru a înțelege potențialul acestui nou cadru de lucru. Astfel că, deși foarte multe organizații confirmă că au fost expuse la informații cu privire la noile concepte, se observă un nivel ridicat de confuzie, neînțelegere sau înțelegere greșită a capabilităților și limitărilor noii tehnologii.

2.2 Modele de implementare

Orice echipament de calcul dispune de resurse esențiale care concură la executarea sarcinilor primite: procesor pentru realizarea calculelor, memorie pentru stocarea datelor și echipamente de intrare/ieșire pentru introducerea și scoaterea datelor din sistem. Aceste tipuri de resurse se regăsesc în toate sistemele informaționale, indiferent că sunt clasice sau virtualizate. Utilizarea virtualizării în arhitecturile sistemelor moderne nu elimină necesitatea existenței acestora, ci doar concură la atingerea unor beneficii: utilizarea eficientă a resurselor, scalabilitate, adaptabilitate, separarea responsabilităților, asigurarea disponibilității etc.

Cloud computing-ul are capacitatea de a crea o gamă largă de medii extrem de flexibile cu un grad mare de adaptabilitate la nevoile organizației. (Sosinsky, 2011) realizează o grupare a acestora în patru categorii în funcție de metodele de implementare, astfel:

- *Cloud-ul public* – este realizat pe baza unor investiții considerabile, de obicei ale unei entități private, fiind pus la dispoziția consumatorilor din rațiuni comerciale. Acest tip de cloud este considerat un model economic de succes permițând companiilor să dezvolte și să publice, cu un efort financiar minim, servicii în cloud. El se pretează pentru cei care nu doresc să investească sume mari în echipamente pe care le vor folosi doar temporar. În acest model companiile pot da în funcțiune și renunța foarte repede la echipamente, în funcțiile de nevoile particulare ale diferitelor proiecte în care sunt angrenate. Infrastructura fizică care deservește clienții este localizată în centrele de procesare ale furnizorului de cloud. Din punct de vedere al asigurării securității datelor acest model este unul cu expunere ridicată din mai multe considerente:
  - Spațiul de stocare, liniile de comunicație sunt folosite în comun cu alți beneficiari de servicii al căror profil nu este cunoscut;
  - Procesarea datelor se face utilizând aceleași echipamente pentru toți utilizatorii, utilizând mecanisme de distribuire în timp a sarcinilor;
  - Administratorii platformei au sau pot obține drepturi de acces la toate resursele existente pe platformă;
  - Auditarea sistemelor este făcută, de cele mai multe ori, intern de către furnizorul de servicii utilizând mecanisme și proceduri aflate sub controlul acestuia. Există posibilitatea de a efectua și auditări externe, dar acestea se fac doar la anumite momente punctuale în timp (nu sunt permanente) și cu costuri suplimentare.
- *Cloud-ul privat* – este reprezentat de acele medii în care resursele sunt în întregime ale unei singure organizații, fiind destinate cu precădere pentru consumul membrilor organizației respective. Această soluție este preferată atunci când organizația dorește să-și administreze singură echipamentele. Drepturile de proprietate a echipamentelor și licențelor aparțin organizației, ea fiind responsabilă de platformă din toate punctele de vedere (instalare, mentenanță, monitorizare, dezvoltare și dezafectare). Utilizatorii au acces la aplicații și servicii folosind echipamente agreate și respectând procedurile

aprobate de către organizație. Cloud-ul privat poate fi dislocat pe echipamente localizate în perimetrul organizației sau în centre de date aflate în administrarea unei alte entități, în ambele cazuri configurarea, exploatarea și administrarea platformei fiind efectuată după preferințele organizației. Personalul care efectuează administrarea este validat de către organizație, de cele mai multe ori fiind sub controlul direct al acesteia. Costurile pentru organizație, asociate cu acest tip de cloud sunt mai ridicate față de alte modele de implementare, dar nivelul de risc este scăzut deoarece:

- Datele sunt manipulate în întreaga lor existență utilizând echipamente care au un grad ridicat de încredere, ele aparținând sau fiind sub directul control al organizației;
- Utilizatorii cu drepturi administrative sunt persoane de încredere cu un nivel ridicat de loialitate față de organizație;
- Procedurile după care se realizează managementul datelor sunt sub controlul strict al organizației;
- Se pot obține rapid rapoarte, cu un nivel ridicat de încredere, referitoare la starea tehnică si operațională a platformei, adaptate la cerințele specifice ale organizației;
- Dezvoltarea procedurilor privind accesul la echipamente este realizată de către echipe cu un nivel ridicat de loialitate și care cunosc procesele organizaționale. Produsele obținute au astfel un grad ridicat de securitate și adaptabilitate la nevoile și specificul organizației.

- *Cloud-ul de comunitate* – este rezultat ca urmare a punerii în comun a resurselor IT de către mai multe organizații pentru a satisface anumite interese, obiective și cerințe similare. Echipamentele sunt localizate într-un centru de date intern sau extern aflat sub controlul membrilor. Acest tip de cloud permite organizațiilor să beneficieze de avantajele operaționale specifice tehnologiei cloud dar limitând în același timp riscurile de securitate. Din punct de vedere al securizării datelor modelul este caracterizat de următoarele elemente:
  - Resursele computaționale (spațiu stocare, linii comunicație etc.) sunt folosite în comun cu ceilalți membri ai comunității, profilul acestora având un nivel acceptabil de încredere;
  - Accesul persoanelor din exteriorul comunității la resursele platformei este limitat;
  - Utilizatorii cu drepturi administrative sunt persoane care au fost validate de membrii comunității, existând mecanisme de control al acestora;
  - Se pot obține relativ rapid, rapoarte, cu un nivel acceptabil de încredere, referitoare la starea tehnică și operațională a platformei;
  - Auditarea internă a sistemelor este făcută utilizând proceduri, instrumente și persoane care sunt sub controlul membrilor comunității;
  - Configurarea, administrarea, accesul și disponibilizarea resurselor se fac după proceduri dezvoltate de membrii comunității necesitând consensul acestora.
- *Cloud-ul hibrid* – este o combinație dintre două sau mai multe tipuri de cloud-uri prezentate anterior care, deși rămân entități distincte, sunt interconectate pentru oferirea de capabilități multiple ale respectivelor modele de implementare. Prin utilizarea acestor arhitecturi organizațiile și persoanele fizice sunt capabile să obțină niveluri superioare de disponibilitate a serviciilor, combinate cu capacități de dare în funcțiune rapidă fără a fi dependente integral de serviciile unor terțe părți. Acest tip de arhitectură necesită resurse interne și externe. În cazul lor se fac compromisuri cu privire la securitatea, flexibilitatea și siguranța datelor prelucrate intern pentru a beneficia de alte avantaje precum redundanță, scalabilitate, disponibilitate etc.

Fiecare dintre aceste modele de livrare a serviciilor vine cu avantaje si dezavantaje în ceea ce privește cantitatea, calitatea și securitatea serviciilor oferite. Cloud-ul public are beneficii operaționale și de cost care avantajează, la o primă vedere, organizațiile care îl aleg și le oferă un

avantaj clar pe piață. Cu toate acestea, datorită riscului ridicat de compromitere a datelor, el nu este pretabil a fi implementat de către organizații care prelucrează informații cu nivel ridicat de sensibilitate, acestea necesitând să se orienteze către alte forme de implementare.

2.3 Modele de livrare a serviciilor

Tehnologia cloud computing se bazează pe o abordare modernă de dezvoltare software denumită arhitectură orientată pe servicii. Tehnica se a pe livrarea către beneficiar a unei suite de funcții, denumite servicii, într-o manieră integrată și orchestrată prin intermediul unor opțiuni și funcționalități. Aceste servicii sunt implementări software ale capabilităților platformei și pot fi utilizate în combinații variate pentru atingerea scopurilor celui care le utilizează. Furnizorii de cloud computing oferă servicii sub forma a trei modele fundamentale (Armbrust M., 2010):

- Infrastructura ca serviciu (IaaS),
- Platformă ca serviciu (PaaS);
- Sofware ca serviciu (SaaS).

Cele trei modele de oferire a serviciilor se diferențiază prin capacitatea utilizatorilor de a avea acces la categoriile de resurse și implicit de a-și personaliza mediile de lucru. În figura 2.1 este reprezentată schematic ierarhia și modelul de integrare al acestora. Separarea se menține și la nivelul responsabilităților referitoare la asigurarea securității datelor, capacitatea de a avea acces la un anumit nivel al resurselor determinând și responsabilitatea asigurării protecției sistemelor la acel nivel.

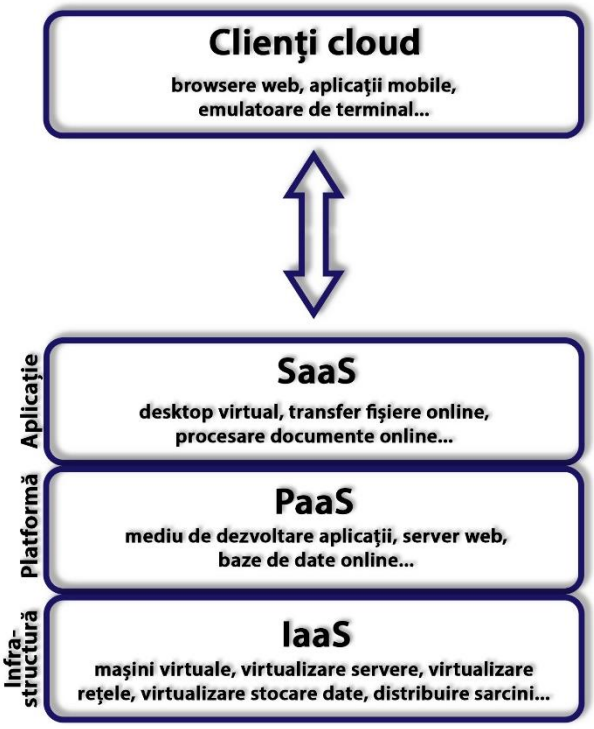

Fig. 2.1 Schema modelelor de servicii în cloud

Infrastructura ca serviciu (IaaS) reprezintă capabilitatea oferită utilizatorului de servicii cloud computing de a putea proviziona capabilități de procesare, stocare, rețea precum și orice altă resursă fundamentală de calculator. Prin utilizarea acestui model se pun la dispoziția beneficiarilor echipamente hardware virtualizate (procesor, spațiu de stocare, memorie, echipamente de rețea etc.) sub forma unor servicii pentru care se plătește în funcție de performanța lor și timpul de utilizare/rezervare.

Platforma ca serviciu (PaaS) este un model de livrare a serviciilor în care furnizorul are capacitatea de a implementa aplicații utilizând limbaje de programare și instrumente puse la dispoziție de către furnizor (ex. C++, Java, Python, .NET). În acest caz utilizatorul are posibilitatea de a dezvolta, utiliza și administra propriile sale soluții software, fără a fi preocupat de problematica asigurării resurselor hardware și software care să facă posibilă desfășurarea unei astfel de activități. Utilizatorul nu are drepturi administrative la platforma suport (infrastructură, servere, spațiu de stocare, sisteme de operare), el putând administra și configura doar resursele puse la dispoziție și este responsabil doar de asigurarea securității datelor la nivel de aplicație. În acest model responsabilitățile asigurării securității, disponibilității tuturor serviciilor sunt în sarcina furnizorului de servicii care trebuie să întrunească condițiile de asigurare la care s-a angajat. Exemple de platforme care oferă astfel de servicii sunt: Amazon Web Services, IBM Bluemix, Cloud Foundry, Google App Engine, Oracle Cloud PaaS, Acquia Cloud etc. (Stackify, 2017).

Modelul sofware ca serviciu (SaaS) reprezintă capabilitatea oferită utilizatorului de a folosi aplicațiile disponibile pe platforma furnizorului. Acestea sunt accesibile prin intermediul a numeroase terminale client, de cele mai multe ori bazate pe tehnologii web (e-mail prin web, site

web, acces la spațiu de stocare prin web etc.). În acest caz consumatorul nu are acces la platforma cloud de suport, la rețea, servere, sisteme de operare, spațiu de stocare el având doar drepturi limitate de personalizare a aplicațiilor pe care le utilizează. În acest caz asigurarea tuturor capabilităților platformei, inclusiv cele de întrunire a condițiilor de securizare a informației sunt în responsabilitatea furnizorului de servicii.

Ca exemple de astfel de platforme se pot aminti: procesoare de documente online ca Google Docs, furnizori e-mail (Gmail, Yahoo Mail), platforme de management al clienților (Salesforce, Microsoft Dinamics CRM).

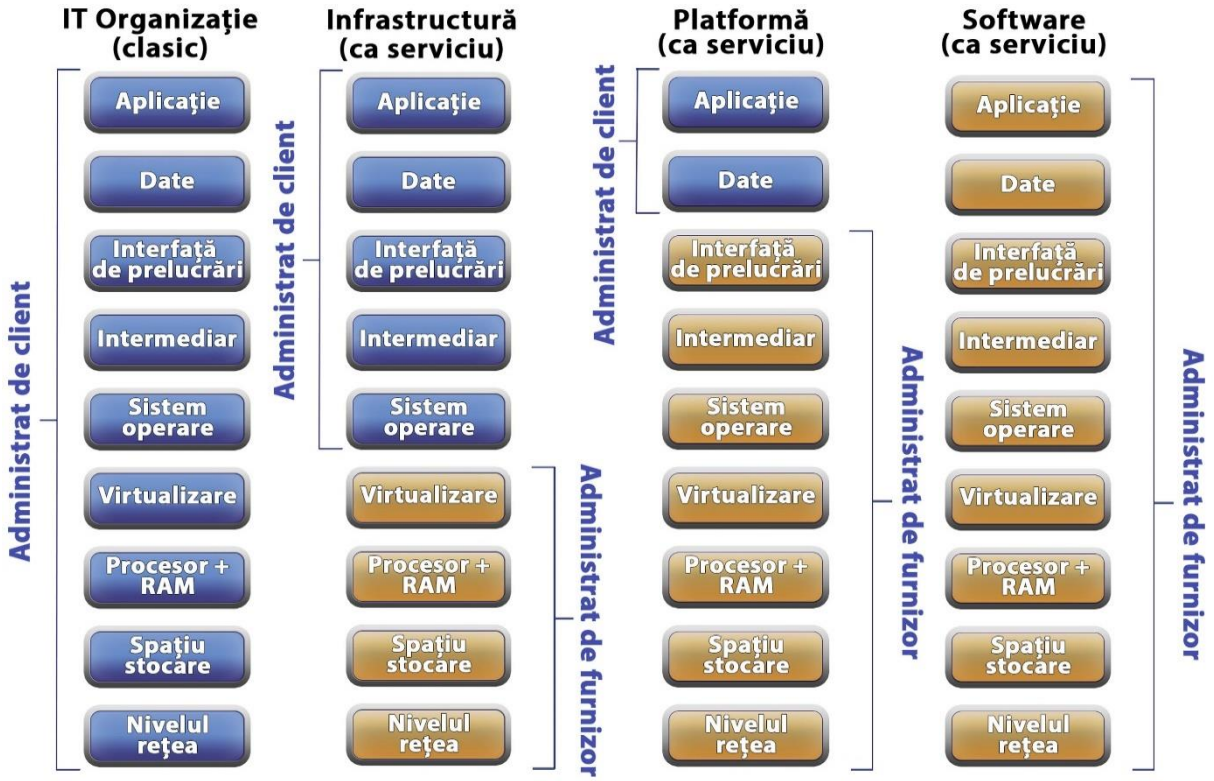

Fig. 2.2 Schema împărțirii responsabilităților între furnizor și consumator

În figura 2.2 este reprezentată grafic situația comparativă a responsabilităților care revin furnizorului și consumatorului de resurse informatice atât în varianta clasică, cât și în cele trei modelele de livrare a serviciilor în cloud computing. Graficul evidențiază de asemenea faptul că, în funcție de categoria de servicii aleasă, responsabilitățile securizării diferitelor componente se distribuie diferit între cei doi actori.

Utilizarea resurselor informaționale în arhitecturile cloud computing modifică spectrul clasic de responsabilități în privința securizării datelor. Înțelegerea noilor concepte de operare a

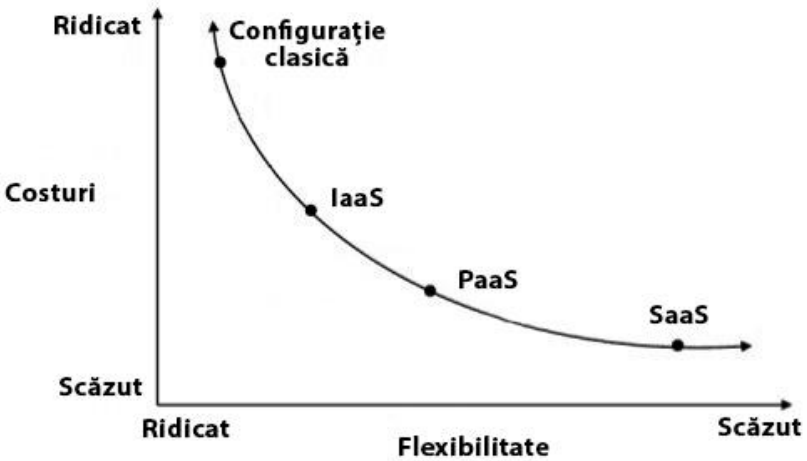

Fig. 2.3 Graficul distribuției costurilor

datelor și a responsabilităților care le revin fiecăruia dintre entitățile implicate constituie un element de bază pentru asigurarea unui management corespunzător a securității datelor.

Un element esențial care face atractivă tehnologia cloud computing este posibilitatea minimizării costurilor organizației în domeniul tehnologiei informației. În analiza IBM din 2014, reprezentată în figura 2.3 se poate observa graficul de distribuție a costului total de posesie - total cost of ownership (TCO) pentru aceste modele de servicii. Acesta este ridicat în sistemele clasice și se micșorează o dată cu centralizarea resurselor și cedarea responsabilităților de administrare a acestora către alte organizații, fiind minim în arhitecturile care folosesc modelul software ca serviciu.

Pe axa orizontală a graficului s-a ales indicatorul "flexibilitate" care în domeniul securității datelor poate fi asimilat cu capacitatea unui beneficiar de a iniția, dezvolta și implementa, după nevoile sale particulare, politicile optime de asigurare a unui cadru sigur de prelucrare a datelor.

Se poate astfel concluziona că avantajele economice ale adoptării tehnologiilor cloud computing sunt invers proporționale cu riscurile aferente compromiterii datelor datorită manipulării acestora de către alte entități. Astfel cu cât mai multe capabilitățile informaționale sunt mai dependente de servicii oferite de alte entități cu atât costurile aferente pot fi minimizate dar se constată o creștere a numărului de riscuri asociate.

2.4 Managementul riscului în sistemele cloud computing

Migrarea datelor organizațiilor în mediul cloud și importanța sporită pe care acest mediu îl are pentru organizații determină și creșterea impactului pe care le-ar putea avea eventualele disfuncții în asigurarea serviciilor. Riscul în domeniul securității datelor pentru sistemele cloud computing-ului se concretizează în probabilitatea ca un client să nu poată beneficia de datele sale dispuse într-un mediu cloud, la întreaga lor valoare, la momentul și în cantitatea de care acesta are nevoie.

La nivelul unei organizații se pot identifica mai multe domenii de risc pe care aceasta trebuie să le administreze: managementul programelor, al investițiilor, al lanțului de furnizare, al personalului, al legalității activității, ș.a.m.d. unul dintre domeniile extrem de sensibile fiind cel al securității datelor.

Managementul riscului este un proces deliberat de înțelegere a acestuia, de luare a unor decizii și implementare a unui plan de măsuri pentru atingerea unui nivel acceptat de organizație raportat la costuri. Managementul riscului include identificarea, evaluarea și controlul nivelului acestuia trebuind abordat ca o activitate holistică care este complet integrată în activitățile desfășurate.

2.5 Riscuri de securitate ale arhitecturii cloud computing

Tehnologia cloud computing are la bază aplicații, platforme și segmente de rețelistică care execută diferite operații, putând oferi o varietate largă de produse și servicii pentru utilizatori individuali sau organizații care activează în mediul guvernamental sau privat din întreaga lume. Cloud computing-ul este construit pe un număr mare de alte tehnologii care conlucrează, cum ar fi: virtualizarea rețelelor de calculatoare, sisteme de operare, baze de date, tehnologii web, distribuirea sarcinilor, planificarea utilizării resurselor, controlul accesului, managementul memoriei etc. Acest mediu de lucru potențează capabilitățile oferite de oricare dintre tehnologiile amintite, determinând îmbunătățirea serviciilor oferite către entitățile care aleg să-l utilizeze.

Cloud computing-ul are și numeroase limitări și vulnerabilități, unele dintre ele apărând ca urmare a noii arhitecturi de lucru, însă majoritatea sunt datorate tehnologiilor care stau la baza acestuia.

Arhitectura de securitate constă în construirea unui mediu de operare care permite manipularea datelor într-un mod sigur în toate stările acestora: în repaus, în procesare și în

transfer. În lista de mai jos sunt prezentate principale provocări pe care le-am identificat specifice acestui mediu de operare:

- Accesul la servere și date
- Securizarea virtualizării
- Securitatea rețelei
- Securitatea datelor
- Segregarea datelor
- Standardizarea
- Transferul datelor
- Managementul actualizărilor de securitate
- Acordul de furnizare a serviciilor
- Interoperabilitate

2.5.1 Accesul la servere și date

În centrele de date clasice realizarea accesului la echipamente este controlat și restricționat utilizând mecanisme multiple de limitate a accesului. Astfel, în afară de mecanismele de control digitale există o serie de mecanisme și proceduri de filtrare a persoanelor care au posibilitatea să acceseze fizic echipamentele. Organizațiile pot avea astfel un control facil și o imagine clară în orice moment asupra persoanelor care au interacționat cu anumite echipamente. Controlul digital al accesului este realizat, implementat și monitorizat de către persoane din cadrul organizației prin utilizarea unor mecanisme interne cu factor ridicat de încredere.

Spre deosebire de acesta, în mediul cloud computing, barierele fizice sunt limitate în mare parte la nivelul furnizorului, iar beneficiarul serviciilor nu are posibilitatea să intervină în acest proces. În funcție de modelul de servicii ales, activitățile de administrare sunt efectuate, în ponderi diferite, de către furnizor și beneficiar. Spre deosebire de furnizor, care are la dispoziție acces direct la infrastructură și poate utiliza legături directe la mediul cloud, beneficiarul trebuie să acceseze resursele prin intermediul unor conexiuni la distanță. Existența acestora și posibilitatea compromiterii lor crește riscul accesului neautorizat la resursele organizației iar securizarea lor devine un element critic în mediul de operare cloud computing.

Mecanismele de control al datelor în arhitecturile clasice sunt direct relaționate cu politicile de securitate care modelează accesul utilizatorilor la ele. Furnizorul de servicii cloud computing trebuie să ofere mecanisme corespunzătoare pentru implementarea în mediul pus la dispoziție a unor astfel de politici, oferind posibilitatea configurării accesului la resurse doar pentru utilizatorii autorizați.

Managementul conturilor de utilizator este o operațiune complexă pentru realizarea căreia trebuie să existe o colaborare strânsă între furnizor și administratorii de rețea ai organizației client. Platforma trebuie să ofere un control strict al accesului, opțiuni de înregistrare a activității utilizatorilor și administratorilor, furnizarea de rapoarte despre activitatea acestora pentru a putea identifica rapid pe cine, când și ce resurse a accesat. Asigurarea unei foarte bune transparențe a resurselor utilizate de către furnizor către beneficiar contribuie la creșterea gradului de încredere al celui din urmă în serviciile utilizate.

2.5.2 Securizarea virtualizării

Virtualizarea este una dintre componentele esențiale a tehnologiei cloud computing fiind utilizată pe larg pentru a îmbunătăți capabilitățile acestui mediu cu numeroase atribute dinamice. În principal, ea este utilizată pentru realizarea capacităților de provizionare, reziliență, salvări de siguranță, restaurarea, integrarea sistemelor vechi, migrarea mașinilor în alte medii etc., datorită avantajelor acesteia în ceea ce privește timpul scurt necesar realizării operațiunilor, dar și a costurilor minime implicate în proces din punct de vedere financiar, material și uman. Mai mult, aceste activități pot fi automatizate și declanșate de anumite evenimente, cum ar fi: încărcare

procesor, memorie sau trafic rețea, detectarea unor defecțiuni în sistem, anumite momente de timp predefinite etc., permițând astfel punerea/repunerea rapidă în funcțiune a serviciilor cu un efort administrativ minim tradus în final printr-o îmbunătățire a calității serviciilor oferite consumatorilor.

Totuși, asigurarea funcționării mai multor instanțe de mașini virtuale pe același echipament fizic, într-o deplină izolare una față de cealaltă nu este o sarcină simplă. Natura dinamică, utilizarea în comun a resurselor fizice și permanenta posibilitate de extindere a mașinilor virtuale îngreunează realizarea și menținerea unei securități ferme în vederea limitării propagării vulnerabilităților și a erorilor de configurare. La fel de complexă este și sarcina de a audita și păstra o evidență clară a profilurilor de securitate ale tuturor mașinilor virtuale la orice moment în timp.

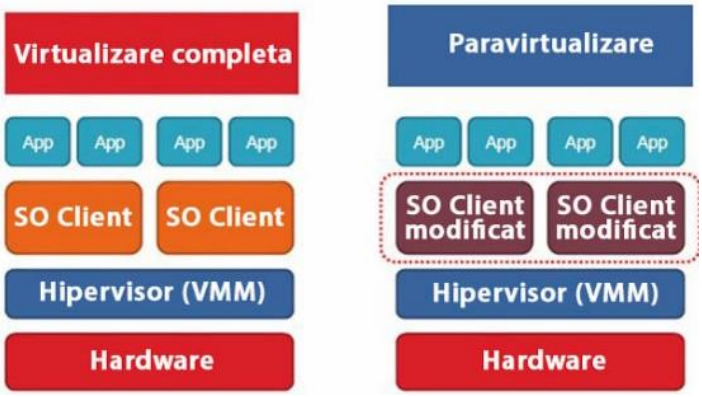

Fig. 2.4 Modele de virtualizare

Virtualizarea completă și para-virtualizarea (figura 2.4) sunt două forme de virtualizare hardware extrem de frecvente în mediul de lucru cloud computing. În prima variantă, sistemul de operare din mașina virtualizată operează la fel ca în mediul clasic și accesează controlerele componentelor hardware emulate fără a ști că lucrează într-un mediu virtual. În paravirtualizare sistemul de operare din mediul virtualizat știe că lucrează într-un mediu virtual și are drivere modificate corespunzător pentru a lansa comenzi de acces la resursele fizice direct mediului gazdă (Durairaj M., 2014).

Avantajele paravirtualizării sunt de ordin operațional, în acest tip de sisteme realizându-se o creștere a eficienței datorită accesării directe a resurselor, a eliminării apelărilor intermediare și a faptului că hipervizorul necesită un nivel redus de resurse computaționale pentru managementul sistemelor găzduite. Totuși, din punct de vedere al securității datelor, virtualizarea completă are o serie de avantaje, cum ar fi:

- Asigură o izolare mai bună a resurselor între mașina gazdă și cea virtuală;
- Elimină riscurile de securitate prin păstrarea driverelor originale;
- Mașinile virtualizate nu sunt conștiente unele de altele.

Majoritatea atacurilor identificate încearcă să distrugă mecanismele de izolare a mașinilor virtuale dintre ele sau față de mediul gazdă, în vederea obținerii accesului la resurse. Nivelul hipervizorului se delimitează astfel ca fiind unul cu un nivel de risc ridicat căruia, deși i se acordă o atenție specială din partea producătorilor, rămâne o țintă de maxim interes datorită potențialului distructiv pe care îl are.

2.5.3 Securitatea rețelei

Arhitectura sistemelor cloud computing se bazează pe interconectarea a numeroase elemente, tehnologia care face posibilă acest lucru fiind cea a rețelelor de calculatoare. În cloud computing acest domeniu este prezent din plin, el fiind mediul de comunicație prin intermediul căruia se realizează accesul clienților la serviciile oferite de furnizor.

Mai mult, cu ajutorul virtualizării, domeniul rețelisticii a avansat spre a veni în suportul beneficiarilor și a oferi o paletă mai largă de capabilități. Astfel, platformele de cloud computing

pun la dispoziție un arsenal complet de instrumente pentru virtualizarea acestei resurse și dezvoltarea de rețele complexe, complet virtualizate. Necesitatea dezvoltării acestor rețele se datorează și modificării tipului de trafic de date. Astfel raportul dintre traficul de date între centrul de date și terminale externe (trafic nord-sud) și traficul de date între mașini de calcul din interiorul unui centru de date(trafic est-vest) a avut o evoluție accentuată în favoarea celui din urmă o dată cu dezvoltarea cloud computingului.

Virtualizarea rețelelor de calculatoare nu a dus la îmbunătățirea directă și a securității datelor transmise. Astfel, problemele asociate cu atacurile care vizează vulnerabilități la primele 4 niveluri ale modelului rețelei Open Systems Interconnection (OSI) (Microsoft, 2018) se regăsesc și în mediul cloud. Mai mult, acestora li se adaugă vulnerabilități ale platformelor de virtualizare. Securizarea datelor în tranzit devine astfel o problemă mai complexă decât în mediile clasice.

2.5.4 Securitatea datelor

Într-un mediu informațional clasic, în care echipamentele utilizate sunt dispuse într-o locație aflată sub controlul și administrarea organizației, acestea fac obiectul politicilor de securitate care reglementează aspecte legate de: protecția fizică, măsuri INFOSEC, de certificare a furnizorilor, de validare a personalului, de stabilire a accesului la resurse, de monitorizare a controlului etc. Spre deosebire de acest mediu, în arhitecturile cloud computing, datele organizațiilor sunt transmise, stocate și prelucrate folosind resursele puse la dispoziție de platforma furnizorului. În aceste platforme organizațiile nu pot implementa sau pot implementa parțial o parte din politicile lor, necesitând concursul furnizorului pentru completarea mecanismelor de securitate. Echipamentele, personalul, liniile de comunicații utilizate nu se află sub controlul strict al organizației și trebuie considerate de către aceasta ca având un nivel limitat de încredere.

Fig. 2.5 Ciclul de viață a datelor

Asigurarea securității datelor într-o astfel de arhitectură necesită instrumente și proceduri adecvate pentru a face față provocărilor din noul mediu. Modelul de securitate al datelor, acceptat ca standard de facto în industrie, este bazat pe trei criterii fundamentale: confidențialitate, integritate și disponibilitate – confidentiality, integrity, availability (CIA) (Panmore Institute, 2016), fiecare dintre acestea necesitând a fi satisfăcute.

Problematica securizării datelor în domeniul cloud computing este una care necesită o abordare holistică, care să țină cont de toate elementele cu care acestea pot interacționa pe întreg ciclul lor de viață (figura 2.5). Ciclul de viață a datelor există și în mediile clasice, dar în mediile cloud computing etapele prin care trec acestea sunt mai complexe, implică mai multe entități. Rezultă astfel o creștere a riscului compromiterii acestora care necesită un management mai atent. Ca o consecință, utilizatorul de servicii cloud computing trebuie să țină seama de noile caracteristici ale mediului de lucru și să adopte mecanisme suplimentare de verificare și monitorizare pentru a preveni brețele de securitate și compromiterea datelor. Pentru contracararea acestor riscuri se utilizează multiple mecanisme și strategii, cum sunt: ascunderea datelor, dispersarea datelor, standardizarea metodelor API, duplicarea datelor, copii de siguranță, degaussing, mecanisme avansate de monitorizare etc.

Criptarea este una dintre cele mai utilizate metode de ascundere a datelor și de asigurare a confidențialității în mediile cloud computing. Indiferent de algoritmii de criptare utilizați, asociată cu această tehnologie este problematica managementului cheilor de criptare, ea influențând radical nivelul de securitate oferit de sistem. Astfel, chiar dacă există implementate

metode avansate de criptare, datele pot fi compromise dacă mecanismele de management al cheilor de criptare sunt implementate necorespunzător.

Implementarea si utilizarea cheilor de criptare are o serie de condiționări datorate specificul mediului de lucru cloud computing. Conform raportului realizat de Institutul Național de Standarde și Tehnologii SUA (R. Chandramouli, 2013) tehnicile de management al cheilor în cloud trebuie să țină seama de particularitățile acestui mediu de lucru pentru identificarea potențialelor riscuri și stabilirea strategiilor adecvate de contracarare. Raportul mai evidențiază că acest domeniu este unul de interes maxim pentru furnizorii de soluții cloud, aceștia înțelegând importanța domeniului și încercând să pună la dispoziția beneficiarilor soluții adecvate.

Următoarele sunt principii care stau la baza dezvoltării soluțiilor de management al cheilor de criptare:

a) Strategia de implementare - se referă la tehnica prin care serviciul de management al cheilor este pus la dispoziția clientului.

Astfel, una dintre strategii este ca această capabilitate să fie integrată de către furnizor alături de celelalte servicii oferite către beneficiar. Deși este o soluție simplă, flexibilă, ușor de implementat și cu impact minim asupra proceselor organizaționale strategia prezintă riscul de a pune în același loc datele și cheile de criptare deopotrivă. Majoritatea furnizorilor de pe piață oferă astfel de servicii (ex. AWS Key Management Service Google Cloud Key Management Service, Microsoft Azure Key Vault, IBM Cloud Key Protect) și pot constitui o alternativă de criptare a datelor, cu costuri scăzute, mai ales când sensibilitatea acestora nu este ridicată.

O a doua soluție este achiziționarea serviciilor de management al cheilor de criptare de la o terță entitate. O astfel de strategie elimină riscurile asociate strategiei anterior prezentate dar are dezavantaje în ceea ce privește costurile suplimentare, creșterea complexității operațiunilor de administrare, scăderea flexibilității, dificultăți de integrare, limitarea posibilităților de partajare a resurselor, îngreunarea muncii colaborative, probleme de guvernanță, dificultăți în identificarea și remedierea defecțiunilor, complexități în atribuirea responsabilității etc.

A treia soluție este aceea a implementării unui sistem de management al cheilor utilizând resurse informatice aflate sub controlul direct al organizației, implementată fie într-o locație internă, fie pe o platformă de tip IaaS la un alt furnizor. Această soluție oferă avantajul separării datelor criptare față de cheile de criptare, dar vine cu limitări în ceea ce privește investițiile pe care organizația trebuie să le facă în resurse dedicate acestui proces, achiziționarea de licențe software, asigurarea pregătirii de specialitate a echipei de mentenanță, limitarea lucrului colaborativ, creșterea traficului datorită necesității ca datele să fie descărcate, decriptate, procesate, recriptate și încărcate înapoi în cloud. Opțiunea de încărcare a cheilor de criptare în cloud și apoi de efectuare a tuturor operațiunilor în cadrul acestuia este una care prezintă un risc maxim de compromitere a datelor și cheilor deopotrivă.

b) Controlul dual – se referă la stabilirea cadrului organizatoric și funcțional care să nu permită controlul cheilor de criptare, doar de către o singură persoană. Crearea, distribuirea și stabilirea accesului la resurse trebuie să necesite colaborarea a cel puțin două entități pentru ducerea la sfârșit a sarcinii. Entitățile pot fi persoane fizice sau aplicații software care se augmentează reciproc în vederea eliminării punctelor unice de compromitere.

c) Separarea atribuțiilor – face referire la stabilirea clară a atribuțiilor fiecărei entități implicată în procesul de management al securității datelor. Astfel, entitățile care asigură managementul cheilor de criptare nu trebuie să aibă acces la datele criptate și nici viceversa.

2.5.4.1 Confidențialitatea datelor

O condiție de bază din cadrul modelului CIA, care trebuie asigurată pentru crearea unui mediu sigur de prelucrare a datelor este confidențialitatea datelor. Ea poate fi definită ca fiind caracteristica datelor de a fi accesibile doar unor entități autorizate nefiind posibilă divulgarea, intenționată sau nu, către alte entități (Cleveland, 2008). Această caracteristică este una care, datorită particularităților sistemelor cloud computing, necesită abordări diferite față de cele specifice mediilor clasice.

Fig. 2.6 Schema dispunerii centrelor de date pentru principalii trei furnizori: Amazon Web Services (portocaliu), Microsoft Azure (albastru) și Google Cloud Platform (roșu)
Sursa: https://www.infoworld.com/article/3008617/

Pentru asigurarea accesului rapid la date și pentru motive de reziliență, în cadrul platformelor cloud datele sunt distribuite în mai multe copii, în mai multe locații la nivel global. Acest model de distribuire a datelor ridică probleme legate de cadrul legislativ care stabilește guvernanța datelor privind stocarea, transferul prin diferite jurisdicții, expunerea lor la diferiți factori dar și de manipularea a datelor cu niveluri diferite de sensibilitate în același cadrul tactic, operațional și strategic.

2.5.4.2 Integritatea datelor

Asigurarea integrității datelor se referă la crearea cadrului necesar, astfel încât modificarea datelor să fie efectuată doar de persoane autorizate. Această caracteristică se realizează în principal prin implementarea, la nivelul sistemului de prelucrare a datelor, a unor mecanisme de control al accesului. Managementul accesului și drepturilor la anumite resurse asigură că utilizarea datelor și a serviciilor este făcută doar de către utilizatori legitimi, nu este abuzată, nu este utilizată greșit, iar datele nu sunt compromise.

Integritatea datelor este un proces relativ ușor de realizat în sisteme simple, izolate, cu acces limitat, dar mult mai dificilă de atins o dată cu creșterea complexității sistemelor, cum este cazul cloud computing-ului. Ea necesită implementarea unor mecanisme ample de configurare a accesului și de monitorizare a integrități datelor. Coruperea poate apărea în orice stadiu al acestora, datorită unor cauze legitime (erori de transmisie, erori de procesare, alterare neintenționată etc.) sau ilegitime, cazuri în care o entitate rău intenționată dorește alterarea datelor în scopul pierderii valorii acestora.

Datorită specificului platformelor cloud computing de a utiliza echipamente și medii de comunicații cu nivel redus de încredere, integritatea datelor este un parametru care necesită considerații mai ample față de mediile clasice. Pentru rezolvarea acestor probleme s-au propus mai multe scheme și modele de securitate, cum ar fi: (Miller, 2010) (Ashley Chonka, 2011) (A. Oprea, 2005). Aceste modele de protocoale încearcă să rezolve problemele integrității datelor prin implementarea unor mecanisme pentru: auditarea datelor, verificarea stării, justificarea recuperabilității datelor - proof of retrievability, creșterea eficienței proceselor etc.

2.5.4.3 Disponibilitatea datelor

Trecută uneori cu vederea, capacitatea de a accesa la momentul dorit datele, sau disponibilitatea datelor, este cea de a treia trăsătură de bază a unui mediu de securitate. Ea întruchipează dezideratul cloud computing-ului de a furniza servicii oriunde și oricând. Din

perspectiva furnizorului de servicii, atingerea acestui deziderat este un element critic al modelului de afacere pe care îl desfășoară.

Construirea unui sistem care să răspundă acestor nevoi necesită investiții de amploare în sisteme complexe care să facă față nevoii crescute de resurse informatice din punct de vedere cantitativ și calitativ. Pentru realizarea acestui lucru nu este suficientă doar implementarea unor sisteme redundante într-un centru de date, ci sunt necesare duplicări ale datelor în centre de stocare specializate. Acestea trebuie distribuite la nivel global și interconectate cu linii de date de mare viteză.

Păstrarea datelor pe platforme aparținând unor alte entități și dependența de serviciile oferite de acestea sporește riscul ca datele să nu fie disponibile la momentul potrivit, ceea ce poate avea un impact considerabil asupra atingerii obiectivelor organizației. În figura 2.11 este prezentată situația întreruperilor serviciilor cloud pentru trei dintre principalii furnizori de servicii cloud pentru anii 2015, 2016 și 2017.

2.5.5 Segregarea datelor

Segregarea poate fi definită ca fiind capacitatea unui sistem informațional de a izola datele unele de altele, în funcție de anumiți parametri (tip, proprietar, rol etc.). Pentru realizarea acestui lucru se poate utiliza o gamă largă de instrumente de control al stocării, procesării, filtrării accesului, segmentării sistemelor etc. Deși nu face parte din modelul CIA (Panmore Institute, 2016) de asigurare a securității datelor, totuși segregarea datelor poate fi considerată ca o caracteristică importantă a unui mediu de prelucrare a informațiilor, mai ales cele bazate pe punerea în comun a resurselor, cum este cazul tehnologiei cloud computing.

Utilizarea în comun, de către toți beneficiarii, a resurselor informatice disponibile pe platformele cloud determină utilizarea acelorași echipamente hardware pentru procesarea, stocarea și transferul datelor. Din punct de vedere al securității datelor, utilizarea aceluiași mediu pentru prelucrarea informațiilor de către entități diferite constituie un risc de securitate și trebuie tratat corespunzător prin mecanisme de izolare a resurselor și de control al accesului. Asigurarea unei segregări slabe a datelor crește riscul executării unor atacuri informatice având ca sursă datele unui alt client.

Oferirea capabilităților de segregare a datelor este o caracteristică aflată sub controlul furnizorului de servicii iar utilizatorul nu are instrumente pentru a monitoriza sau modifica parametri. Criptarea datelor este una dintre măsurile cele mai frecvente, aflate la îndemâna beneficiarului pentru a minimiza acest risc, însă nu poate fi considerată ca o măsură utilizabilă în toate situațiile. Există cazuri în care acest lucru nu este posibil datorită incompatibilităților la nivel operațional cu alte aplicații, complexității induse în mediul organizațional sau cerințelor datorate lucrului colaborativ. Se impune așadar utilizarea unor mecanisme adiționale pentru separarea accesului la date și izolarea lor. Utilizarea mai multor măsuri, din spectre diferite, permite păstrarea segregării datelor și limitarea răspândirii compromiterii acestora, chiar dacă una dintre soluții este indisponibilă sau anulată prin diferite mecanisme de către utilizatori rău intenționați.

2.5.6 Standardizarea

Furnizorii de produse și servicii din categoria tehnologiei informației clasice sunt supuși auditărilor și certificărilor de securitate, activitate care este standardizată și a atins un nivel de maturitate ridicat. La fel ca și în mediul clasic și în domeniul cloud computing sunt necesare o serie de standarde și certificări care trebuie îndeplinite de furnizorii de servicii. Totuși, din cauza domeniului relativ nou, extrem de complex, standardelor apărute până în prezent încă le lipsește consistența, maturitatea, validarea și recunoașterea unanimă a industriei.

Interesul extrem de ridicat pe care îl manifestă o mulțime de entități față de acest domeniu și lipsa de standarde unanim acceptate a determinat ca multiple organizații precum National Institute of Standards and Technology, Institute of Electrical and Electronics Engineers Standards Association, International Telecommunication Union, Cloud Security Alliance,

European Union Agency for Network and Information Security etc. să creeze grupuri de lucru pentru a rezolva această problemă. Acest tip de abordare descentralizată a dus la apariția unui număr mare de standarde, fiecare dintre ele punând accentul pe o anumită latură, în funcție de domeniul de interes al organizației care l-a dezvoltat.

Acreditarea de securitate pentru un furnizor de servicii cloud trebuie să acopere mai multe aspecte: tehnologic, operațional, personal, confidențialitate, integritate, disponibilitate, securitate fizică, redundanță etc. Pe partea de personal, organizații precum Cloud Security Alliance, SANS Institute, Information Security Professionals3 etc. au dezvoltat certificări și cursuri de pregătire formale pentru specialiștii în securitate. Acest tip de certificări cuprinde aspecte legate de protejarea rețelelor, testarea penetrabilității, modalități de răspuns la incidente, investigarea infracțiunilor informatice, auditare etc. Din punct de vedere operațional, familia de standarde ISO 27000 conține elemente care ajută organizațiile să asigure securizarea resurselor, dintre acestea standardul ISO 27001 fiind recunoscut ca unul dintre cele mai complete din domeniul managementului securității în mediile informatice.

2.5.7 Transferul datelor

Datele în tranzit sau în mișcare sunt acele date care se află în transfer dintr-o locație în alta utilizând medii de comunicație private sau publice. Protecția datelor în mișcare se referă la implementarea unui set de măsuri prin care să se asigure securitatea acestora pe parcursul transferului. Liniile de comunicație sunt un element esențial al mediilor de lucru cloud computing, întrucât sunt utilizate pentru livrarea/accesarea serviciilor, iar asigurarea securității datelor în cadrul acestora este un element critic pentru securitatea întregului sistem. Pe de altă parte, aceste medii sunt în afara perimetrului organizației, se află sub controlul altor organizații, existând un risc considerabil de compromitere a acestora.

Dintre riscurile asociate transferului de date se pot aminti:

- Blocarea parțială sau totală a accesului clientului la platforma furnizorului;
- Incapacitatea canalelor de comunicație de a face față volumului de date;
- Copierea datelor și extragerea informațiilor;
- Alterarea conținutului;
- Redirecționarea traficului.

Criptarea este una dintre cele mai folosite tehnici de protecție a datelor în mișcare, fiind utilizată pentru limitarea accesului neautorizat la date. Numeroase protocoale (HTTPS, SSL, TLS, FTPS etc.) implementează algoritmi de criptare optimizați pentru transferul datelor. Totuși, ea trebuie să fie complementată de o serie de măsuri, care să acopere lipsurile acesteia.

În vederea minimizării riscului de indisponibilitate a serviciilor este necesară calibrarea acestora în funcție de nevoile clientului. De asemenea, este recomandată asigurarea unor legături redundante care să preia parțial sau integral traficul atunci când legăturile principale nu fac față. Limitarea accesului fizic la echipamentele și liniile de comunicații, precum și validarea personalului care execută managementul acestora este necesară pentru limitarea riscului de compromitere.

2.5.8 Managementul actualizărilor de securitate

Adaptabilitatea și diversitatea tehnologiei cloud computing poate uneori fi considerată și un dezavantaj. Astfel, datorită multiplelor modele sub care aceste servicii pot fi oferite poate provoca confuzie și neînțelegere privind responsabilitățile care le revin părților implicate în domeniul aplicării actualizărilor de securitate.

O latură specială a acestui proces este posibilitatea automatizării sistemului de instalare a actualizărilor de securitate. O astfel de capabilitate îmbunătățește capacitatea sistemului de acoperire a breșelor de securitate și, prin scăderea timpului de reacție, minimizează timpul de vulnerabilitate la atacuri.

În studiul privind investigarea breșelor de securitate efectuat de (Verizon, 2016) s-a observat că 90% din incidentele de securitate au exploatat vulnerabilități pentru care existau

actualizări de securitate vechi de cel puțin 6 luni. Organizațiile care adoptă tehnologiile cloud computing sunt supuse riscului de neînțelegere sau înțelegere greșită a drepturilor, dar mai ales a responsabilităților pe care le au. Neîndeplinirea acestor obligații poate duce la exploatarea unor vulnerabilități și compromiterea securității datelor lor sau a altor consumatori ai serviciilor acelei platforme.

2.5.9 Acordul de furnizare a serviciilor

Un acord de furnizare a serviciilor este de obicei o înțelegere între două părți, furnizor și cumpărător, având ca scop definirea unui nivel clar de așteptări cu privire la serviciile care vor fi utilizate.

Orientarea pe servicii a mediului cloud computing crește importanța acestui acord între furnizor și beneficiar, el conținând stipulări privind cantitatea și calitatea serviciilor, precum și a tuturor elementelor adiționale respectivei înțelegeri. Asigurarea securității datelor în serviciile oferite trebuie tratată corespunzător, pentru crearea unui cadru de înțelegere mutuală privind drepturile și responsabilitățile ce le revin celor două părți implicate, dar și a penalităților care se vor suporta dacă termenii înțelegerii nu sunt respectați.

Întrucât securitatea mediului cloud computing este rezultatul conlucrării între furnizor și beneficiar, acordul trebuie să stabilească un nivel de asigurare a serviciilor în temeni de: cantitate, calitate, disponibilitate, redundanță, securitate, auditare etc.

2.5.10 Interoperabilitate

Interoperabilitatea reprezintă capacitatea a două sau mai multe sisteme de a conlucra unul cu celălalt pentru atingerea unui scop. Fiecare dintre soluțiile cloud existente pe piață în momentul de față are anumite elemente care le diferențiază de cele ale competitorilor. Deși sunt utile pentru că răspund mai bine necesităților fiecăruia dintre consumatori, diferențele pot duce la blocarea utilizatorilor într-o anumită platformă și imposibilitatea acestora de a-și migra complet datele către alte platforme.

Prin blocarea capacității unui utilizator de a alege dintre alternativele tehnologice existente se limitează capacitatea acestuia de a-și eficientiza activitatea. Acest blocaj are impact și asupra asigurării securității datelor prelucrate în sistem și limitează opțiunile beneficiarului în procesul de alegere a instrumentelor de îmbunătățire a gradului de confidențialitate, integritate sau disponibilitate a resurselor. Din perspectiva securizării datelor, problema blocării într-o anumită platformă - platform lock-in limitează opțiunile echipei responsabile de securizarea datelor. Imposibilitatea migrării datelor între sisteme sau de a integra sisteme oferite de terțe părți în configurațiile actuale nu permite utilizarea altor instrumente de securizare a datelor în afara celor oferite de furnizorul de servicii cloud.

2.6 Concluzii

Modelul cloud computing aduce în spectrul domeniului tehnologiei informației un nou model arhitectural de utilizare a resurselor informaționale în care optimizarea utilizării acestora este un element cheie. Modelul se bazează pe o centralizare a resurselor hardware concomitent cu o distribuire a utilizării și a responsabilităților de management. Acest nou model de utilizare a tehnologiei modifică spectrul riscurilor privind compromiterea informațiilor. Noua paradigmă de manipulare a datelor necesită abordări noi privind managementul riscurilor de securitate care să țină cont de particularitățile acestui sistem.

Cloud computing-ul este o tehnologie care oferă foarte multe avantaje pentru următoarea generație de aplicații din domeniul tehnologiei informației. Mediul modern de activitate în care operează organizațiile actuale este strict condiționat de indicatori de eficiență și eficacitate, tehnologia cloud computing putând oferi avantaje competitive în ceea ce privește minimizarea costurilor, minimizarea investițiilor CAPEX sau prelucrarea și oferirea rapidă de informații către decidenți pentru a-i ajuta în luarea deciziilor.

Cu toate acestea, există în momentul de față o serie de bariere care limitează expansiunea și adopția acesteia, dintre care cele mai importante sunt cele legate de realizarea securității datelor. Cloud computing-ul mută datele organizațiilor în centre mari de date externalizate, care au un nivel redus de încredere. Noul cadru de utilizare a resurselor de tehnologia informațiilor și de manipulare a datelor creează noi riscuri de securitate care trebuie avute în vedere de către specialiștii în securitatea datelor. Avantajele economice ale migrării către platformele cloud computing trebuie atent cântărite în comparație cu riscurile compromiterii datelor, înainte de a angaja organizația pe această cale.

3. Strategia de protecție a datelor în platformele cloud computing

3.1 Importanța securizării informației

Mediul în care performează organizațiile moderne este bazat într-o foarte mare măsură pe informație și implicit pe elemente de tehnologia procesării acesteia. Datorită beneficiilor pe care tehnologia informațională le aduce, asistăm la o integrare din ce în ce mai profundă a acestor elemente la nivelul celorlaltor componente ale unei organizații, fapt care face ca aceste elemente să influențeze direct desfășurarea proceselor organizaționale, dar mai ales eficiența lor. Organizațiile care înțeleg avantajele utilizării tehnologiei în procesul de prelucrare a datelor și care decid să folosească oportunitățile oferite de aceasta au șanse sporite să beneficieze de atuuri concurențiale și să obțină superioritate față de alți actori similari.

Tehnologiile moderne pot oferi avantaje deosebite organizațiilor care le adoptă dar, datorită imaturității acestora, vin împreună cu riscuri de multe ori necunoscute. Mecanismele de protecție a datelor sunt elemente care necesită investiții în resurse, personal și modificări în procesele organizației, necesitând costuri crescătoare, proporțional cu dimensiunea și dinamica organizației. De multe ori, ele sunt privite cu reticență ca fiind investiții care necesită costuri, fără a aduce beneficii organizației. Mai mult, ele induc limitări în sistem datorită impactului negativ pe care îl pot avea asupra eficienței proceselor organizaționale desfășurate la nivelul organizației.

Spectrul strategiilor utilizate de organizații pentru securizarea resurselor informaționale este limitat, remarcându-se utilizarea cu predilecție a următoarelor strategii: „securitate prin niveluri” și „apărare în adâncime”. Există numeroase instrumentele tactice și operaționale comune între cele două, unii cercetători considerându-le chiar ca fiind una și aceeași strategie (Shenk, 2013), însă există elemente de bază care le diferențiază, precum complexitatea și filozofia de abordare a amenințărilor.

3.2 Securitate prin niveluri

Strategia „securitate prin niveluri”, denumită și „apărare pe niveluri” presupune combinarea mai multor mecanisme de securitate pentru protejarea unor date sau sisteme informatice (Craggs, 2017). Ideea de bază a conceptului este aceea că nu există un instrument perfect de protecție, dar că prin utilizarea unui set de instrumente, minusurile unora pot fi acoperite de celelalte. Tehnologii precum firewall-ul, antivirusul, filtrarea e-mail, criptarea datelor, update-urile de securitate pot fiecare individual să protejeze resursele într-un fel în care celelalte nu sunt în stare. Un antivirus poate opri un cod distrugător să ruleze pe stația gazdă, dar nu poate opri un atac de tip “heartblead” de compromitere a protocolului de comunicație SSL sau “VLAN hopping” de evadare a pachetelor din VLAN-ul asignat.

3.3 Apărarea în adâncime

„Apărarea în adâncime” este, în momentul de față, cea mai utilizată strategie pentru protecția resurselor informatice ale unei organizații. Ea presupune dispunerea mai multor mecanisme defensive complementare, cu rolul de a opri un atacator, chiar dacă unele dintre ele sunt penetrate (figura 3.2).

Strategia, numită și „abordarea castelului” și-a dovedit validitatea în mediul militar clasic, fiind importată și adaptată la specificul mediului informațional. Ea are la bază filosofia conform căreia nu este posibil să se realizeze protecția totală, completă a unui sistem, indiferent de colecția de măsuri de securitate adoptate.

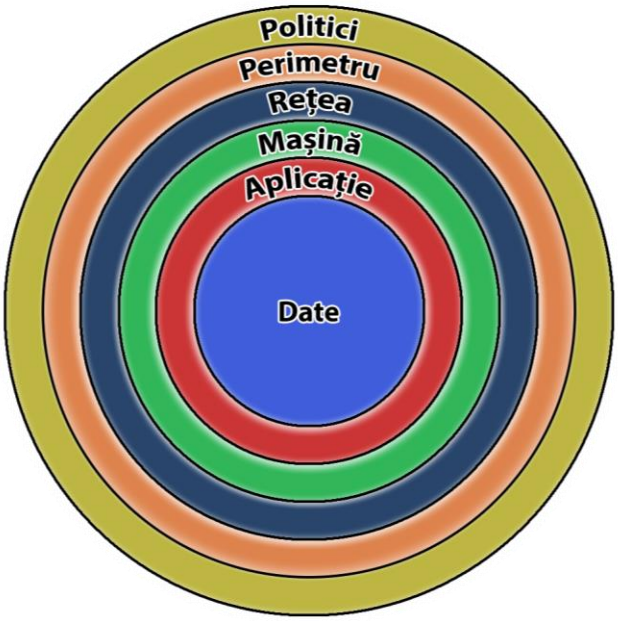

Fig. 3.2 Schema modelului „apărare în adâncime”

Se consideră astfel că, dacă un atacator are suficient timp la dispoziție, acesta va reuși într-un final să depășească mecanismele de protecție ale apărătorului. Este necesară utilizarea mai multor bariere de protecție dispuse pe toate căile posibile de penetrare, cu rolul de a obstrucționa acțiunile atacatorului, a-i zădărnici eforturile, a-i consuma resursele, a-i scădea viteza de atac și de a crea timpul necesar apărătorilor pentru organizarea defensivă până în punctul în care atacatorul este nevoit să renunțe la atac.

Strategia consideră resursele din perimetrul controlat ca unele de încredere și pune un accent deosebit pe monitorizarea perimetrului și a căilor de comunicație cu exteriorul, pentru identificarea cât mai rapidă a unui atac și punerea în aplicare a procedurilor de reacție. Strategia consideră că datele organizației, în toate formele sale, sunt procesate utilizând echipamente cu nivel ridicat de încredere, care se află sub controlul organizației, fiind dispuse într-un mediu sigur, accesul la acest mediu fiind extrem de bine controlat. Transferul datelor către alte entități necesită respectarea unor proceduri complexe, care se bazează pe analizarea nivelului de importanță a datelor. În funcție de acest nivel se alege formatul sub care vor fi transmise și canalul de comunicație care urmează a fi folosit.

Arealul de prelucrare a datelor este împărțit în trei zone:

a) *Zona internă* – este formată din ansamblul activelor unei organizații care se află sunt sub strictul ei control. De obicei este delimitată perimetral de un sistem de mecanisme de izolare, resursele din interiorul acestuia fiind considerate ca având un nivel înalt de încredere.

La nivelul punctului de intrare în zonă există mecanisme complexe de monitorizare și filtrare a traficului, de cele mai multe ori sub forma unor firewall-uri și a sistemelor de prevenire a intruziunilor.

b) *Zona demilitarizată (demilitarized zone - DMZ)* este o zonă în care sunt dispuse echipamente care oferă servicii unor beneficiari atât din interiorul cât și din exteriorul organizației. În această zonă se dispun de obicei servere de tipul – mail, web, FTP, DNS, RADIUS etc. Sisteme de tipul firewall sunt dispuse la punctul de legătură între DMZ și zona internă, permițând doar o conectivitate limitată cu aceste sisteme. Similar acestora există sisteme tip firewall care filtrează posibilitățile de comunicație cu sistemele din zona externă, făcând din zona DMZ o zonă cu un nivel mai ridicat de siguranță față de zona externă.

c) *Zona externă* – este zona care se află în afara controlului organizației, dispusă în exteriorul perimetrului acesteia. Această zonă este de cele mai multe ori asimilată cu zona Internet-ului. Echipamentele și canalele de comunicație din această zonă se află sub administrarea unor alte entități, organizației fiindu-i oferite capabilități de comunicație, de cele mai multe ori sub formă de servicii..

Strategia încearcă să micșoreze șansele de compromitere a datelor cauzate de acțiunile unui atacator sau datorate erorilor de manipulare. Pentru acesta strategia utilizează numeroase

mecanisme de protecție pentru securizarea infrastructurii informaționale a unei organizații, care pot fi împărțite în următoarele categorii principale:

a) Protecția fizică – se referă la dezvoltarea și implementarea unui set de măsuri de limitare a accesul fizic la elementele componente ale arhitecturii rețelei. Deopotrivă, este limitat atât accesul la locațiile de dispunere a serverelor, la liniile de cablu, la mediul wireless, la echipamentele de rețelistică, cât și la terminale. Doar persoanele autorizate și validate de organizație pot avea acces la aceste echipamentele, fiecare în conformitate cu atribuțiile care le revin. Instrumente fizice utilizate pentru implementarea acestui aspect sunt: porți, garduri, bariere și uși cu acces controlat, dulapuri cu chei în care sunt dispuse echipamentele, mecanisme de protecție a liniilor de cablu, poziționarea echipamentelor Wi-Fi astfel încât raza de acoperire a rețelelor să nu depășească spațiile controlate, carcase cu protecție pentru echipamente, containere securizate pentru depozitarea mediilor de stocare, proceduri pentru disponibilizarea echipamentelor etc.

b) Protecția personalului – presupune ansamblul de proceduri și măsuri de verificare și validare a personalului care au ca scop asigurarea accesului la resursele informaționale ale unei organizații, în funcție de rolul pe care îl au în organizație. Astfel de proceduri presupun verificări ale personalului la intrarea în organizație, la anumite intervale de timp precum și ori de câte ori există suspiciuni cu privire la integritatea sau loialitatea acestora. Cu cât persoana este pe o poziție mai înaltă în ierarhia organizației, cu atât este mai probabil că va utiliza informații cu nivel ridicat de importanță și deci este necesară asigurarea unui nivel cât mai ridicat a loialității acesteia.

Mecanismele de management al accesului la resurse, stabilite la nivel intern, filtrează drepturile utilizatorilor de a accesa resursele organizației. Unul dintre principiile de bază este cel al "necesității de a cunoaște" prin care drepturile de acces implementate permit accesul utilizatorilor la resursele informaționale numai dacă aceștia au nevoie de respectivele resurse pentru desfășurarea activității.

c) Protecția lanțului de aprovizionare – se referă la luarea măsurilor pentru asigurarea conformității între produsele și serviciile achiziționate și standardele de securitate ale organizației. Utilizarea programelor de achiziție în care prețul cel mai mic este criteriul de bază nu este întotdeauna cea mai eficientă metodă de achiziție, mai ales atunci când se are în vedere securitatea sistemelor. Instrumente, care aparent pot realiza aceleași funcționalități, pot avea limitări de operaționalitate, pot fi inserate vulnerabilități hardware/software astfel încât funcționalitatea acestora este limitată sau pot fi exploatate de atacatori pentru compromiterea sistemelor din care fac parte (Electronic Resellers Association International - ERAI, 2017).

d) Protecția Informatică - este reprezentată de totalitatea mecanismelor, procedurilor și instrumentelor hardware și software care asigură protecția datelor în sistemele informatice. Implementarea mecanismelor de securitate la nivelul sistemelor informatice de calcul necesită integrarea a numeroase instrumente din mai multe categorii: securizarea resurselor, controlul accesului, monitorizarea utilizării resurselor, asigurarea confidențialității, integrității și disponibilității resurselor, auditarea serviciilor, disponibilizarea sigură a echipamentelor, securitatea transferurilor de date, răspunsul în caz de incidente etc.

3.4 Provocări de securitate specifice mediului tehnologic actual

Evoluția pe care a avut-o cloud computing-ului în ultima decadă a constituit baza dezvoltării a numeroase alte tehnologii, cum ar fi: internetul lucrurilor, big data, rețele definite prin software etc și a determinat modificarea profundă a mediului tehnologic tradițional. Capabilitățile oferite de aceste tehnologii (mobilitate ridicată, orientarea pe servicii, transferul rapid a unor cantități mari de date, prelucrarea rapidă a acestora, acces rapid la resurse aflate la distanță, fiabilitate crescută, costuri optimizate, creșterea eficienței proceselor etc.) au fost apreciate de organizații, determinând o creștere a ratei de absorbție și propulsând și mai mult eforturile în cercetarea și dezvoltare. În egală măsură tehnologiile au atras și atenția infractorilor

cibernetici care au dovedit o adaptabilitate sporită, încercând permanent noi metode de a specula vulnerabilitățile acestor tehnologii încă imature pentru a obține acces la informațiile prelucrate.

3.4.1 Tehnologia ca serviciu

Acest concept reprezintă un nou model de utilizare a tehnologiei bazat pe flexibilitate înaltă, agilitate avansată, elasticitate ridicată, minimizarea costurilor, acces rapid la date, redundanță sporită etc. Nou paradigmă de prelucrare a datelor aduce o serie de avantaje care suscită interesul organizațiilor și persoanelor fizice. Totuși, acest nou cadru modifică spectrul clasic al amenințărilor de securitate, alterându-le pe de o parte pe cele clasice și introducând noi elemente de risc, pe de altă parte. Principiile noii paradigme nu mai sunt în conformitate cu principiile de bază ale strategiei "apărare în adâncime" folosită atâția ani de organizații pentru securizarea activelor. Elementele componentele are sistemului informațional, dar mai ales datele nu se mai regăsesc în interiorul perimetrului organizației, sub controlul direct al acesteia, ci sunt stocate, procesate și transmise utilizând echipamente supervizate de alte entități. Acest model de utilizare a resurselor informaționale prezintă o serie de riscuri specifice.

Calitățile de bază ale tehnologiei precum flexibilitatea, scalabilitatea, adaptabilitatea permit crearea de medii de lucru avansate care combină tehnologii clasice cu cele cloud. Aceste avantaje pot fi suprimate de imposibilitatea asigurării unui mediu de securitate corespunzător, cauzată chiar complexitatea configurațiilor care pot fi create – „complexitatea este inamicul securității" (Schneier, 2008).

3.4.2 Internetul obiectelor - *Internet of Things*

Capacitatea de a interconecta, comunica și administra de la distanță un număr nelimitat de dispozitive automatizate, utilizând de cele mai multe ori Internetul, a devenit un element prezent atât în mediul organizațional actual, cât și la nivel de uz individual.

Avantajele utilizării acestei tehnologii determină ca securizarea capabilităților oferite să se constituie ca un efort de importanță maximă. Obiectele sunt dispuse în locații nesecurizate în afara perimetrelor organizaționale, iar transferul datelor se execută utilizând canale de comunicație care nu sunt de încredere. În aceste condiții, există un risc ridicat ca agenți rău intenționați să desfășoare acțiuni împotriva terminalelor, cu scopul de a prelua controlul acestora sau a liniilor de comunicație, de a altera funcționarea acestora și de a bloca sau altera conținutul datelor comunicate (H.Weber, 2010). Este necesar ca echipamentele să poată diferenția între sarcinile autentice sau falsificate și să decidă dacă să execute sau nu o anumită sarcină.

Strategia "apărare în adâncime" necesită implementarea unei multitudini de mecanisme suprapuse, bazate pe proceduri operaționale și instrumente de autentificare, limitare a accesului, criptare, auditare etc. Ea necesită un control al locației echipamentelor și al liniilor de comunicație, precum și resurse consistente pentru asigurarea funcționării eficiente a instrumentelor de securizare a datelor. Date fiind particularitățile tehnologiei „internetul obiectelor" multe dintre acestea sunt imposibil de implementat sau sunt nepractice, deoarece necesită alocări de resurse considerabile.

3.4.3 Cantități mari de date - *Big Data*

Big Data este un concept care descrie prelucrarea și stocarea unor cantități mari de date structurate și nestructurate care provin din interiorul organizației, dar mai ales din exteriorul acesteia (Seref Sagiroglu, 2013). Această cantitate mare de informație este generată de senzori, sisteme și persoane, din orice locație. Datorită importanței ridicate a acestor date pentru companii (Jonathan Levin, 2014) acestea încearcă, prin utilizarea de tehnologii și arhitecturi specifice, extragerea de valoare economică din datele colectate prin utilizarea de proceduri specifice de captare, transfer și analiză rapidă.

Sistemele clasice defensive nu sunt proiectate să proceseze cantități mari de date care vin într-un timp scurt pe canale de comunicație cu factor limitat de încredere, de la o multitudine de surse, multe dintre ele dispuse într-un mediu necontrolat (în afara perimetrului organizației).

Filozofia strategiei este aceea de a „încetini” acțiunile atacatorului și de a scădea ritmul de atac prin punerea de diverse bariere în fața agresorului. Acest mod de lucru este incompatibil cu tehnologia cantităților mari de date. Acestea au nevoie de transferul și prelucrarea rapidă a datelor, iar aplicarea procedurilor clasice de validare nu este posibilă, întrucât întârzierile introduse în sistem sunt incompatibile cu specificul acestora.

3.4.4 Modificarea profilului infractorului cibernetic

Dezvoltarea amplă pe care a avut-o mediul cibernetic a atras companiile și persoanele private în a exploata avantajele acestuia, ceea ce a determinat o creștere a influenței domeniului tehnologic pentru succesul activităților desfășurate. În egală măsură, potențialul noilor tehnologii, corelat cu importanța majoră pe care o are informația în lumea modernă a determinat și creșterea interesului persoanelor rău intenționate, care încearcă în mod ilegal să acceadă la informație sau să indisponibilizeze și corupă date și sisteme.

Generația actuală de infractori cibernetici este radical diferită de cea inițială. Mediul cibernetic actual este populat cu structuri și organizații criminale, cu forme de organizare complexe, independente sau sponsorizate parțial sau total de stat (Jan Kallberg, 2013) (Betz, 2017). Acestea au la dispoziție cantități considerabile de resurse materiale, financiare și de timp, precum și posibilitatea de a atrage inteligență și ”know-how” în cadrul lor.

Strategia „apărare în adâncime” a fost dezvoltată pentru a face față cu unor atacuri venite din partea unor actori cu resurse limitate care pot acționa într-un orizont de timp scurt. Modul de acțiune a apărătorilor vizează intrarea într-o stare critică, ce presupune luarea de măsuri defensive pentru blocarea acțiunilor desfășurate de agresor. Cu cât această stare critică este menținută o perioadă mai lungă de timp, cu atât organizația este forțată să-și utilizeze ineficient resursele prin alocarea acestora pentru activități care nu aduc profituri sau induc ineficiențe în procesele pe care le desfășoară.

3.4.5 Modificarea strategiilor de atac

Cantitățile considerabile de resurse care stau la dispoziția organizațiilor criminale informatice, precum și motivația diferită au determinat modificarea strategiilor și tacticilor folosite de aceștia pentru atingerea obiectivelor. Astfel, strategiile acestora sunt caracterizate de sofisticare, comercializare și organizare (Grabosky, 2014). Sofisticarea strategiilor cibernetice se referă la gradul crescut de complexitate a acțiunilor atât prin nivelul tehnologic utilizat, cât și prin numărul și amploarea acțiunilor desfășurate. Un aspect demn de menționat aici este utilizarea atacurilor cibernetice în combinație cu acțiunile de război clasic în vederea limitării capacităților defensive ale apărătorului și amplificării efectelor acțiunilor fizice (Marie Baezner, 2017).

Agresorul cibernetic modern nu urmărește obținerea rapidă de rezultate, iar în acest sens s-a constatat dezvoltarea strategiei „amenințare avansată persistentă - advanced persistent threat (APT)”. Strategia presupune utilizarea cu preponderență a unor tactici de tipul „ perturbare și distrugere - disruption and destruction” și ”decepție și mascare - deception and mimicry” (OGÎGĂU-NEAMȚIU F. M., 2018) care au un risc minim de detecție. Acțiunile sunt coordonate de la un punct de comandă din exterior și nu riscă compromiterea prin extragerea rapidă, brutală a tuturor datelor la care au acces, ci mai degrabă se încearcă păstrarea accesului la resursele compromise pentru o perioadă cât mai lungă de timp, răspândirea infectării și extragerea celor mai importante informații.

Un element important care este în mare parte trecut cu vederea de către strategia „apărare în adâncime” și al cărui rol în protejarea datelor infrastructurilor moderne este ridicat este factorul uman. Dezvoltarea rețelelor sociale, a nevoilor crescute de comunicare și lucru colaborativ a creat posibilitatea ca un atacator, cu instrumente adecvate, să poată aduna o multitudine de informații referitoare la personalul, echipamentul, politicile de protecție, arhitectura informațională a unei organizații fără ca măcar să execute vreo acțiune ofensivă împotriva dispozitivelor de protecție a acesteia.

3.4.6 IT ca bun de larg consum - *IT Consumerization*

Fenomenul *IT Consumerization* reprezintă manifestarea utilizării tehnologiei private pentru realizarea sarcinilor de serviciu. Dezvoltarea internetului și capabilitățile pe care le-a adus acesta, atât în mediul de afaceri cât și în viața oamenilor a determinat creșterea numărului de persoane care utilizează echipamentele personale pentru a efectua sarcini de serviciu în afara orelor de program sau din alte locații decât perimetrul organizației.

Una dintre cele mai semnificative tendințe este Bring Your Own Device (BYOD), care presupune utilizarea echipamentelor personale tip telefoanelor, tabletelor, laptopurilor sau a echipamentelor USB personale pentru prelucrarea datelor organizației.

Tendințele de suport sau eliminare a acestui fenomen sunt diverse și depind de specificul organizației. Unele organizații au atras astfel de tehnologii observând beneficiile costurilor reduse cu resursele și ale creșterii eficienței angajaților prin utilizarea unor echipamente care le sunt adaptate nevoilor și preferințelor lor. Pe de altă parte, echipele de securitate au încadrat acest fenomen în așa numitul „shadow IT" care include totalitatea harware-ului și software-ului din organizație care nu se află sub controlul lor și care reprezintă un factor de risc al securității datelor.

Aceste avantaje ridică provocări considerabile strategiei „apărare în adâncime", care trebuie să acomodeze și administreze echipamente cu grad limitat de încredere pentru prelucrarea datelor organizației. Strategia clasică pleacă de la premisa că echipamentele organizației se regăsesc cu preponderență în interiorul perimetrului, iar traficul de date cu entități externe se realizează doar în circumstanțe speciale.

3.4.7 Rețele definite software - *Software Defined Networks*

Cerințele mediului IT modern, caracterizate prin capabilități avansate în domeniu precum agilitate, viteză și flexibilitate au fost tratate la nivel de server, prin crearea de medii virtualizate care răspund rapid nevoilor organizaționale. Apariția și dezvoltarea conceptului de rețele definite software este o inițiativă care dorește alinierea infrastructurii de distribuție a datelor, la noile cerințe, prin înlocuirea echipamentului fizic de rețelistică cu aplicații și controlere software.

În această paradigmă, prin utilizarea unor tehnologii cheie precum virtualizarea rețelei, automatizarea prin programare, separarea funcțională un administrator de rețea poate realiza redirecționarea fluxurilor de date dintr-un punct central de management, fără a fi necesar să reconfigureze fizic echipamentele. Poate de asemenea să redistribuie serviciile dintr-o rețea în funcție de locația unde sunt necesare indiferent de echipamentele la care sunt conectate serverele care oferă respectivele servicii.

Pe lângă avantajele oferite, noua tehnologie aduce și noi riscuri de securitate care provoacă capabilitățile mecanismelor defensive utilizate de strategia „apărare în adâncime". În viziunea acestei strategii, principalele echipamente de rețea care au și rol de protecție a datelor (firewall, router, switch) sunt protejate, pe lângă mecanisme software și de o serie complexă de mecanisme și politici care permit accesul la configurația acestora doar a persoanelor autorizate. Deși dispun de instrumente de administrare de la distanță, inițializarea și programarea de bază a acestora se poate desfășura doar din anumite spații controlate, limitându-se astfel posibilitățile de compromitere. Aceste echipamente reprezintă piloni de securitate pe care se bazează strategia de protecție a datelor și, deși limitează unele dintre capabilitățile dinamice ale rețelei, ele conferă avantaje în domeniul securității.

Tehnologia rețelelor programabile, prin capabilitățile de reprogramare de la distanță crește riscul ca resursele rețelistice ale unei organizații să fie compromise prin exploatarea unor astfel de echipamente. Accesul fizic nu mai este necesar, deci măsurile de ordin fizic de limitare a accesului au aplicabilitate redusă. Cresc astfel riscurile ca un atacator să eludeze mecanismele defensive și să transfere cod nociv sau chiar să preia controlul dispozitivului și să-l transforme dintr-un puternic pilon al apărării într-un vector de atac.

3.5 Studiu de caz

Provocările tehnologiilor moderne asupra strategiilor de apărare au fost analizate în cadrul unei cercetări desfășurate în cadrul Institutului de Cercetare-Dezvoltare al Universității Transilvania din Brașov, în perioada 2014-2016 având ca obiectiv îmbunătățirea nivelului de securitate a mediului informațional din cadrul acestuia.

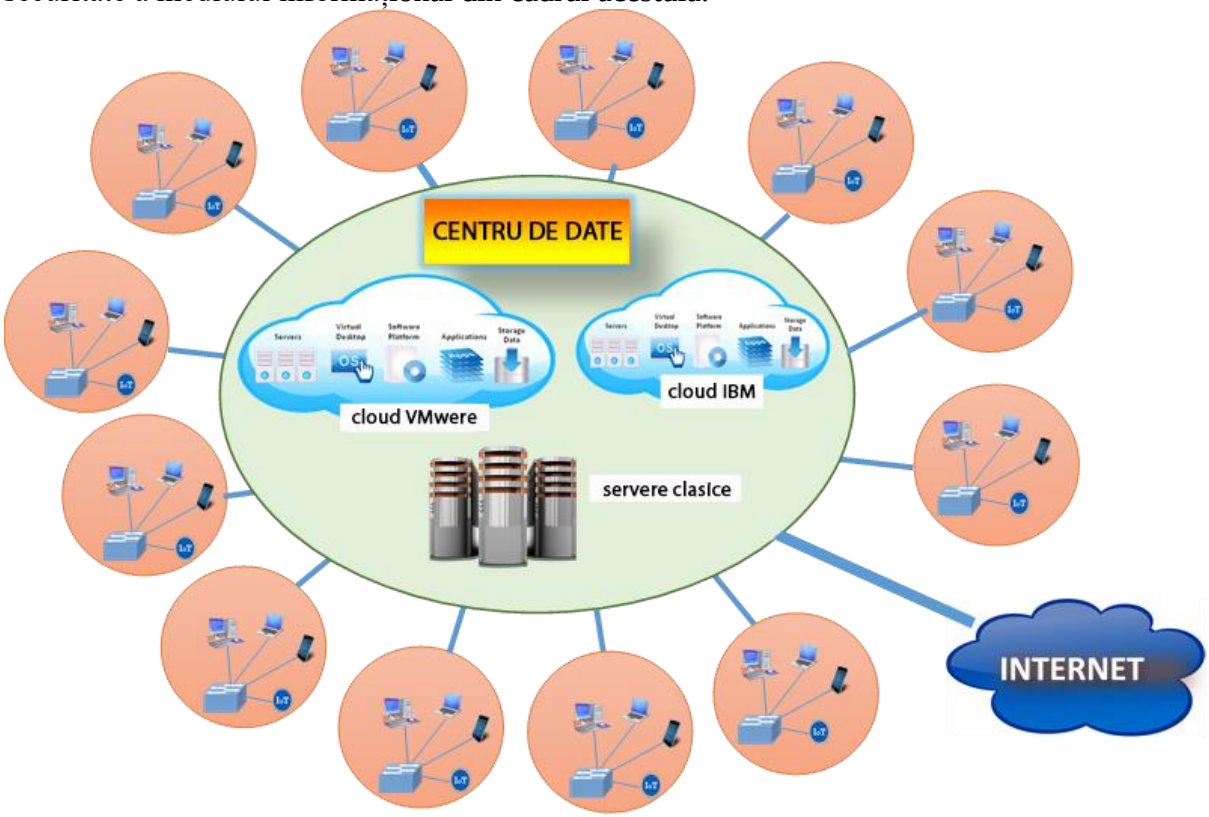

Fig. 3.9 Schema arhitecturii informaționale din cadrul
Institutului de Cercetare-Dezvoltare al Universității Transilvania din Brașov

Institutul este compus din 11 laboratoare de cercetare și o clădire administrativă, concentrând o infrastructură modernă și complexă de cercetare, constând în linii integrate de echipamente high-tech pentru cercetare avansată în domeniul dezvoltării durabile. Arhitectura informațională din cadrul institutului, reprezentată în figura 3.9, este formată dintr-un centru de date modern, dezvoltat cu preponderență pe tehnologii cloud computing și 12 module funcționale care oferă clienților capabilități de interconectare cu centrul de date prin intermediul unor conexiuni de bandă largă având la bază o rețea de distribuție de fibră optică.

Având ca principal obiectiv cercetarea, centrul de date a fost dezvoltat astfel încât să satisfacă nevoile tuturor laboratoarelor de cercetare și deci să acomodeze o varietate mare de tehnologii de ultimă generație, dar și echipamente și software clasice. Acestea au o eterogenitate ridicată, oferind o paletă largă de capabilități. Unele dintre ele au o flexibilitate ridicată și permit programarea pentru o varietate mare de sarcini, în timp ce altele au un nivel ridicat de specializare și sunt dedicate doar pentru efectuarea unui anumit tip de operațiuni.

Dintre caracteristice principale ale acestui mediu se remarcă următoarele:

- *diversitate* - fiecare dintre aceste module utilizează echipamente și software de specialitate, având diferite cerințe operaționale de funcționalitate și oferind beneficiarilor capabilități diverse;
- *accesul la resurse* – dat fiind specificul instituției (educație și cercetare) și neconcentrarea corpurilor de clădire ale Universității „Transivania” într-o singură locație, în numeroase cazuri este nevoie de accesul la resurse din afara perimetrului institutului, pe perioade de timp variate și utilizând diferite tipuri de terminale;

- *dinamica personalului* - persoanele care au nevoie de acces la resursele informaționale sunt studenți, membri ai corpului profesoral al universității, dar și invitați, cercetători, specialiști colaboratori, furnizori sau administratori ai resurselor. O parte dintre utilizatori fac parte din organizație, necesită acces constant pe o perioadă mai lungă de timp și utilizează cu preponderanță terminale localizate în interiorul institutului. Pe de altă parte, o categorie semnificativă este formată din utilizatori care necesită acces la resurse doar în anumite momente de timp, din diferite locații din afara perimetrului institutului de cercetare și de pe terminale cu grad limitat de încredere;
- *performanță* – desfășurarea eficientă a proceselor de cercetare și învățământ necesită capabilități de nivel înalt în ceea ce privește performanțele de calcul, stocare și transfer al datelor. De asemenea, este necesară oferirea de posibilități avansate pentru back-up și redundanță, minimizarea timpilor în care resursele nu sunt disponibile la capacitățile normale, reziliență, recuperare date etc.
- *inovație* – mediul operațional din cadrul institutului trebuie să acomodeze atât echipamente și software mature, dar și unele inovative, aflate în stadiul de cercetare, al căror impact asupra celorlalte resurse ale rețelei încă nu este pe deplin studiat.

Abordarea inițială a echipei de securitate a fost aceea de a realiza securitatea mediului de lucru prin utilizarea de mecanisme, instrumente, politici și proceduri specifice strategiei clasice „ apărarea în adâncime”. Astfel s-au identificat și implementat instrumente, cum ar fi: firewall-uri, soft-uri antivirus, soft-uri antimalware și numeroase alte tehnologii.

Cu toate că s-au implementat un spectru larg de măsuri de securitate pe mai multe niveluri, cu alocări semnificative de resurse materiale, sistemul a experimentat în perioada analizată (2014-2016) numeroase incidente de securitate.

Analizele efectuate de echipa de securitate au scos la iveală următorii vectori de compromitere a sistemelor:

- exploatarea vulnerabilității sistemelor din cauza neefectuării corespunzătoare a update-urilor sistemelor de operare și a soft-urilor utilizate;
- infectarea sistemelor prin accesarea de către clienți a unor aplicații nocive și disponibile pe Internet;
- compromiterea sistemelor prin utilizarea necorespunzătoare a conturilor de utilizator;
- infectarea sistemelor prin conectarea la resursele rețelei a unor terminale (laptop, telefon, tablete) personale deja infectate;
- infectarea sistemelor prin utilizarea unor echipamente de stocare tip memory stick infectate;
- incompatibilități între soluțiile de virtualizare implementate;
- incompatibilități între aplicații sau între aplicații și sisteme de operare și de virtualizare;
- deficiențe ale actualizărilor de securitate care determină blocarea aplicațiilor;
- scanarea cu deficiențe a datelor care sunt livrate în cantități mari;

Analiza efectuată a constatat că măsurile de securitate implementate pentru securizarea mediului de lucru au limitări considerabile. Astfel, utilizarea mecanismelor specifice strategiei clasice de apărare a resurselor informaționale ale organizației nu reușește să facă față nevoilor actuale ale organizației și se impune identificarea unor noi paradigme care să înlocuiască sau să completeze actuala strategie.

3.6 Analiza viabilității strategiilor clasice

Tehnologia are în momentul de față un impact dramatic asupra mediului organizațional actual, având capacitatea de a influența decisiv procesele organizaționale și modul de desfășurare a acestora. Tehnologia informațională nu mai este doar un element de suport al activității, ci a evoluat într-un element de nivel strategic, fiind un important agent ce influențează schimbarea la nivelul întregii organizații. Ea se constituie astfel într-un element de importanță critică în

procesul decizional, putând constitui elementul de optimizare a proceselor și de eficientizare a utilizării resurselor sau chiar de creare de noi oportunități.

În războiul clasic cinetic, gradientul de pierdere al forței - loss of strength gradient (LSG) este un indicator care arată că puterea distructivă a unui atacator este invers proporțională cu distanța până la țintă (Boulding, 1962). Agresorul va încerca permanent să reducă acest dezavantaj și să se apropie de țintă cât mai mult. Același autor a remarcat totuși că, o dată cu dezvoltarea tehnologică, metodele moderne de livrare a încărcăturii distructive la țintă au evoluat iar indicatorul LSG nu mai are relevanța corespunzătoare. Utilizarea tacticilor precum bombardament strategic, război asimetric etc. fac ca distanța fizică între agresor și țintă să nu mai fie un element care să influențeze radical puterea distructivă a acestuia.

Mediul cibernetic se disociază și el de tipicul războiului clasic. Viteza foarte mare de transfer a încărcăturii distructive către sursă permite agresorului cibernetic să se poziționeze „departe" de țintă. Realitatea a evidențiat faptul că în mediul virtual distanța geografică dintre agresor și țintă este de fapt un avantaj pentru primul dintre ei. Prin rutarea succesivă a traficului prin mai multe echipamente distribuite în diferite zone geografice pe glob, viteza de atac este minim afectată, dar este îngreunat mult, efortul echipelor defensive de identificare a sursei atacului.

Strategiile clasice de atac, presupun din partea atacatorului, desfășurarea de acțiuni complexe și costisitoare pentru construirea direcției de atac iar, o dată adoptată, schimbarea acesteia necesită costuri considerabile. Pe baza acestui principiu și apărătorii, încearcă identificarea cât mai timpurie a acestei direcții și dispunerea corespunzătoare a cât mai multor mecanisme defensive. Mediul cibernetic permite atacatorului să utilizeze algoritmi automați de redirecționare a traficului care permit schimbarea direcției de atac foarte ușor, cu costuri minime. Mecanismele defensive nu pot fi relocate sau ajustate cu tot atât de mare flexibilitate oferind posibilități de acțiune atacatorului.

O altă caracteristică a conflictului clasic este aceea că cele două părți își cunosc oponenții și se încearcă descurajarea inamicului prin promovarea sau chiar amplificarea capabilităților de care o parte dispune. Se încearcă obținerea victoriei prin astfel capitularea inamicului, minimizarea acțiunilor combative și minimizarea resurselor pierdute. În cadrul războiului cibernetic atacatorul nu dorește să fie identificat și efectuează operațiuni pentru ascunderea și disimularea sa. El nu dorește să își demoralizeze inamicul prin dezvăluirea capabilităților sale, nu încearcă evitarea conflictului.

Spre deosebire de mediul clasic, în mediul virtual atacatorul nu este preocupat de pierderile resurselor cibernetice avute, fiind mai degrabă interesat de identificarea vulnerabilităților și utilizarea eșecurilor pentru îmbunătățirea viitoarelor atacuri. Refacerea capacității de luptă este un proces mult mai puțin costisitor comparativ cu beneficiile obținute de sacrificarea resurselor.

Posibilitatea mediului cibernetic oferită unui atacator de a-și disimula acțiunile și identitatea îi conferă acestuia protecție în fața acțiunii normelor legislative în vigoare. Din cauza vidului legislativ din domeniu (Shackelford, 2014) al multor țări, a lipsei unui consens legislativ internațional în domeniu, utilizarea unor echipamente dislocate în zone geografice diferite și aflate sub jurisdicții a diferite state îngreunează sau chiar face imposibilă tragerea la răspundere a infractorilor cibernetici.

Starea de obscuritate în care este poziționat apărătorul îi limitează inițiativa și este forțat să efectueze cu predilecție acțiuni defensive. O tactică specifică războiului clasic este aceea ca, după slăbirea forței atacului inițial, apărătorul să execute operațiuni contraofensive pentru combaterea sau chiar anihilarea atacatorului. În mediul virtual contraatacul nu apare decât rar, foarte târziu raportat la viteza de atac, deoarece executarea unor astfel de acțiuni nu are decât un vag fundament legislativ, iar costurile efectuării de către o organizație a unor astfel de acțiuni nu aduc avantaje economice.

Prin tacticile și procedeele utilizate agresorul provoacă organizația să construiască multiple niveluri de protecție, din ce în ce mai complexe, care necesită cantități considerabile de

resurse și costuri de administrare. Aceste măsuri au de asemenea și un efect negativ indirect, asupra eficienței membrilor organizației și a proceselor desfășurate. Posibilitatea ca oricine, la orice oră și din orice locație să fie în măsură să execute atacuri pe orice direcție, forțează organizațiile să adopte poziții nesustenabile economic care pot duce la eșecul acestora.

Din cauza specificului Internetului și a vidului legislativ, chiar dacă atacul este oprit, totuși agresorul nu este neutralizat. Acesta poate oricând să renunțe la atacul curent și să revină la alte faze ale atacului (Alonso, 2016) sau să încerce exploatarea altor vulnerabilități. Mai mult decât atât el poate utiliza mai departe informațiile obținute din atacurile eșuate, în desfășurarea de acțiuni mult mai complexe.

Pentru mulți ani strategia „apărare în adâncime" a constituit principala strategie de protejare a datelor organizației. Dezvoltarea noilor tehnologii și a arhitecturilor moderne de manipulare a datelor forțează capabilitățile acesteia, evidențiindu-i limitările și în anumite cazuri, ea devenind mai degrabă o povară decât un avantaj. Arhitecții și dezvoltatorii de sisteme nu au considerat securitatea datelor ca o componentă esențială a arhitecturilor sistemelor și aplicațiilor informatice, ci mai degrabă ca un element care obstrucționează activitatea, necesită costuri și induce ineficiență. Ca o consecință a acestei abordări, echipele de securitate au fost nevoite să construiască, în jurul acestor arhitecturi, sisteme defensive de protecție din ce în ce mai complexe o dată cu proliferarea tipurilor și numărului de atacuri și evoluția modelului infractorului cibernetic.

Din cauza acestor motive se poate trage concluzia că organizațiile moderne nu mai pot considera strategia „apărare în adâncime" ca element de bază a arhitecturii de protecție a infrastructurilor lor informaționale. Securitatea datelor este un element cheie în organizațiile moderne care necesită mecanisme adaptate la particularitățile și provocările mediului cibernetic actual.

3.7 Propuneri

Ca urmare a deficiențelor identificate în utilizarea strategiei actuale de protejare a activelor informaționale ale unei organizații, am identificat o serie de inițiative astfel:

a) Securitate prin minimizarea riscurilor sau prioritizarea securității

Propunerea se referă la abordarea domeniului securității datelor unei organizații pe principii de management al riscului. Costurile suportate de organizație în vederea creării unui mediu sigur de prelucrare a datelor trebuie raportate la importanța pe care o au datele pentru organizație.

La baza unei astfel de abordări rezidă efectuarea de către organizație a unui plan complex de identificare a activelor informaționale și de evaluare a impactului pe care compromiterea acestora le-ar putea avea asupra organizației. Pe baza acestui plan s-ar putea direcționa resursele organizației pentru protejarea cu prioritate a resurselor cu impact major, realizându-se astfel o creștere a eficacității și deci a investițiilor în securitate. Datorită impactului redus, resursele cu importanță mică ar benefica de alocări de resurse limitate sau de priorități scăzute în cazul unor atacuri. Acestea ar fi „sacrificate" de organizație pentru scăderea vitezei de propagare a atacului, voalarea eforturilor atacatorului, obținerea timpului necesar pentru identificarea caracteristicilor atacului și punerea în aplicare a măsurilor în caz incident informatic.

b) Automatizarea securității

Această inițiativă are la bază imposibilitatea factorului uman de a controla în detaliu medii informatice complexe precum și viteza scăzută de reacție în raport cu viteza de derulare a atacurilor informatice. Un sistem de protecție automat, integrator se bazează pe informațiile provenite de la un număr mare de senzori, distribuiți în întregul mediu informațional aflat în zona de interes. Acesta poate monitoriza permanent modul de utilizare a resurselor și reacționa rapid la eventualele tentative de compromitere a rețelei. Sistemul integrează o multitudine de senzori, dispuși în multiple locații (terminale, servere, echipamente de rețelistică, firewall etc.)

care adună permanent informații despre entitățile prezente în rețea și modul de utilizare a resurselor.

Rolul factorului uman în acest sistem este cel decizional și de auditare a performanței. Astfel, acesta este responsabil cu stabilirea procedurilor de reacție precum și a nivelurilor la care acestea se pun în aplicare, care trebuie să fie în strictă corespondență cu necesitățile operaționale și politica de securitate informațională a organizației.

c) Atragerea implicării utilizatorilor

Strategia clasică a apărării în adâncime, consideră utilizatorul resurselor informatice ca un element care are un rol redus în asigurarea securității datelor. Acestuia îi este definit un cadru operațional static în care trebuie să funcționeze și el cunoaște în orice moment locația în care se află datele și ce echipamente sunt utilizate pentru procesarea acestora. Responsabilitățile acestuia referitoare la asigurarea protecției datelor sunt restrânse la identificarea elementelor de funcționare anormală și de semnalare a acestora către echipele specializate de securitate.

d) Securitate prin design

Dezvoltarea sistemelor clasice este focusată pe construirea capabilităților funcționale, lăsând componenta de securizare a produsului ca o componentă care trebuie implementată ulterior. Această abordare, de acoperire a vulnerabilităților pe măsură ce acestea sunt identificate menține organizațiile într-o stare de risc permanent și necesită alocări de resurse considerabile pe termen lung.

Strategia securității prin design se referă la considerarea securității ca un element critic al performanței unui sistem încă din fază de proiectare. În acest model, atât pentru produsele hardware, software, cât și pentru serviciile oferite trebuie avute în vedere caracteristici de securitate în ceea ce privește manipularea datelor și menținerea funcționării normale a sistemelor.

e) Dezvoltarea unei legislații globale în domeniu

Caracterul globalizator al utilizării tehnologiei, precum și viteza foarte mare de transfer a datelor sunt utilizate de către infractorii cibernetici pentru efectuarea acțiunilor distructive și ascunderea identității acestora. Prin disimularea acțiunilor și direcționarea vectorilor de atac prin intermediul mai multor echipamente succesive, localizate în jurisdicții diferite, se îngreunează posibilitatea apărătorului de a identifica infractorul și de a adopta măsuri eficiente pentru neutralizarea acestuia în timp oportun.

f) Apărarea activă

Conceptul apărării active vine să completeze cel clasic și propune un nou mod de acțiune pentru protejarea activelor organizației. Modelul se bazează pe efectuarea de acțiuni preventive cu scopul de a identifica riscurile din mediul de operare intern și extern și de a efectua acțiuni pentru managementul acestuia. Aceste acțiuni au rolul de descurajare a infractorilor, pe de o parte și de minimizare a riscului de compromitere a resurselor, pe de altă parte.

3.8 Concluzii

Internetul a apărut din dorința de a exploata capabilitățile comunicaționale din ce în ce mai avansate ale tehnologiei. La momentul apariției internetului și în primele sale etape de dezvoltare, securitatea datelor nu a fost considerată o problemă critică, fiind făcute doar tangențial considerații privind natura acesteia. Pentru o bună perioadă de timp securitatea a fost considerată doar un nivel adițional, adăugat peste arhitectura informațională, fiind privită de cele mai multe ori ca un element care blochează performanța sistemelor, introduce ineficiențe în acestea și necesită investiții care nu returnează beneficii.

Strategiile clasice utilizate pentru protejarea activelor informaționale ale organizațiilor care activează în domeniul cloud computing nu mai fac față provocărilor acestui mediu de operare a datelor. Studiu de caz efectuat în cadrul Institutului de Cercetare-Dezvoltare al Universității Transilvania din Brașov, în perioada 2014-2016, a scos în evidență că o arhitectură clasică defensivă nu poate asigura un mediu de securitate optim pentru capabilități specifice cloud computing-ului.

Caracterul static pur reactiv al acestora lasă inițiativa de partea atacatorului și pune o presiune permanentă pe sistemele defensive ale organizațiilor. Valoarea ridicată a informației a determinat atragerea în domeniul infracțional a unor resurse consistente materiale și umane care au permis dezvoltarea de instrumente complexe de atac bazate pe utilizarea rău intenționată a unor capabilități tehnologice legitime. Vacuumul legislativ și caracterul pur defensiv al strategiilor clasice de protejare a capabilităților informaționale permit un spectru larg de acțiuni ale atacatorului care necesită alocarea constantă de resurse informaționale defensive, proces care este nesustenabil pe termen lung de către organizații.

4. Token-izarea ca tehnică de securizare a informației

4.1 Studiu privind metodele actuale de obscurizare a informației

Obiectivul acestui capitol este acela de a analiza și de a compara tehnicile actuale de obscurizare a datelor utilizate în industrie, evidențiind în același timp potențialul de utilizare al token-izării într-un domeniul mai larg de activități decât cel în care este utilizat în prezent.

De la apariția sa, tehnologia cloud computing a atras organizațiile moderne prin numeroasele avantaje pe care aceasta le oferă (Salesforce, 2016). Din păcate, noul mediu de operare, prin modificarea cadrului de prelucrare a datelor necesită abordări inovative cu privire la modalitățile de securizare a resurselor informaționale ale unei organizații.

Obscurizarea informației este una dintre cele mai frecvente metode utilizate pentru protejarea datelor sensibile în mediul informațional. Deși este o componentă critică a mediului de securitate informațional, ea nu reușește să asigure întregul spectru de necesități ale securizării datelor, necesitând a fi integrată în ansamblul general de instrumente specifice.

Există mai multe tehnici de obscurizare a datelor care pot fi grupate, în funcție de modificările pe care le execută asupra datelor originale, în trei mari categorii:

- criptarea (toate datele din pachetul de informație sunt afectate și procesul este reversibil);
- mascarea datelor (nu toate datele din pachetul de informație sunt afectate, dar procesul este ireversibil);
- token-izarea datelor (nu toate datele din pachetul de informație sunt afectate, iar procesul este reversibil).

4.1.1 Criptarea datelor

Criptarea reprezintă procesul de conversie a informațiilor sau datelor într-un format care împiedică accesul neautorizat la ele (Oxford Dictionary, 2018). Criptarea se realizează prin utilizarea unor operații matematice complexe, bazate pe algoritmi criptografici specifici pentru alterarea pachetului de date original, astfel încât rezultatul să poată fi descifrat în timp util doar de către persoane autorizate. Accesul persoanelor autorizate la informația utilă este făcut prin utilizarea unei chei de decriptare.

Algoritmii moderni de criptare a informației pot fi împărțiți în două mari categorii: simetrici și asimetrici. Fiecare dintre aceștia are avantaje și dezavantaje iar alegerea utilizării unuia dintre ei este dictată de nevoile situațiilor particulare și constrângerile operaționale. În ambele cazuri, unul dintre aspectele cele mai importante ale criptării este acela că funcția de criptare este o bijecție (Dasgupta S., 2008), astfel încât există o funcție inversă care oferă o modalitate de a reconstrui mesajul original pe baza unei chei.

Implementarea criptării datelor este una dintre cele mai frecvent utilizate metode pentru protejarea acestora. Metoda are și numeroase limitări și constrângeri de utilizare, cum ar fi:

- este puternic consumatoare de resurse computaționale, necesitând alocarea de resurse dedicate pentru implementarea unor capabilități hardware și software. Acest lucru o face nepractică pentru sisteme care au la dispoziție doar o cantitate limitată de resurse;
- necesită sisteme complexe pentru asigurarea securității cheilor de criptare;
- necesită, pentru integrarea eficientă, reproiectarea amplă a proceselor organizaționale;

- necesită resurse sporite pentru întreținerea sistemului;
- crește dificultatea integrării sistemelor moderne cu cele vechi;
- limitează capabilități esențiale ale mediului cloud computing, precum: munca colaborativă, partajarea resurselor și induce complexități ridicate în mediile cu dinamică și mobilitate sporită a resurselor/personalului;
- limitează eficiența angajaților, necesitând executarea unor operații suplimentare pentru accesarea informațiilor;
- nu oferă posibilitatea efectuării unor procese analitice pe datele criptate, analize care ar ajuta organizația în obținerea unor avantaje.

4.1.2 Mascarea datelor

Mascarea este o a doua metodă de obscurizare a datelor prin care se creează o versiune asemănătoare, dar falsă, a unei secțiuni dintr-un pachet de date care înlocuiește secțiunea originală (Rouse, 2017). Există mai multe tehnici utilizate pentru mascarea datelor (substituirea, amestecarea, variația numărului și a datelor, nulizarea, ștergerea etc.), la baza selecției cu privire la metoda care urmează să fie utilizată fiind mai multe criterii, precum: necesitățile operaționale, integrarea aplicațiilor, flexibilitatea, costurile etc. Principala caracteristică a acestei tehnici este aceea că datele mascate nu pot fi convertite înapoi la datele originale, deoarece funcția de conversie a datelor nu este reversibilă; mai mult, ea nu necesită nici măcar să fie o funcție injectivă.

În general, algoritmii de mascare necesită resurse computaționale mai scăzute decât criptarea și induc influențe minime în procesele organizaționale. Totuși, utilizarea măscării ca tehnică de obscurizare a datelor are câteva limitări care restrâng spectrul de utilizare a acesteia:

- este un proces unidirecțional, neoferind posibilitatea refacerii datelor originale;
- nu poate fi utilizată pentru a comunica date sensibile dar utile aplicațiilor și utilizatorilor legitimi;
- nu poate fi aplicată la toate datele din pachetul de informație, necesitând efectuarea unor selecții;
- crește riscul de expunere accidentală datorat utilizării unor algoritmi de selecție necorespunzători.

4.1.3 Token-izarea

A treia metodă de obscurizare a datelor – token-izarea – reprezintă procesul de înlocuire a unui element de date sensibil dintr-un pachet de date cu un echivalent non-sensibil, denumit token, care nu are semnificație sau valoare exploatabilă (Care & Litan, 2016). Token-ul este o referință (identificator) care se raportează la datele sensibile printr-un sistem de token-izare. Sistemul oferă capabilități de a ascunde sau afișa date sensibile în funcție de nivelul de acces la informații al celui care face solicitarea.

Pentru a fi capabil să furnizeze astfel de servicii, sistemul păstrează o bază de date a corespondenței token - date sensibile asociate, denumit seif. La fel ca și în cazul criptării, în care managementul cheilor de criptare reprezintă un element critic al sistemului și în cazul sistemelor de token-izare menținerea seifului de date în stare optimă de operare și protejarea lui împotriva accesului neautorizat se constituie ca una dintre principalele cerințe care condiționează calitatea serviciilor oferite de către sistem.

Implementarea token-izării, ca metodă de obscurizare a datelor unei organizații, oferă posibilitatea filtrării accesului la informația utilă astfel încât aceasta poate fi accesată doar de către entitățile autorizate. Sistemul este dinamic, independent și efectuează operațiunile autonom, astfel încât capabilitățile oferite sunt pretabile pentru utilizarea în mediile cu dinamică ridicată.

Token-izarea realizează protecția informațiilor prin înlocuirea doar a informațiilor sensibile cu unele fără valoare. Astfel, asupra pachetului de date rezultat se pot aplica o serie de procese analitice, fără a compromite securitatea informațiilor, întrucât nu toate datele din pachet

sunt alterate de către proces. În acest fel token-izarea se aseamănă cu procesul de mascare a datelor, putând fi utilizată cu succes în procese care au nevoie de date reale.

4.2 Analiză comparativă a tehnicilor de obscurizare a datelor

Pentru a oferi o mai bună înțelegere a celor trei tehnici de obscurizare a datelor și pentru a identifica avantajele și punctele slabe am desfășurat o analiză comparativă din trei perspective: cerințele hardware și software, capacitățile de securizare a datelor și impactul asupra proceselor organizaționale de afaceri.

Modelul utilizat este bazat pe modelul propus de (Rhoton, 2009), în care evaluarea riscurilor este calculată pe baza probabilității și a impactului asupra sistemelor pe care le-ar avea producerea riscului anticipat. Astfel, costul unei investiții trebuie sa fie mai mic sau egal cu valoarea informației protejate. Analiza comparativă dorește să scoată în evidență care dintre aceste metode de obscurizare a datelor este mai utilă de utilizat, ea trebuind să satisfacă la nivel optim atât problematica securizării datelor, cât și a reducerii costurilor cu investițiile în securitate.

O componentă de noutate introdusă în această analiză este componenta de influență asupra proceselor organizaționale. Integrarea tehnologiei în cadrul proceselor organizaționale poate aduce avantaje pentru organizații, dar implementată necorespunzător poate genera limitări ale performanței sistemelor care estompează avantajele aduse. În general, securizarea datelor necesită introducerea unor etape suplimentare de manipulare a datelor și are un impact negativ asupra performanței sistemului.

4.2.1 Capabilități de securizare a datelor

Pentru analizarea capabilităților de securitate a datelor s-a utilizat modelul bazat pe triada CIA (confidențialitate, integritate și disponibilitate) (Panmore Institute, 2016) completat cu caracteristicile de autentificare și non-repudiere a informației.

Sistemele bazate pe criptare asigură confidențialitatea prin transformarea datelor originale și necesită posesia unei chei pentru accesul la acestea. Managementul cheilor de criptare este un proces amplu care necesită sisteme de comunicații securizate suplimentare în cazul criptării simetrice sau sisteme complexe și costisitoare de integrare a infrastructurii de chei publice – public key infrastructure (PKI) în cazul criptării asimetrice. Implementarea și gestionarea sistemelor de gestionare a cheilor de criptare în medii cloud computing, în care se pune un accent puternic pe lucrul colaborativ, cu cerințe mari de acces partajat la resurse, cu mobilitate și dinamică ridicată a utilizatorilor, este o sarcină foarte dificilă, introduce o mare complexitate a sistemului și limitează disponibilitatea datelor. Furnizarea integrității datelor în sistemele bazate pe criptare se realizează prin implementarea funcțiilor criptografice de hash cu ajutorul cărora se poate determina rapid dacă mesajul original a fost modificat.

Sistemele bazate pe criptare pot oferi capabilități de autentificare prin utilizarea unor chei secrete și a semnăturilor digitale, în timp ce non-repudierea este asigurată prin implementarea unor sistemelor complexe PKI. Criptarea poate fi utilizată pentru toate tipurile de date dintr-o organizație, aflate în stări de tranzit sau repaus. Studiul efectuat de (Maha Tebaa, 2013) a constatat că poate fi utilizată chiar și pe timpul procesării datelor necesitând însă resurse computaționale deosebite.

Sistemele care utilizează mascarea ca și metodă de obscurizare asigură confidențialitatea și integritatea datelor prin înlocuirea datelor sensibile cu unele fără valoare într-un proces unidirecțional. Astfel, accesul la datele originale este limitat și acestea nu pot fi modificate sau compromise.

Integritatea datelor mascate nu se constituie într-o cerință de bază deși, pentru realizarea compatibilității cu alte aplicații, uneori există anumite cerințe privind formatul acestora. Algoritmii de mascare pot fi proiectați să mascheze datele pe baza unor șabloane care au instrumente de verificare a integrității, cum ar fi controlul sumelor. Sistemele bazate pe mascare

nu oferă ele însele disponibilitate, autentificare sau non-repudiere, realizarea acestor capabilități în sistemele informaționale necesitând utilizarea unor sisteme suplimentare.

Teoretic, mascarea datelor poate fi utilizată pentru a ascunde orice tip de date dintr-o organizație, dar aplicarea nediscreționară reduce aproape la zero valoarea întregului pachet de date. Din cauza imposibilității reconstruirii formei originale, înainte de efectuarea efectivă a procedurii de mascare este necesară aplicarea unor algoritmi de selecție a datelor care urmează a fi mascate. De asemenea, este necesară crearea unui șablon de mascare, astfel încât rezultatele să fie compatibile cu alte aplicații.

Mascarea datelor sensibile se poate efectua chiar dacă acestea sunt în transfer sau în procesare. Bineînțeles, după efectuarea operațiunii acestea sunt eliminate/înlocuite, deci procesul de mascare le elimină și nu mai pot fi readuse la faza inițială.

În sistemele bazate pe token-izare confidențialitatea și integritatea datelor este asigurată atât prin înlocuirea datelor originale sensibile cu datele non-sensibile cât și prin limitarea accesului la seiful de date. Accesul la aceste date se realizează prin implementarea unor sisteme de autentificare bazate pe tehnologii suplimentare, deoarece token-izarea nu oferă astfel de capabilități.

Disponibilitatea datelor este ușor de asigurat în sistemele de tokenizare cu amploare redusă, dar devine o sarcină complexă atunci cât token-izarea este utilizată extensiv pentru pachete mari de date. Acest risc poate fi minimizat prin implementarea unor proceduri stricte de clasificare a datelor și de limitare a utilizării tehnologiei doar pentru anumite categorii. Distribuirea bazei de date cu token-i pe mai multe sisteme poate spori disponibilitatea, dar introduce alte probleme. Astfel realizarea operațiilor sincronizarea continuă a bazei de date și back-up cresc în complexitate odată cu creșterea numărului de înregistrări și condiționează eficiența unor astfel de sisteme la un anumit prag critic al numărului de tranzacții.

Sistemele de token-izare pot fi utilizate pentru asigurarea securității datelor sub orice formă a acestora, însă nu oferă instrumente pentru autentificare sau non-repudiere pentru care este necesară utilizarea unor sisteme adiționale.

4.2.2 Costuri în investiții hardware și software

Fiecare dintre cele trei tehnologii are cerințe diferite în ceea ce privește resursele computaționale necesare pentru asigurarea bunei funcționări a sistemelor. Din cauza faptului că procesul de criptare se bazează pe algoritmi matematici complecși acest tip de sisteme sunt consumatoare ridicate de putere de calcul și necesită investiții considerabile în echipamente hardware și software dedicate. Sistemele trebuie calibrate corespunzător pentru a susține capacitățile maxime de încărcare și pentru a minimiza riscul de eșec în momentele de vârf ale cererii. Astfel o mare parte a performanței acestora rămâne neutilizată în perioadele de funcționare normală.

Cheile de criptare/decriptare sunt elemente critice pentru securitatea datelor, iar compromiterea sau indisponibilitatea acestora determină pierderea valorii întregului pachet de date obscurizat. Dacă pentru sistemele cu criptare simetrică acest lucru este rezolvat prin asigurarea unor canale adiționale de comunicare și prin compromisuri cu privire la capabilitățile dinamice și a timpului de răspuns, la sistemele cu criptare asimetrică respectivele limitări au fost eliminate prin dezvoltarea unor sisteme adiționale complexe de chei publice care necesită alocări de resurse consistente.

Managementul cheilor de securitate solicită numeroase costuri în ceea ce privește proiectarea, implementarea și gestionarea unui sistem care să satisfacă nevoile organizaționale care activează în special în medii dinamice, cu operațiuni frecvente asupra cheilor (furnizare, ștergere, reînnoire, arhivare etc.). Sistemul de management al cheilor de securitate în mediile cloud computing poate fi externalizat și transferat către entități terțe (securitatea ca serviciu) determinând o scădere a costurilor, dar cu un compromis în ceea ce privește creșterea riscului de pierdere a securității datelor datorat creșterii numărului potențialilor vectori de atac asupra confidențialității datelor din noul mediu de operare al datelor.

Capabilitățile extinse ale sistemelor de obscurizare bazate pe criptare pot genera costuri nejustificate prin utilizarea necorespunzătoare. Versatilitatea ridicată atrage utilizatorii în suprautilizarea sistemelor pentru criptarea unor date pentru care acest lucru nu este necesar. Clasificarea incorectă a informațiilor, în special supraclasificarea pentru evitarea compromiterii datelor, necesită redimensionări ale sistemelor care să acomodeze aceste cereri și generează costuri nejustificate.

Tehnologiile de mascare și de token-izare a datelor nu se bazează pe algoritmi sau sisteme complexe pentru desfășurarea corespunzătoare a procesului, având necesități limitate în ceea ce privește cerințele de infrastructură și costurile de întreținere.

Procesul de mascare elimină total sistemele de gestionare a cheilor și infrastructura complexă a sistemului de chei publice, necesitând resurse de calcul limitate și sarcini administrative minime. Token-izarea necesită investiții dedicate în resurse computaționale cu predilecție în domeniul gestionării token-ilor, al securizării canalelor de comunicație și al administrării seifului de date. Sistemul de gestionare a cheilor de criptare este limitat la asigurarea legăturii securizate cu seiful de date și are o influență minimă asupra complexității sistemului.

Sistemul token-izării se bazează pe o bază de date centrală, pentru care managementul acesteia crește rapid în dificultate o dată cu creșterea numărului de token-i din cadrul ei. Utilizată intensiv în medii de lucru distribuite global o astfel de bază de date necesită resurse considerabile pentru menținerea în stare optimă de funcționare, cu păstrarea indicatorilor de calitate a serviciilor oferite. De asemenea, o bază de date amplă, eventual distribuită la distanță va solicita resurse ridicate pentru administrarea, realizarea copiilor de siguranță, actualizarea înregistrărilor și efectuarea altor operațiuni asupra sistemului. Ea crește amplitudinea și complexitatea operațiunilor de întreținere și cantitatea de resurse necesare funcționării adecvate.

4.2.3 Impactul asupra proceselor organizaționale

În organizațiile moderne tehnologia a trecut de la stadiul de funcție de suport a proceselor acesteia, putând fi considerată un potențator al eficacității activităților derulate. În majoritatea cazurilor, implementarea politicilor de securitate a datelor în cadrul organizațiilor, în cazul de față a tehnologiilor de obscurizare a datelor, impune limitări care au un impact negativ asupra proceselor și limitează eficiența acestora.

Din această perspectivă, criptarea este cea mai invazivă dintre cele trei metode, iar prin sistemele complexe pe care le adaugă crește riscul de apariție a erorilor. De asemenea, pentru integrarea acestei tehnologii în fluxul operațional organizațional este necesară reproiectarea proceselor interne specifice. Această reproiectare este una extinsă și determină introducerea unor etape suplimentare care necesită efectuarea unor activități suplimentare și alocări de timpi de procesare. Se constată astfel o limitare a performanței sistemului.

Tehnologia mascării datelor presupune operațiuni mai puțin complexe și are influențe limitate asupra proceselor interne derulate în organizație. De cele mai multe ori, implementarea ei presupune adăugarea unui nivel care realizează înlocuirea datelor. Tehnologia necesită schimbări limitate în procesele organizaționale și este puternic utilizată de organizații pentru stabilirea rapidă a unui mediu de informație securizat. Marele dezavantaj al acestei tehnologii este că ea limitează accesul persoanelor legitime la datele obscurizate, pentru realizarea acestui lucru fiind necesară utilizarea unor alte tehnologii suplimentare.

Impactul tehnologic al token-izării asupra proceselor organizaționale este determinat de complexitatea medie a acestei tehnologii. Ea obscurizează datele sensibile ale organizației, permițând în același timp accesul persoanelor și aplicațiilor legitime la ele. Integrarea cu alte sisteme este relativ simplă, complexitatea sistemului fiind mai ridicată doar în partea de securizare a seifului de date și a managementului token-ilor.

Implementarea token-izării introduce întârzieri minime de timp în procesele organizaționale, necesită modificări pentru integrarea aplicațiilor și reproiectarea unor procese, impune actualizarea procedurilor de operare și instruirea utilizatorilor. Se poate concluziona că

adoptarea token-izării are un impact, asupra proceselor organizaționale, care este mai mare decât cel al tehnologiei de mascare, dar este considerabil mai mic în comparație cu tehnologia criptării.

Analiza de mai sus scoate în evidență faptul că fiecare tehnică de obscurizare are unele avantaje care o recomandă a fi utilizată de organizații în anumite medii/aplicații în funcție de nevoile și condițiile specifice. Astfel:

Criptarea

- se poate aplica tuturor tipurilor de date dintr-o organizație;
- poate fi folosită pentru a asigura transferul de date sensibile și chiar prelucrarea acestora în medii nesigure;
- oferă capabilități avansate de securitate cum ar fi autentificarea și non-repudierea;

Mascarea

- creează un mediu de testare curățat de date sensibile, care se aseamănă cu cel de producție, optim pentru ca echipele de cercetare - dezvoltare să efectueze teste în condiții cât mai realiste;
- oferă, păstrând securitatea, date reale cercetătorilor pentru a determina eficacitatea produselor, pentru a identifica necesitățile clienților și nivelul de satisfacție;
- pune date curățate la dispoziția companiilor care monitorizează profilul clienților în vederea îmbunătățirii serviciilor sau pentru a maximiza eficacitatea publicității;
- oferă instrumente pentru îmbunătățirea activității de colaborare, asigurând în același timp protecția datelor sensibile;
- are o influență minimă asupra proceselor organizaționale din organizație;
- necesită resurse hardware și software limitate precum și eforturi administrative minime.

Token-izarea

- necesită costuri hardware, software și de mentenanță limitate;
- are un impact minim asupra proceselor organizaționale;
- optimizează capacitățile de externalizare prin limitarea riscului de compromitere a datelor (chiar dacă mediul de stocare al furnizorului de servicii a fost compromis, sunt compromiși doar token-ii dar nu și datele sensibile);
- oferă suport pentru respectarea reglementărilor guvernamentale referitoare la manipularea datelor personale (standardul de securitate din industria plăților electronice - Payment Card Industry Data Security Standard – PCI/DSS, legea privind portabilitatea și atribuirea responsabilității privind informațiile din sănătate - Healthcare Information Portability And Accountability Act - HIPAA, legea federală privind managementul securității informațiilor - Federal Information Security Management Act - FISMA, Sarbanes-Oxley Act -SOX, reglementarea protejării datelor la nivel european- General Data Protection Regulation - GDPR etc.);
- oferă suport pentru respectarea reglementărilor privind localizarea datelor cu caracter personal. În sistemele de calcul cloud, datele sunt prelucrate utilizând aplicații distribuite la nivel global sau, pentru creșterea rezilienței, sunt salvate în mai multe locații distribuite geografic în întreaga lume. Acest lucru nu este întotdeauna în conformitate cu legislațiile locale care interzic procesarea/salvarea datelor cu caracter personal în afara unor anumite zone geografice. Prin tokenizare datele sensibile sunt păstrate în seif, în timp ce în exterior sunt manipulate doar tokeni lipsiți de valoare.
- oferă date curățate pentru mediile de testare și dezvoltare;
- îmbunătățește capacitățile de colaborare între entități, prin furnizarea de date curățate de informații sensibile, pentru procesare și analiză ulterioară.

4.3 Potențialul de utilizare a token-izării

În momentul de față, token-izarea este utilizată preponderent în asigurarea unor sisteme securizate de date pentru plățile electronice cu cardul. Standardul PCI-DSS (PCI Security Standards Council, 2018) utilizează token-izarea doar pentru securizarea numărului contului primar – primary account number (PAN) și impune un set de cerințe privind sistemul și formatul

token-ului care este specific sectorului financiar. Cu toate acestea, tehnologia nu este limitată la aceste tipuri de date și are potențialul de a fi utilizată și pentru alte tipuri de date, cum ar fi: cod numeric personal, număr de cont bancar, nume, adresa de e-mail, număr de telefon, alte date sensibile. Tehnologia nu este restrictivă la nivelul sectorului plăților electronice cu cardul, putând să fie utilizată și în alte sectoare de activitate.

Din motive de securitate, în industria financiară, token-ii sunt construiți prin utilizarea unor funcții de generare a numerelor aleatoare. Cu toate acestea, în funcție de nevoile operaționale, se pot implementa algoritmi pentru construcția de token-i alfanumerici după modele predefinite, similare celor utilizate în mascarea datelor. Acest lucru este util pentru a asigura o integrare corectă a aplicațiilor cu alte sisteme. În acest fel, token-izarea poate fi utilizată pentru a înlocui mascarea, iar organizațiile vor putea oferi un mediu integrat, securizat, cu date curățate, în scopuri de testare și dezvoltare. Sistemul are de asemenea capacitatea de a permite utilizatorilor legitimi să acceadă la datele originale prin apelarea funcțiunilor de reconversie token - dată originală.

Sistemele de token-izare au avantaje față de criptare, prin reducerea costurilor cu investițiile, scăderea complexității sistemelor, minimizarea sarcinilor administrative, reducerea influenței asupra proceselor organizaționale. Specific pentru mediile de lucru moderne, bazate pe tehnologii cloud computing, token-izarea oferă suport avansat pentru munca colaborativă, mobilitatea ridicată, dinamica avansată a forței de muncă, oferind acces la informații în funcție de nivelul de acces al solicitantului.

Token-izarea nu este soluția perfectă pentru asigurarea securității datelor în sistemele moderne de cloud computing și vine cu dezavantaje, cum ar fi:

- nu este adecvată a fi utilizată intensiv pentru toate datele din organizație, acestea necesitând o scanare și filtrare prealabilă;
- performanța sistemelor care administrează baza de date a tokenilor din seif este critică pentru funcționarea întregului sistem. Dacă sistemul este utilizat la scară largă, bazele de date se extind rapid determinând creșterea timpului de reacție a sistemului, creșterea complexității sarcinilor administrative, creșterea dificultății sincronizării bazei de date distribuită în mai multe instanțe, ceea ce duce la o creștere a costurilor și o limitare a performanței sistemului;
- se bazează pe alte tipuri de măsuri pentru securizarea legăturii de comunicare între seiful de date și terminalele client;

Token-izarea oferă capabilități și poate înlocui, cu anumite limitări, sistemele clasice de obscurizare a datelor bazate pe criptare și mascare. Prin eliminarea doar a informațiilor sensibile din pachetele de date, ea poate fi utilizată în locul mascării, oferind aceleași capabilități ca cea din urmă. Pe de altă parte, pentru că este o funcție bijectivă și oferă posibilitatea utilizatorilor legitimi să acceseze datele sensibile, ea poate să fie utilizată în locul criptării. Concentrarea datelor sensibile în seiful de date restrânge amprenta de vulnerabilitate a datelor. Dispunerea acestuia într-o locație fizică aflată sub controlul organizației permite implementarea unor mecanisme și măsuri de securitate cu costuri financiare și umane reduse. Tehnologia oferă capabilități avansate specifice mediului cloud computing: dinamică ridicată a resursei umane, mobilitate ridicată, lucru în comun, viteză de procesare, conformitate cu reglementările privind stocarea datelor cu caracter personal.

4.4 Concluzii

În acest capitol am realizat o analiză a tehnicilor de obscurizare a informațiilor: criptarea, mascarea și tokenizarea. Am comparat aceste tehnici din mai multe puncte de vedere pentru a scoate în evidență spectrul de capabilități pe care fiecare tehnică îl posedă și avantajele oferite pentru mediile de manipulare a datelor.

Niciuna dintre tehnicile de obscurizare a datelor nu este răspunsul perfect la provocările moderne de securizare a datelor în platformele cloud computing cu care se confruntă organizațiile actuale. Fiecare dintre aceste tehnologii încearcă rezolvarea problemelor dintr-o

anumită perspectivă cu limitări particularizate în ceea ce privește investițiile dedicate, educarea utilizatorilor, impactul negativ asupra performanței proceselor organizației, alocarea de resurse pentru mentenanța sistemului etc.

Provocările pe care le aduc caracteristicile mediului informațional modern precum dinamică extinsă, necesitatea muncii în comun, acces la date din orice locație etc. necesită utilizarea unor tehnologii dinamice care să permită accesul la informații în funcție de natura solicitantului cu minim efort operațional. Token-izarea are avantaje care o recomandă pentru o utilizare mai largă în mediile informatice actuale. Ea reușește să asigure un cadru securizat de acces la date în funcție de calitatea solicitantului, cu impact minim asupra proceselor interne ale organizației și eficientizarea costurilor. Prin constrângerile pe care le impune forțează organizația să aplice o metodă eficientă de tratare a securității datelor, prin necesitatea identificării și clasificării informațiilor din cadrul ei.

5. Automatizarea obscurizării datelor în sisteme de prelucrare a informațiilor bazate pe tehnologii cloud computing

5.1 Obscurizarea datelor în mediul clasic actual

Datele reprezintă una dintre cele mai importante resurse ale organizațiilor moderne, iar modul în care acestea reușesc să le valorifice condiționează în mod critic atingerea obiectivelor stabilite. Protejarea datelor se constituie astfel, alături de alte procese precum culegerea, procesarea, curățarea, vizualizarea, transmiterea etc. ca elemente esențiale ale managementului informațional.

În mod tradițional, aceste procese au fost realizate manual, prin directa intervenție a omului. Motivele care au stat la baza acestui fenomen sunt determinate de factori precum: diversitatea formelor de reprezentare a informațiilor, diversitatea surselor, complexitatea limbajului uman, incapacitatea sistemelor tehnice de a se ridica la nivelul capabilităților intelectului uman etc. Astfel, și procesul de securizare a datelor s-a bazat pentru o lungă perioadă de timp exclusiv pe factorul uman. Dezvoltările tehnologice apărute au determinat încercarea de integrare a elementelor de tehnologie în fluxurile informaționale pentru obținerea unor beneficii, precum: transmiterea rapidă a datelor de la sursă la destinație, creșterea nivelului de confidențialitate a datelor, culegerea datelor etc.

Obscurizarea datelor este o parte componentă a procesului de securizare a datelor care presupune operațiuni de alterare a acestora în vederea ascunderii semnificației și imposibilității compromiterii informației, chiar dacă ajung în posesia unor entități neautorizate.

Procesul de obscurizare a datelor este format în principal din următoarele etape:

- analiza;
- clasificarea în conformitate cu valorile organizației și reglementările din domeniu;
- obscurizarea datelor pentru protejarea lor prin alterarea formei de reprezentare.

Complexitatea operațiunilor de identificare a informației și de apreciere a valorii acesteia pentru organizație au determinat ca dintre aceste etape primele două să se bazeze în mare parte pe intelectul uman, doar ultima integrând cu succes elemente tehnologice.

5.1.1 Importanța clasificării datelor

Clasificarea datelor este procesul de încadrare a acestora în diferite categorii, în funcție de anumite criterii (valoarea informației, domeniul de apartenență, locație, sensibilitate etc.) (Aggarwal, 2014). În domeniul managementului securității informaționale, clasificarea datelor este o etapă critică efectuată pentru minimizarea amprentei de vulnerabilitate și reducerea investițiilor în securizarea activelor informaționale. Astfel, prin gruparea datelor în categorii și identificarea unor măsuri de protecție a acestora, corespunzătoare sensibilității lor, se obțin mai multe beneficii, cum ar fi:

- limitarea costurilor cu protecția informațiilor - cu cât nivelul de clasificare a informațiilor este mai ridicat, cu atât complexitatea sistemelor care le procesează este mai mare și generează o creștere a costurilor. Prin clasificare se realizează limitarea acestor cheltuieli evitându-se utilizarea unor sisteme complexe pentru protecția unor date care nu necesită un nivel ridicat de securitate;
- îmbunătățirea nivelului de securitate și minimizarea riscurilor de compromitere a datelor prin aplicarea unor reguli de management corespunzătoare;
- alinierea la anumite standarde de protecție a datelor - la momentul actual există o serie de standarde și legi care reglementează modul de asigurare a securității anumitor tipuri de informații (PCI, HIPPA, SOX, FISMA, GDPR etc.) care reglementează modul de protecție, locația unde pot fi stocare, modul de acces etc. Prin clasificarea informațiilor se asigură premisele unei procesări corespunzătoare categoriei din care fac parte acestea;
- identificarea rapidă a apariției unor erori în sistemul de protecție și limitarea nivelului de compromitere - prin crearea unui mediu controlat se asigură doar accesul persoanelor legitime la datele la care acestea sunt autorizate. Monitorizarea accesului furnizează informații critice cu privire la identificarea existenței unor vulnerabilități și declanșarea procedurilor de limitare a extinderii compromiterii și la alte sisteme.

5.1.2 Limitări ale sistemelor actuale

Procesul clasic utilizat de organizații pentru clasificarea datelor se bazează în mare măsură pe utilizarea factorului uman. Astfel, se utilizează experiența, cunoștințele și un sistem de referință pentru analiza datelor, identificarea informațiilor și asignarea acestora la nivelul de clasificare corespunzător. La momentul de față, deși există capabilități tehnologice pentru prelucrarea automată a informațiilor, sistemele care au apărut au funcționalități strict limitate (filtre bayesiene de clasificare automată a unui mail în spam) sau aplicații de management al documentelor care se bazează pe factorul uman pentru realizarea clasificării. Utilizarea acestui proces are limitări considerabile. cum ar fi:

- supra-clasificarea – atribuirea, întregului pachet de date, nivelul cel mai înalt de clasificare al informațiilor conținute în pachet. Acest lucru determină imposibilitatea accesării legitime a informațiilor din pachet care au un nivel mai mic de clasificare (marketing, cercetare și dezvoltare, testare etc.);
- clasificarea incorectă datorită rezilienței scăzute a sistemului (decizia poate fi alterată din numeroase motive, precum: inexperiență, timp limitat, cantitate mare de date, motivație limitată, loialitate scăzută, stres, utilizarea principiului „better to be safe than sorry” etc.;
- creșterea nejustificată a cheltuielilor cu sistemele care prelucrează informații cu nivel ridicat de clasificare prin supra-clasificarea datelor;
- limitarea flexibilității și a performanței organizației;
- creșterea impactului asupra proceselor organizaționale din cauza dificultăților de integrare a diferitelor sisteme și oameni;
- limitarea vitezei de propagare a informației în cadrul organizației și creșterea timpilor de reacție a acesteia;
- limitarea performanței resursei umane prin impunerea efectuării unor sarcini adiționale care nu aduc valoare;
- creșterea costurilor cu mentenanța sistemelor informaționale, soluțiile de back-up și restaurare a datelor;
- imposibilitatea sistemelor manuale de a face față specificului mediului informațional actual, precum: viteza crescută de transfer, procesarea datelor în platforme online din exteriorul perimetrului organizației, creșterea traficului de date est-vest, cantități mari de date venite din medii nesigure;
- limitarea lucrului colaborativ în cadrul organizațiilor.

În lucrarea de față se propune un sistem automat de obscurizare a informației în care aportul uman este minim. Pentru maximizarea beneficiilor în ceea de privește costul,

accesibilitatea, reziliența, integrarea operațională, sistemul propus are la bază tehnologii cloud computing. În acest sistem analiza, clasificarea și obscurizarea informației se realizează utilizând algoritmi automați bazați pe algoritmi de învățare automată și prelucrare a limbajului natural.

5.2 Prelucrarea automată a datelor

5.2.1 Analiza și identificarea informației

Domeniul identificării informației – information retrieval reprezintă știința căutării și identificării unor materiale de formă nestructurată, care satisfac o cerere de informație (Christopher D. Manning, 2008). Procesul de căutare se realizează asupra conținutului unuia sau mai multor fișiere sau metadate, indiferent că acestea se află localizate într-o bibliotecă de fișiere sau sunt disponibile în Internet.

Identificarea informațiilor într-un mediu informațional reprezintă o provocare pentru un sistem informatic, întrucât există o mare diferență între modul de reprezentare a informației între om și mașină. În momentul conversiei datelor preluate din mediul exterior în format digital se efectuează mai multe transformări ale acestora. Astfel, procesul de transmitere a informației între cele două sisteme are de suferit, iar ulterior regăsirea informațiilor se realizează cu dificultate.

Cel mai utilizat tip de fișier pentru stocarea datelor este reprezentat de cel în care datele sunt stocate sub formă de text. Fișierele care stochează date sub formă de text beneficiază de avantajul că utilizează omul ca element de preprocesare a datelor și de reprezentare simbolistică a acestora. Astfel, conversia informației în date care să poată fi stocate de calculator se face de către om, după un algoritm cunoscut de acesta și utilizat ulterior și la procesul de regăsire. Din punct de vedere al prelucrării informației, acest tip de fișiere, spre deosebire cel video, imagine sau audio are și avantajul că în general necesită resurse computaționale mai reduse, fiind una dintre modalitățile fundamentale de reprezentare a informației.

5.2.2 Măsuri de bază pentru regăsirea informației

Cele mai importante aspecte ale regăsirii informației în fișiere text sunt legate de noțiunea de relevanță și de problematica aproximării căutării bazându-ne pe cuvinte cheie. Dacă prin utilizarea unui sistem de căutare a informației se returnează un număr de instanțe se pune problema aprecierii relevanței acelor instanțe în raport cu cererea de informație solicitată.
Următoarele sunt notații specifice sistemelor de identificare a informației:

- Relevant - reprezintă mulțimea tuturor instanțelor relevante față de interogare (Kent, 1955);
- Identificat - definește mulțimea tuturor instanțelor identificate ca și corespunzătoare de către algoritmul de căutare (Kent, 1955);
- |X| - numărul de instanțe din setul X;
- Pozitiv adevărat – reprezintă instanțe pozitive identificate corect;
- Negativ adevărat – reprezintă instanțe negative identificate corect;
- Pozitiv fals – reprezintă instanțe pozitive identificate greșit;
- Negativ fals – reprezintă instanțe negative identificate greșit.

5.2.3 Metode de identificare a informației

Metodele de identificare a informației se împart în două categorii principale: metode care realizează selecția informației prin compararea cu un anumit model și metode care oferă o ierarhizare a informației în funcție de anumite criterii de relevanță indicate.

5.2.3.1 Modelul Boolean

Modelul boolean este unul dintre cele mai vechi și mai simple modele de recuperare a informațiilor. Este bazat pe teoria seturilor și algebra booleană (Baeza-Yates, 1999). În acest model fiecare document este identificat ca un set de termeni index. Termenii de index sunt elemente din pachetul de informație care sunt definitorii pentru stabilirea semnificației informației (cuvinte, indicatori, indici numerici etc.). Interogarea este o expresie booleană de

forma: „cuvânt1 AND cuvânt2”, „cuvânt1 OR cuvânt2”, „cuvânt1 AND cuvânt2 NOT cuvânt3”. Sistemul de identificare a informației construit în această paradigmă va executa interogări utilizând expresia booleană definită și va returna toate pachetele de informație care satisfac relația. Algoritmul și complexitatea unor astfel de sisteme este simplă și sunt relativ ușor de implementat, dar au dezavantajul de a nu fi potrivite în cazul în care utilizatorul nu cunoaște bine formula sau setul de date din care vrea să selecteze informația.

5.2.3.2 Modelul vectorial

Modelul bazat pe vectori încearcă rezolvarea problemei de asociere parțială, precum și inexistența unei metode de ierarhizare a instanțelor returnate. În acest model, pachetele de informație sunt reprezentate cu un vector de indecși.

$$\overrightarrow{v_j} = \{p_{1j}, p_{2j}, \dots, p_{nj}\} \quad (5)$$

unde n este numărul total de indecși, iar p_{1j} reprezintă ponderea unui index. Astfel, spre deosebire de modelul boolean care ține cont doar de prezența/ absența indecșilor, acest model calculează relevanța instanțelor și ierarhizează rezultatele în funcție de un model mai complex de prezență al acestora.

Similaritatea este maximă când unghiul dintre cei doi vectori este zero, adică atunci când vectorii coincid. Pachetele de informație returnate sunt cele pentru care se depășește un anumit prag de similaritate, nivelul pragului putând depinde de vectorul de căutare. Prin utilizarea acestui tip de paradigmă se realizează un optim de potrivire, nefiind necesară potrivirea exactă între pachetul de informație și vectorul de căutare. Ierarhizarea se realizează în funcție de rezultatele obținute la calcularea similarității.

5.2.3.3 Modelul probabilistic

În modelul probabilistic problematica regăsirii informațiilor este abordată în funcție de probabilitatea ca pachetul de informație să fie relevant față de cererea făcută (Baeza-Yates, 1999). Se presupune că fiecare pachet de informație are o relevanță independentă față de cererea de căutare.

Principiul de ierarhizare probabilistică este următorul: „Dacă răspunsul sistemului de recuperare a referințelor la fiecare cerere este un clasament al documentelor în colecție, în ordinea descrescătoare a probabilității de relevanță pentru utilizatorul care a prezentat cererea, unde probabilitățile sunt estimate la fel de precis posibil pe baza oricăror date care au fost puse la dispoziția sistemului pentru acest scop, eficacitatea generală a sistemului pentru utilizatorul său va fi cea mai bună care se poate obține pe baza acestor date.” (Robertson, 1977)

5.2.3.4 Modelul bazat pe logica fuzzy

Modelele prezentate până acum au presupus că termenii indecși sunt independenți unul față de celălalt. Prin asocierea unui pachet de informație cu un set de termeni independenți se pierde din mesajul purtat, iar rezultatele obținute la căutări au niveluri reduse de relevanță. În modelul bazat pe teoria fuzzy, fiecare termen al interogării definește un set de pachete de informație într-o anumită pondere. Astfel, fiecărui pachet de informație p, i se asociază un grad de relevanță la o anumită interogare.

Se calculează suma indicilor de corelare pentru fiecare index al vectorului de căutare față de fiecare element de informație din pachet. Formula asigură că ori de câte ori apare un element de informație, care este puternic relaționat de un element index de căutare atun ci și relevanța este ridicată.

5.2.4 Procesarea limbajului natural – natural language processing (NLP)

Una dintre limitările istorice ale utilizării sistemelor informatice pentru clasificarea automată a informațiilor este legată de complexitatea și multiplele variații ale formelor acestora. Indiferent că este vorba de text, grafică sau sunet informația poate lua o formă variată de reprezentări, combinări, alterări, nuanțe care depind de o serie largă de factori dificil de

cuantificat (educație, cultură, canale de comunicație, etc.) și care pot altera în mod radical mesajul transmis.

NLP este o ramură a științei datelor care presupune efectuarea unor procese sistematice de analiză, înțelegere și derivare a informațiilor din limbajul natural uman. Algoritmii din această clasă sunt aplicați asupra limbajului uman materializat sub formă de text, această formă de reprezentare a limbajului fiind una dintre modalitățile cele mai utilizate și accesibile sistemelor informatice. Folosind NLP și componentele sale se pot organiza cantități mari de date text, se pot automatiza numeroase sarcini și se pot rezolva o gamă largă de probleme, cum ar fi: extragerea automată a ideilor principale, traducerea automată, recunoașterea numelui entității, extracția relațiilor, analiza sentimentului, clasificarea datelor etc.

Deoarece textul prezintă un nivel ridicat de nestructurare a datelor, sunt prezente în el numeroase tipuri de zgomot. Este necesară efectuarea unei operații de preprocesare a datelor înainte de începerea efectivă a prelucrării acestora. Acest proces presupune efectuarea anumitor operațiuni care realizează curățarea și standardizarea textului și îl pregătesc pentru analiză. În figura 5.1 este prezentată arhitectura procesului de curățare a datelor.

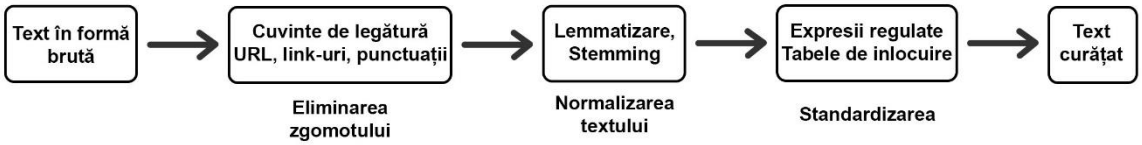

Fig. 5.1 Fluxul de curățare a datelor

5.3 Învățarea automată

Învățarea automată este un domeniu al inteligenței artificiale care urmărește dezvoltarea capacității unui sistem informatic de a efectua o sarcină, fără a fi programat în mod expres să o execute. În contextul analizei de text, aceasta reprezintă dezvoltarea, prin utilizarea unui set de instrumente, a capacității unui sistem de a identifica modele, părți ale discursului, concepte folosite, a sentimentului, precum și a altor aspecte ale textului.

Deși învățarea automată este un domeniu al informaticii, aceasta diferă de abordările computaționale tradiționale. În calculul tradițional, algoritmii sunt seturi de instrucțiuni programate explicit, utilizate de computere pentru a calcula sau a rezolva probleme. Numeroase abordări de creare a algoritmilor de învățare automată și de reprezentare numerică a cunoașterii se bazează pe încercarea de emulare a comportamentului uman, rezultând un domeniu multidisciplinar din care fac parte: informatica, biologia, neurologia, psihologia, teoria informației, probabilități și statistică, teoria complexității informaționale, teoria deciziei etc.

Algoritmii de învățare a mașinilor permit sistemelor informatice să se antreneze pe intrări de date și să utilizeze analize statistice pentru a obține valori de ieșire care se încadrează într-un anumit interval. Învățarea trebuie să ducă la crearea de "reguli" care să ajute soluționarea unor probleme, dintr-un spațiu mai larg de cunoaștere decât cel care s-a utilizat pentru procesul de învățare.

5.3.1 Învățarea supervizată

Învățarea supervizată este un tip de învățare automată care se bazează pe un set predefinit de exemple de probleme rezolvate și încearcă construirea unei funcție de evaluare (șablon) care să ofere posibilitatea rezolvării unor noi probleme din aceeași categorie. Etapa inițială, denumită și etapa de antrenare a sistemului este faza în care sistemul este expus la aceste probleme rezolvate. Caracterul de supervizare este determinat de faptul că, în etapa de antrenare a sistemului, setul de probleme este oferit împreună cu clasa corespunzătoare.

Setul de date de antrenament este reprezentat de o mulțime de perechi atribut-valoare (x,y), unde x este problema iar y este categoria căreia îi aparține problema.

Scopul etapei de învățare este introducerea de date în sisteme pe baza cărora să se construiască funcția f(x). Antrenarea se oprește când eroarea sistemului este sub un nivel maxim admis.

5.3.2 Învățarea nesupervizată

Învățarea nesupervizată este acel tip de învățare în care se utilizează date pentru antrenarea sistemului, dar nu se oferă răspunsurile corecte. În aceste sisteme scopul nu este definit anterior, iar algoritmul este lăsat singur să identifice concepte posibile și modele încă necunoscute. Acest tip de învățare este utilizat pentru analizarea unor date despre care nu se cunosc răspunsurile, întrucât nu pot fi observate, este imposibilă măsurarea lor sau ele nu există.

Un algoritm de învățare nesupervizată construiește concepte pentru a clasifica datele, le evaluează și le dezvoltă pe cele pe care le consideră "importante". Conceptele sunt considerate importante dacă acoperă o parte din date, nefiind obligatoriu să le acopere pe toate. Învățarea nesupervizată permite identificarea unor concepte complet noi, plecând de la date cunoscute. Procesul de creare de noi concepte are limitări în ceea ce privește numărul și relevanța acestora, întrucât acest gen de algoritmi nu pot învăța noi metode de a crea și evalua concepte. Obținerea unor rezultate superioare necesită modificarea algoritmului, în ceea de privește complexul de operații pentru crearea de noi concepte, precum și regulile euristice de evaluare a acestora. (Nillson N., 1998).

5.3.3 Învățarea cu întărire

Este domeniul învățării automate care studiază algoritmii și tehnicile care încearcă să-și modifice retrospectiv modelul de lucru pentru a îmbunătăți rezultatele. Pentru a realiza acest lucru, se utilizează mecanisme pentru a „răsplăti" sistemul în funcție de cât de mult se apropie de rezultatul corect. Algoritmii învățării cu întărire încearcă să afle ce trebuie să facă pentru a maximiza aceste recompense, iar acest proces este realizat fără intervenții din exterior. Acest feedback este singura metodă de învățare a sistemului, de a se autoregla pentru îmbunătățirea rezultatelor.

Acest lucru face ca sistemele bazate pe învățarea cu întărire să aibă un grad de complexitate mai ridicat. În sistem nu se mai introduc direct informații despre cum să se corecteze, el având instrumente să aprecieze dacă rezultatul obținut se apropie sau nu de optim. Mai mult, feedback-ul nu apare întotdeauna, necesitând ca sistemul să posede instrumente pentru a se autoregla în vederea îmbunătățirii modelului (MacKey David J., 2003). Învățarea cu întărire este utilă în condițiile în care nu există date de antrenament, nu se pot identifica cu precizie rezultatele valide sau eronate, fie din cauza complexității reprezentaționale, fie din cauza inexistenței unor informații de încredere (Nillson N., 1998). Se dispune însă de posibilitatea validării unei soluții obținute de sistem, chiar și doar prin comparația cu alte soluții posibile.

5.4 Prezentarea modelului propus

Luând în calcul limitările identificate la sistemul clasic de procesare a informațiilor, provocările organizațiilor moderne specifice mediului informațional cloud computing precum și dezvoltările tehnologice în domeniu în acest capitol am propus un nou sistem de obscurizare a datelor organizației. Acest model se bazează pe sisteme automate de analiză, învățare și clasificare a datelor de intrare și apoi de selecție și executare a procedurilor de obscurizare a informațiilor.

Rolul elementului uman în cadrul acestui sistem este alocat doar procesului decizional. Responsabilitatea executării muncii repetitive de clasificare a informațiilor este atribuită sistemului automat, elementul uman fiind necesar în momentul în care se întâlnesc date care sunt în afara spectrului de cunoștințe, iar sistemul trebuie antrenat/reantrenat.

Sistemul este alcătuit din două module principale: clasificarea automată a datelor prezentat în figura 5.2 și obscurizarea datelor prezentat în figura 5.3. Elementul de intrare în sistem este un pachet de date care trebuie analizat, iar ieșirea este un obiect obscurizat. În funcție

de nivelul de clasificare a informațiilor conținute în pachetul de date sistemul va efectua automat analize, decizii și prelucrări, iar la ieșire obiectul va fi criptat, mascat, token-izat sau nemodificat.

5.4.1 Modulul de clasificare a datelor

Rolul acestui modul este acela de a realiza clasificarea automată a datelor de intrare. El este reprezentat schematic în figura 5.2. Obiectul de date inițial constă în informații text, dar poate fi extins cu conținut imagine, audio sau video prin adăugarea unor componente suplimentare. De asemenea, pentru îmbunătățirea capabilităților acestuia, îi poate fi adăugată și o componentă de analiză a metadatelor asociate (cine a trimis mesajul, cine este destinatarul, ce canal de comunicație a fost utilizat, care este calitatea sursei și a destinatarului, alți indicatori).

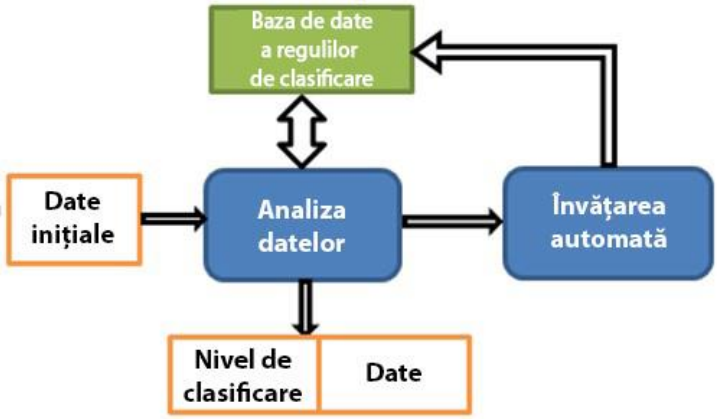

Fig. 5.2 Modulul de clasificare automată a datelor

La ieșire, acest modul va returna nivelul de clasificare a informației din cadrul pachetului de date introdus ca variabilă de intrare. Modulul este format din două componente prezentate în continuare.

5.4.1.1 Componenta de analiză a datelor

Această componentă din cadrul modulului de clasificare automată a datelor este responsabilă cu analiza datelor de intrare și atribuirea nivelului corespunzător de clasificare. În cadrul ei se execută următoarele acțiuni:

- preprocesarea;
- normalizarea;
- standardizarea;
- secvențierea;
- analiza datelor și compararea cu baza de cunoștințe;
- decizia cu privire la atribuirea nivelului de clasificare;
- declanșarea procesului de actualizare a bazei de date.

Modelul are la bază concepte specifice tehnologiilor de procesare a limbajului natural, astfel încât etapele de preprocesare, normalizare, standardizare și secvențiere sunt etape specifice acestor tipuri de algoritmi și au rolul de a pregăti datele pentru procesarea propriu - zisă. Pentru stabilirea ipotezelor de clasificare sistemul execută operațiuni de analiză a datelor, în raport cu un set de reguli stabilite, în baza de date cu reguli, denumită și baza de date a cunoștințelor.

Baza de date a cunoștințelor este formată dintr-un set de indicatori specifici și nivelul de clasificare corespunzătoare (informații financiare, nume, informații despre misiunea organizației, modele de date, metadate etc.). Baza de data a cunoștințelor este dezvoltată și actualizată cu ajutorul componentei de învățare automată prezentată în secțiunea 5.4.1.2.

Sistemul încearcă clasificarea datelor în fiecare dintre clase, returnând o anumită eroare. Clasa pentru care eroarea este minimă este clasa în care este cel mai probabil să se regăsească informația conținută în pachetul de date. Dacă eroarea este sub un anumit nivel stabilit și acceptat de organizație, atunci clasificarea se consideră corectă, iar datele sunt transmise către modulul de obscurizare. În cazul în care eroarea este mai mare decât nivelul stabilit, atunci este solicitată intervenția umană pentru a asista sistemul.

5.4.1.2 Componenta de creare a bazei de date a cunoștințelor

Pentru minimizarea interacțiunii umane cu sistemul, baza de date a cunoștințelor este dezvoltată utilizând algoritmi specifici învățării automate. Din cauza faptului că se cunoaște foarte bine de dinainte modelul datelor și nu este necesară crearea unor concepte noi s-a utilizat pentru sistemul automat de învățare paradigma învățării supervizate. Astfel, suportul uman este necesar în etapa inițială, pentru construirea bazei de date a cunoștințelor inițiale ale sistemului, dar și atunci când eroarea de clasificare depășește un prag acceptat.

Etapa inițială este reprezentată de dezvoltarea bazei de date cu cunoștințe și de inițializare a sistemului, de către o echipă de specialiști care cunoaște foarte bine mediul informațional al organizației, valorile acesteia, dar și capabilitățile și modul de funcționare a sistemului. Echipa trebuie să alcătuiască o bibliotecă cu tipurile de informații din cadrul organizației, să organizeze un sistem de clase și să atribuie fiecărei informații clasa corespunzătoare. De asemenea, ea trebuie să introducă în sistem aceste informații, astfel încât acestea să reprezinte baza de date cu cunoștințe în funcție de care sistemul se va raporta pentru clasificarea următoarelor pachete de date primite.

Această etapă este critică pentru funcționarea corectă a sistemului și se urmărește asigurarea implementării tehnice corecte a valorilor organizației. Baza de date a cunoștințelor este particulară pentru fiecare organizație în parte, ea depinzând de domeniul de activitate, cultura organizațională, specificul mediului operațional, scara valorilor etc., astfel încât aceleași informații pot avea niveluri de clasificare diferite în organizații diferite.

Intervenția umană asupra bazei de date a cunoștințelor mai este necesară în momentul în care eroarea de clasificare este mai mare de o anumită valoare sau în momentul în care se produce o modificare a valorilor organizației. În primul caz înseamnă că sistemul a identificat, în pachetul de date, informații noi despre care nu are o experiență anterioară și nu este în măsură să le clasifice într-una dintre clase, în mod corespunzător. Al doilea caz în care se impune intervenția umană este acela al actualizării bazei de date a cunoștințelor datorită unor modificări apărute în mediul organizațional: modificarea claselor, modificarea unor activități, modificări în legislație etc. Intervenția externă este necesară, întrucât sistemul nu beneficiază de senzori pentru preluarea acestor modificări ale mediului organizațional și nu are posibilitatea actualizării autonome a bagajului de cunoștințe.

5.4.2 Modulul de obscurizare a datelor

Modulul, reprezentat în figura 5.3, are rolul de alterare a formei datelor, prin aplicarea de proceduri și algoritmi diferiți, în funcție de nivelul de clasificare identificat de către modulul anterior. Pentru fiecare dintre categoriile de clasificare a datelor definite trebuie dezvoltat un set de proceduri și algoritmi care să asigure obscurizarea datelor în conformitate cu necesitățile mediului informațional al organizației.

Elementele de bază sunt modulele de criptare, token-izare sau mascare dar, pot fi stabilite instrumente suplimentare, cum ar fi: lansarea unei mașini virtuale pentru prelucrarea datelor într-un mediu independent, stabilirea unor legături de comunicare securizate cu echipamentele de stocare a datelor, configurarea controlului accesului la date etc.

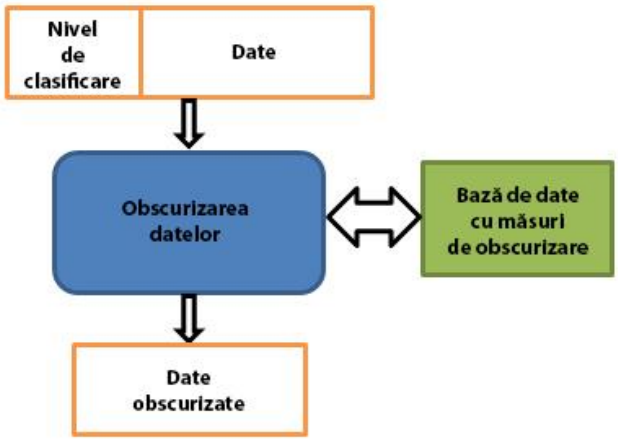

Fig. 5.3 Modulul de obscurizare a datelor

Baza de date cu regulile de obscurizare este una modulară și permite actualizarea și schimbarea în funcție de modificările apărute în politica de securitate a organizației.

5.4.3 Implementarea modelului

Sistemul propus a fost implementat într-un mediu cloud computing, folosind capacitatea de procesare a limbajului natural (NLP) a modulului de calcul Watson oferit pe platforma IBM Bluemix. Întrucât sistemul este valabil doar pentru un set limitat de dicționare s-a ales cel specific pentru limba engleză.

Pentru efectuarea testării a fost creată o organizație ipotetică care activează în domeniul militar și care trebuie să proceseze date din trei categorii de clasificare: "unclassified", "confidential" și "secret". Pentru acesta s-au creat cele trei clase corespunzătoare celor trei categorii de clasificare a informației (figura 5.4):

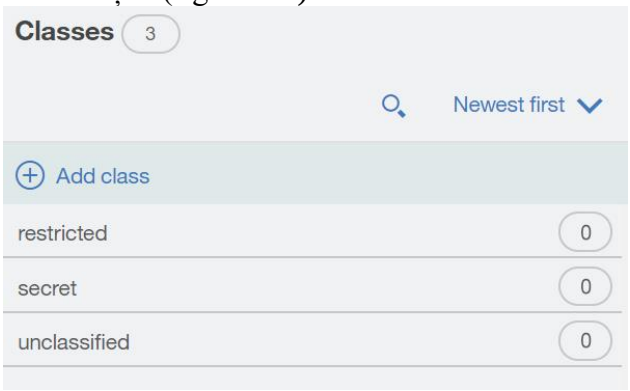

Fig. 5.4 Definirea claselor

Următoarea etapă este aceea a creării bazei de date a cunoștințelor care să stea la baza procesului de clasificare automată a informațiilor. Întrucât sistemul se bazează pe învățarea supervizată, s-a realizat o clasificare manuală a informațiilor organizației reprezentative pentru fiecare clasă. Această parte este una critică pentru întregul proces, deoarece pe baza "experienței" definite, sistemul va efectua procesul de clasificare.

Pentru aceasta s-a folosit un dicționar de cuvinte și expresii care se consideră relevante pentru activitatea organizației și care identifică valorile acesteia. Pentru clasa "unclassified" care reprezintă informațiile cu cel mai mic grad de clasificare se consideră că acestea nu trebuie obscurizate, întrucât pot fi accesate de către orice persoană din interiorul și exteriorul acesteia. Pentru această categorie, care este și cea mai largă, s-a identificat un set de 700 elemente.

Clasa "restricted" conține informații care sunt specifice mediului operațional al organizației și trebuie să fie cunoscute numai de o parte din membrii acesteia. În această categorie s-au identificat 220 elemente. Tot din această categorie fac parte și informațiile confidențiale cum ar fi coduri CNP, adrese, numere de cont, la care accesul trebuie asigurat doar unor anumite categorii de persoane.

Clasa "secret" conține informații de nivel strategic extrem de valoroase pentru organizație care trebuie să fie cunoscute doar de către un număr extrem de limitat de persoane din cadrul organizației. Din această clasă s-au identificat un număr de 80 de elemente.

După identificarea informațiilor, acestea au fost introduse în baza de date a cunoștințelor, după cum se poate observa din figura 5.5.

Fig. 5.5 Popularea claselor

Sistemul este capabil să învețe din experiențele întâlnite, dar pentru ca acesta să își actualizeze baza de date cu informații noi și să-și reantreneze clasificatorul este necesară asistența umană pentru validarea datelor. Lucrul acesta va fi verificat în faza de testare a funcționalității.

Modulul de obscurizare a informațiilor execută proceduri de alterare a conținutului pachetului de date în funcție de nivelul de clasificare a acestora. Pentru realizarea acestui lucru s-au definit următoarele modalități de obscurizare acceptate de organizație:

- Pentru informațiile din clasa "secret" se va utiliza criptarea simetrică;
- Pentru informațiile din clasa "restricted" se va utiliza mascarea și tokenizarea;
- Pentru informațiile din clasa "unclassified" nu se vor altera datele.

Prin alegerea acestor algoritmi de obscurizare se asigură o creștere graduală a costurilor sistemelor de asigurare a securității datelor corespunzătoare cu valoarea informației.

5.4.4 Dezvoltarea interfeței cu utilizatorul

Pentru realizarea interacțiunii utilizatorului cu aplicația de obscurizare a datelor am dezvoltat o interfața bazată pe tehnologii web – figura 5.6. Acesta poate fi accesată prin utilizarea unui browser iar apelarea serviciilor de clasificare se face într-un mod transparent utilizatorului.

Sistemul propus are capacitatea de a fi integrat în sistemul organizațional ca o aplicație, un serviciu sau ca un nivel transparent de securitate, prin dezvoltarea unor API-uri specifice. Includerea cerințelor de facilitare a utilizarea a aplicației și de utilizarea a unor protocoale pentru integrarea facilă cu arhitecturile cloud computing va asigura din faza de cercetare/proiectare a produsului va asigura o integrare ușoară în cadrul infrastructurii IT existente, cu costuri financiare reduse și un impact negativ minim asupra proceselor organizației.

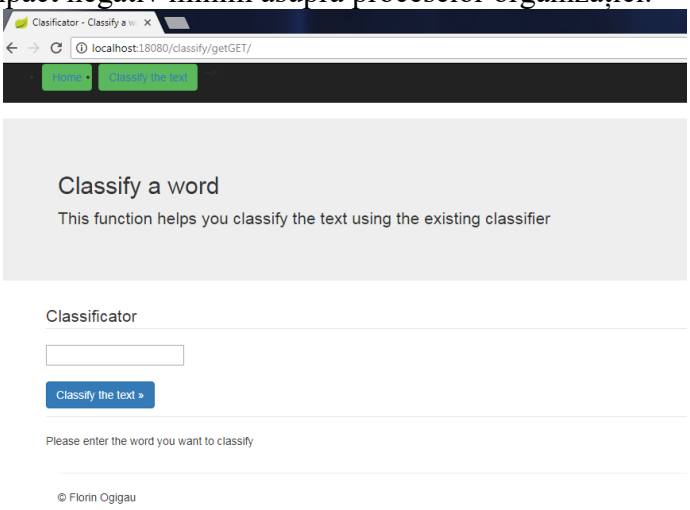

Fig. 5.6 Interfața aplicației

5.4.5 Testarea funcționalității sistemului

În etapa de testare a sistemului s-au ales pachete de date care conțineau informații din diferite clase care au fost utilizate pentru efectuarea de interogări. S-a considerat ca pragul de 0,05 este eroarea maximă acceptată de organizație pentru clasificarea informației. Nivelul acceptat al erorii trebuie stabilit de către organizație și va fi un compromis între avantajele sistemului și costurile construirii și exploatării acestuia.

În prima etapă s-au introdus cereri de clasificare în sistem despre care acesta fusese antrenat anterior. Pentru aceste probe, pentru care sistemul a avut deja o "experiență" anterioară (figura 5.7), răspunsul a fost returnat cu o eroare de 0,01 și 0,02. Eroare returnată este sub pragul de 0,05 și deci se poate trage concluzia că procesul de clasificare a fost realizat corespunzător.

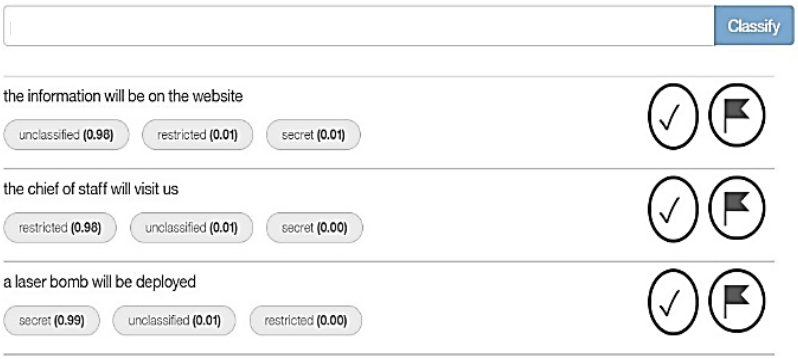

Fig. 5.7 Procesul de clasificare pentru date antrenate

În etapa a doua de testare s-au introdus cereri de clasificare a unor date despre care sistemul nu avea o experiență anterioară (figura 5.8). În acest caz, sistemul a returnat o eroare maximă de clasificare de 0,35, eroare care este mai mare decât pragul acceptat de către organizație.

Fig. 5.8 Procesul de clasificare pentru date neantrenate

Această eroare arată importanța antrenării corespunzătoare a sistemului și erorile mari pe care acesta le dă atunci când procesul de învățare nu este efectuat corespunzător. Pentru reducerea acestei erori este necesară intervenția umană și introducerea noii informații în baza de date cu cunoștințe. După efectuarea acestui pas, la o nouă solicitare de clasificare a datelor, se obțin rezultatele din figura 5.9:

Fig. 5.9 Reclasificarea informației

De această dată rezultatele clasificării au eroarea zero, deoarece informația pentru care s-a solicitat clasificarea este chiar informația utilizată pentru antrenarea clasificatorului.

5.5 Analiza de oportunitate a sistemului

În afară de evaluarea funcționării sistemului, am considerat necesară și efectuarea unei analize pentru evaluarea utilității acestuia, în vederea relevării beneficiilor pe care acest sistem le oferă mediului de securitate al unei organizații.

Procesul de evaluare a eficienței investițiilor în domeniul securității este unul dificil (Cioacă, 2015), din cauza mai multor factori precum:

- evaluarea valorii reale a informațiilor;
- estimarea probabilităților de apariție a evenimentelor de încălcare a securității;
- cuantificarea pierderilor în unitățile financiare;
- evaluarea descurajării atacatorului etc.

Evaluarea performanțelor sistemului propus s-a făcut printr-o analiză comparativă cu sistemul clasic de obscurizare a informațiilor, cel de-al doilea fiind cel mai folosit în organizațiile actuale. Analiza a fost efectuată pe două direcții:

- prima a fost aceea de a calcula și compara costurile financiare totale ale instalării și utilizării sistemelor;
- cea de-a doua a fost aceea de a dezvolta o analiză de risc comparativă între cele două sisteme care vizează să compenseze limitările procesului de cuantificare a indicatorilor de securitate.

5.5.1 Analiza de cost

Analiza comparativă a costurilor sistemelor de obscurizare a datelor, automat și clasic, constă în compararea sumei costurilor pentru modulele de clasificare și de obscurizare ale celor două sisteme. Deoarece, în ambele sisteme, modulele de obscurizare utilizează în mare măsură elemente tehnologice (criptare, mascare, token-izare) am considerat că aceste costuri sunt aproximativ egale în ambele cazuri.

Pentru comparație, am considerat sistemul automat ca fiind compus din echipamente hardware și produse software, în timp ce pentru sistemul clasic am echivalat efortul angajaților cu munca unei persoane care efectuează doar sarcini de clasificare a datelor întreaga zi lucrătoare (8 ore). În tabelul 5.1 am calculat coeficientul relativ de coordonare (k) pentru a identifica raportul între costurile sistemului bazat pe om și cel automat. Am luat în considerare următoarele costuri principale pentru sistemul automat: costul cu echipamentele hardware, costul cu licența software, costul de antrenare a sistemului, costul chiriei pentru spațiu, costul mentenanței. Pentru sistemul manual am luat în calcul următoarele costuri principale: costul cu salariul, costul cu materialele necesare, costul chiriei, costul pregătirii operatorilor, costul manipulare și stocare a documentelor.

Prin prelucrarea datelor primare am obținut următoarele rezultate:

Tabel 5.1 Coeficientul relativ de coordonare

T (luni)	K manual/automat
0	0.185
1	0.533
2	1.124
3	2.740
4	2.748
5	2.751

Din tabelul 5.1 se observă că, în primele două luni de funcționare, costurile sistemului automat de clasificare sunt mult mai mari decât cele ale sistemului manual. Acest lucru se datorează în mare măsură faptului că implementarea sistemelor automate necesită investiții inițiale mai mari în activele tehnologice software și hardware. O altă diferență este aceea că, pentru sistemele automate activitatea umană în faza de implementare și învățare are un grad mai mare de complexitate și este mai costisitoare decât cea pentru sistemele clasice. Începând cu luna a doua, costurile pentru funcționarea sistemului automat sunt aproximativ egale sau mai mari decât costurile corespunzătoare sistemului manual.

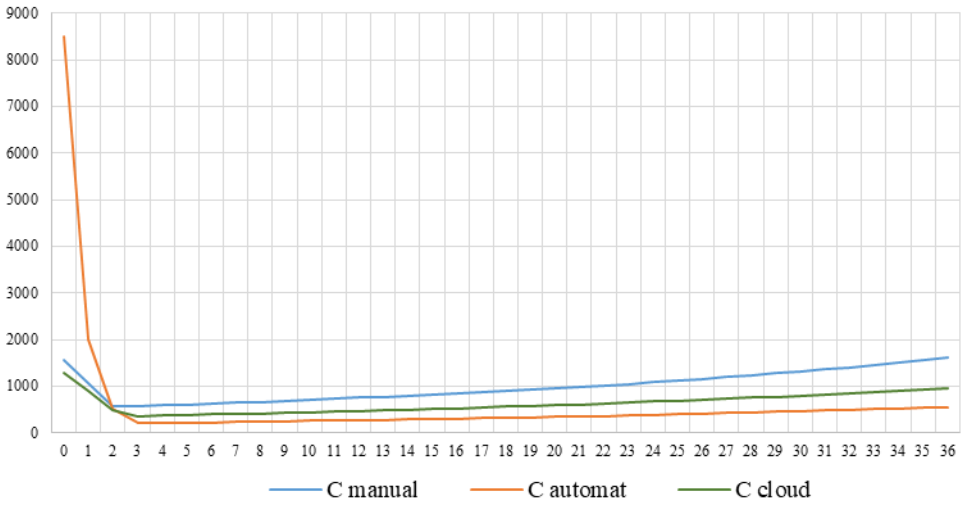

Fig. 5.15 Evoluția comparativă a costurilor pentru sistemul manual, automat și cloud computing pentru o perioadă de 3 ani

În continuare am realizat o prognoză pentru primii trei ani de lucru/funcționare și am realizat o reprezentare vizuală a evoluției celor două tipuri de costuri, așa cum se poate observa în graficul din figura 5.15.

Utilizarea unui sistem clasic pentru efectuarea clasificării datelor este eficientă numai pentru primele două luni, după care este mult mai eficient să se utilizeze un sistem automat. Reducerea costurilor CAPEX, corespunzătoare implementării inițiale a sistemului automatizat în cadrul unei organizații, poate fi făcută prin implementarea sistemului de clasificare a datelor într-o arhitectură cloud computing IaaS sau SaaS.

Această diferență a costului sistemului automatizat este mult mai evidentă atunci când crește volumul de muncă. În organizațiile mari, necesarul cu clasificarea datelor este mai ridicat decât capacitatea unei persoane, așa cum am apreciat în faza inițială. În aceste organizații sunt necesare resurse suplimentare (umane + materiale), ceea ce duce la o creștere rapidă a costurilor. Sistemul automat poate susține mai eficient acest tip de muncă suplimentară.

Creșterea cantității de date care urmează a fi clasificată poate fi gestionată ușor prin redimensionarea sistemului, pentru a face față unei puteri de calcul suplimentare necesare. Considerații privind capabilitățile de scalare trebuie avute în vedere încă din faza de proiectare a acestuia. Impactul costului creșterii necesarului de putere computațională poate fi minimizat, în soluția bazată pe arhitectura cloud computing, prin simpla trecere la un plan de serviciu superior. După efectuarea calculelor pentru această situație, am obținut graficul din figura 5.16.

Estimând, din luna a 13-a, o creștere a volumului de muncă echivalentă cu volumul de muncă a 10 persoane, am calculat din nou coeficientul relativ de coordonare (k) obținând: $k_{h/m}$ = 27.197. Astfel, costul pentru noul sistem manual de clasificare este aproximativ de 27 de ori mai mare decât costul pentru utilizarea unui singur sistem automat redimensionat.

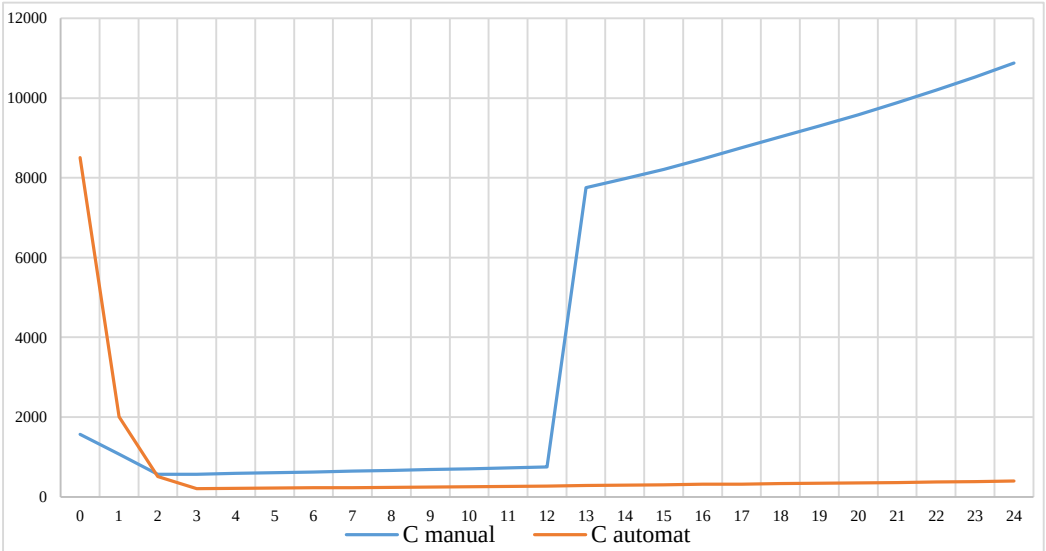

Fig. 5.16 Evoluția comparativă a costurilor pentru sistemul manual și automat când volumul de muncă crește

O altă analiză care scoate în evidență diferența dintre costurile celor două sisteme este analiza comparativă a costurilor cumulate. Am realizat o astfel de analiză comparativă a costurilor pentru trei cazuri: volumul de muncă necesar clasificării este echivalent cu volumul de muncă al unei persoane, volumul de muncă necesar clasificării este echivalent cu volumul de muncă a două persoane și volumul de muncă necesar clasificării este echivalent cu volumul de muncă a trei persoane.

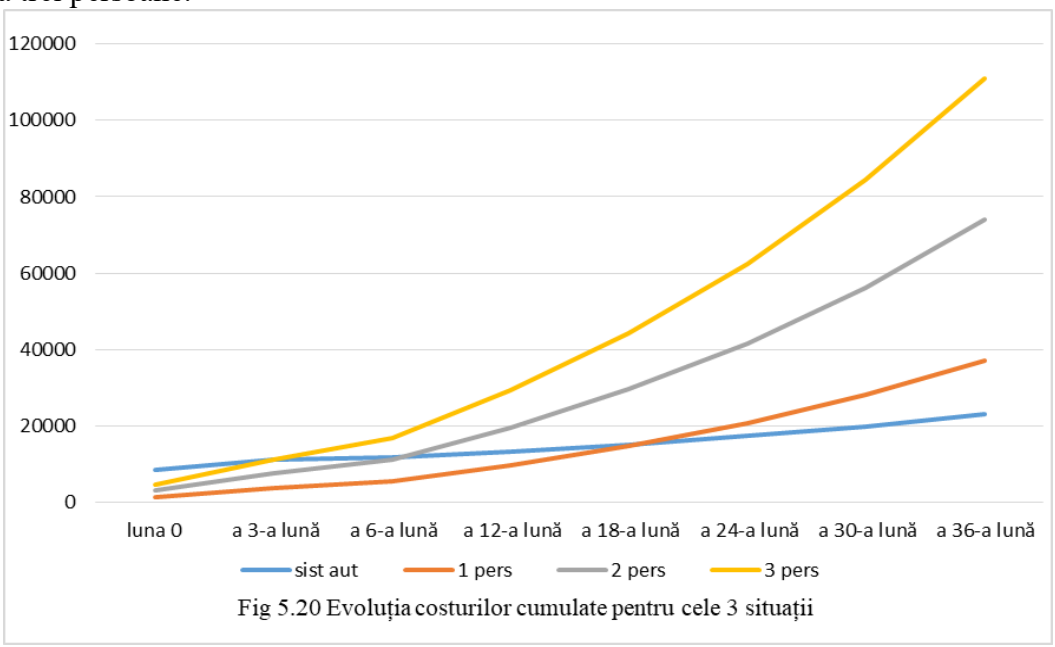

Fig 5.20 Evoluția costurilor cumulate pentru cele 3 situații

Astfel, pentru un sistem cu un volum de muncă echivalent cu cel efectuat de o persoană, costurile sistemului manual devin mai mari decât cu cel automat după luna nouăsprezece. De asemenea, pentru un sistem cu un volum de muncă echivalent cu cel efectuat de două persoane costurile sistemului manual devin mai mari după șapte luni de exploatare, iar pentru un sistem cu un volum de muncă echivalent cu cel efectuat de trei persoane costurile sistemului manual devin mai mari după doar trei luni de exploatare. Situația comparativă a acestor costuri este prezentată grafic în figura 5.20.

Se poate concluziona astfel că, pe termen lung, utilizarea unui sistem automat de obscurizare a informațiilor are costuri mai scăzute decât utilizarea unui sistem manual.

Deși inițial un sistem automat de obscurizare a informațiilor presupune investiții mai ridicate, totuși din cauza costurilor necesare funcționării, de la un moment dat costurile totale ale

sistemului automat vor deveni mai mici decât ale sistemului manual. Momentul în care se petrece acest lucru depinde în principal de volumul de informație prelucrat de organizație. Astfel, cu cât volumul de date este mai mare, cu atât momentul critic este mai aproape de timpul de dare în funcțiune.

5.5.2 Analiza de risc

Pentru a compensa limitările modelului financiar, în analiza securității sistemului, am realizat în continuare o analiză comparativă a managementului riscului de securitate pentru cele două sisteme. Am analizat astfel, modul în care cerințele privind securitatea datelor (Panmore Institute, 2016) sunt administrate în ambele sisteme. Am inclus în această analiză o serie de indicatori precum flexibilitatea, subiectivitatea, scalabilitatea, reziliența, factori operaționali etc. care sunt dificil de cuantificat financiar, dar care au un impact semnificativ asupra nivelului de asigurare a securității datelor și deci a gradului de acceptanță a acestui model în cadrul unei organizații.

Pentru sistemul manual trebuie luate în considerare elemente care influențează modul în care sistemul (lucrătorul) îndeplinește sarcinile: rutină, plictiseală, lipsa motivației, stresul, oboseala, capacitatea redusă de muncă din cauza bolii, lipsa stimulentelor pozitive, frica de a fi penalizat, lipsa de implicare în muncă, indisciplina, indiferența, lipsa de experiență, imposibilitatea de a respecta standardele și procedurile existente, neputința de a se adapta la noile realități, lipsa timpului suficient pentru procesarea informațiilor, neconcordanța dintre obiectivele personale și obiectivele organizației, lipsa de comunicare între el și superior, lipsa unui control și a unei monitorizări adecvate. De asemenea, dinamica forței de muncă poate fi văzută ca un risc de securitate a datelor. Procesul de dobândire a specialiștilor în clasificarea datelor poate fi influențat de numeroși factori, precum numărul specialiștilor existenți (prea mulți sau prea puțini dintre ei), costul formării unui nou specialist, condițiile sociale și politice, situația pieței muncii etc. În procesul de identificare și formare a forței umane suplimentare, nivelul securității datelor suferă din punct de vedere al erorilor de clasificare, disponibilității sau chiar confidențialității acestora.

Un alt element dificil de cuantificat financiar, dar care poate fi analizat din perspectiva riscului de securitate este acela al disponibilității datelor. Viteza mică de procesare a datelor specifică sistemului manual, precum și sarcinile adiționale, de validare și transfer manual al datelor între sisteme, pentru realizarea obscurizării și transferului către destinatar, pot avea impact ridicat asupra capacității sistemului de a răspunde eficient la nevoile mediului operațional.

Când ne referim la sistemul automatizat trebuie luate în calcul elemente precum: erori de proiectare, erori de învățare a sistemului automat, erori ale procedurilor de preprocesare a datelor, modul de integrare cu fluxurile operaționale, capacitatea de reziliență a sistemului etc.

Rezumând toate elementele menționate mai sus, am luat în considerare pentru analiza de risc 10 indicatori pe care i-am considerat edificatori în influențarea modului de funcționare a celor două sisteme. Pentru a realiza măsurarea am construit o scală de la 1 (minim) la 5 (maxim) pentru cuantificarea impactului fiecărui indicator asupra activității normale. Sistemul care realizează minimul de puncte oferă un mediu mai sigur pentru prelucrarea datelor.

Tabel 5.3 Analiza de risc

Nr. Crt.	Indicator	Sistem manual	Sistem automat
1.	Scalabilitate	4	1
2.	Erori de clasificare	2	3
3.	Factori externi	4	2
4.	Factori operaționali	4	1
5.	Adaptabilitate / Flexibilitate	3	2
6.	Rutina (capacitatea de a repeta	4	1

	aceeași sarcină fără eroare)		
7.	Timpul necesar soluționării unei sarcini	4	1
8.	Păstrarea confidențialității datelor	3	1
9.	Dependența de tehnologie	1	5
10.	Complexitatea sarcinii	4	2
	Total	33	19

Așa cum se poate observa din tabelul 5.3, sistemul manual are valori maxime și consideră ca influențe maxime negative asupra mediului de securitate următorii indicatori: scalabilitatea, influența factorilor externi și operaționali, capacitatea de a efectua din nou aceeași sarcină fără eroare, timpul necesar pentru a termina sarcina și modul în care aceasta reacționează la o creștere a complexității sarcinii.

Indicatorul de scalabilitate arată capacitatea unui sistem de a acomoda noi capabilități, de a se schimba rapid pentru a acomoda un număr sporit de sarcini sau pentru a-și extinde suportul în cazul modificării obiectivelor organizației. Am considerat că sistemul automat poate satisface astfel de provocări mult mai rapid și necesită mai puține eforturi în comparație cu sistemul uman, care are un nivel ridicat de rezistență la schimbare (Grama, 2017).

De asemenea, am apreciat că funcționarea normală a sistemului manual este mult mai probabil să fie afectată negativ de rutină sau de factori externi și operaționali decât sistemul automat și necesită mai mult timp pentru a procesa o sarcină, iar dacă complexitatea sarcinii este mărită (ex. numărul grupelor de clasificare crește, materialul de clasificat este complex) va genera o creștere rapidă a erorilor.

Am considerat de asemenea că sistemul bazat pe mașină nu clasifică datele la fel de bine ca sistemul uman, deoarece astfel de sisteme sunt încă o tehnologie imatură aflată în faza de cercetare - dezvoltare. Sistemul automat a obținut un punctaj mai ridicat la indicatorul dependență tehnologică, care evaluează situația în care o organizație are dificultăți, din cauza incompatibilităților tehnice, în a-și muta datele pe o altă platformă.

Însumând și comparând punctajele obținute se observă că sistemul automat a obținut un punctaj mai mic decât cel manual (19 versus 33). Se poate trage astfel concluzia că în cadrul acestui sistem riscurile asociate cu securitatea datelor sunt gestionate mai bine și că, per ansamblu, utilizarea unui astfel de sistem determină un management mai bun al securității datelor.

5.6 Beneficiile modelului propus

Modelul propus de obscurizare a informațiilor oferă următoarele avantaje principale:

- Scade timpul de clasificare a informațiilor, oferind posibilitatea organizațiilor de a procesa și transfera rapid și în siguranță informații. Se crește astfel capacitatea acestora de a identifica și reacționa la schimbările apărute în zona de interes;
- Crește capacitatea organizațiilor de a procesa rapid cantități mari de informații din mediul intern, dar și extern;
- Eficientizează utilizarea capabilităților organizației alocând efectuarea sarcinilor repetitive unor mașini și folosind resursa umană doar pentru procesul de luare a deciziilor;
- Crește randamentul resursei umane din cadrul organizației, permițându-i să se concentreze pe sarcini productive și minimizând necesitatea de a efectua operațiuni administrative;
- Minimizează investițiile în tehnologie prin eliminarea costurilor nejustificate în sisteme complexe de obscurizare și manipulare a datelor, datorate erorilor de supraclasificare;
- Poate scădea investițiile CAPEX prin adoptarea sistemului de clasificare automată într-o formă specifică cloud computing IaaS sau SaaS;

- Crește capacitatea organizațiilor de lucru în comun și de partajare a informațiilor atât la nivel intern cât și extern, fără a limita securitatea datelor;
- Crește eficiența procesului de manipulare a informațiilor;
- Minimizează riscurile de securitate, crescând încrederea în sistemul de securizare a informațiilor;
- Necesită supraveghere (umană) minimă după efortul inițial de instalare;
- Este adaptată mult mai bine specificului traficului de date actual din cadrul centrelor de date (est-vest);
- Are o scalabilitate mare, adaptându-se rapid la modificările apărute în mediul operațional;
- Are o disponibilitate ridicată, permițând utilizarea la orice oră și din orice locație, atâta timp cât există o legătură de date;
- Crește confidențialitatea datelor, prin eliminarea interacțiunii cu factorul uman;
- Îmbunătățește disponibilitatea datelor oferind rapid, într-o formă securizată, acces la informațiile solicitate.

Analizând rezultatele ambelor inițiative de cercetare, putem concluziona că organizațiile care au o cantitate mare de date sau care au o strategie orientată pe termen lung vor avea costuri reduse în cazul în care aleg să folosească sisteme de obscurizare automatizate în locul celor clasice. Din punct de vedere al analizei riscurilor, platforma automată realizează un nivel mai ridicat de securizare a datelor, fiind de preferat celei manuale. Utilizarea acestei platforme într-o arhitectură cloud pentru a furniza servicii necesită o analiză sporită a securității și implementarea unei strategii complexe de securizare a datelor.

5.7 Concluzii

Viteza și cantitatea mare de informații cu care organizațiile moderne trebuie să opereze fac ineficient sistemul clasic bazat pe om pentru obscurizarea informațiilor și necesită introducerea unor mecanisme care să optimizeze procesul și să răspundă nevoilor actuale.

Cloud computing-ul, prin accesul rapid la cantități mari de resurse computaționale, a facilitat dezvoltarea tehnologiilor de procesare a limbajului uman. Limitările sistemelor clasice care nu dispuneau de resurse suficiente pentru analiza acestei forme de reprezentare a informației pot fi depășite, iar aceste tehnologii sunt din ce mai ce prezente în arealul tehnologic actual.

Domeniul securității informației este unul critic pentru organizațiile moderne, iar securizarea informațiilor este o componentă esențială a mediului organizațional. Cu toate acestea trebuie ca, prin mijloacele utilizate, acesta să afecteze cât mai puțin eficacitatea proceselor operaționale și să nu limiteze posibilitățile organizației de a profita de oportunitățile care apar. Clasificarea datelor este nucleul procesului de securitate. Ea necesită existența unor politici, strategii și proceduri adecvate pentru a asigura protecția datelor, fără a afecta negativ procesele organizaționale.

Sistemul de obscurizare propus răspunde nevoilor organizațiilor moderne de acces rapid la cantități mari de informații, de optimizare a utilizării resurselor, de abordare a securității dintr-o perspectivă de management a riscului sustenabilă. Organizațiile moderne trebuie să administreze în mod constant cantități mari de informații, iar utilizarea factorului uman limitează eficiența sistemului și generează costuri marginale nejustificate.

Sistemul propus folosește tehnologia procesării automate a limbajului natural și minimizează intervenția umană în proces. De asemenea, el se aliniază principiului securitate prin design, propus în capitolul 2 și este dezvoltat într-o viziune cloud computing, astfel încât să poată fi livrat ca și serviciu.

6. Concluzii generale, realizări și contribuții originale, direcții viitoare de cercetare și diseminare

6.1 Concluzii generale

Evoluțiile tehnologice din ultimul deceniu și în primul rând dezvoltarea capabilităților de oferire a resurselor computaționale sub formă de servicii prin cloud computing constituie un puternic element perturbator atât la nivelul organizațiilor cât și la nivel individual. Modul clasic de utilizare al tehnologiei este provocat de noile modalități de operare ceea ce solicită eforturi considerabile pentru adaptarea la noile cerințe.

Avantajele economice oferite de utilizarea tehnologiei în această nouă arhitectură de lucru au atras numeroase categorii de utilizatori în a încerca integrarea acestor capabilități în spectrul de activități derulate. Se constată astfel o utilizare ridicată a elementelor tehnologice, utilizare care crește în complexitate pe măsură ce numeroase noi servicii sunt dezvoltate sau combinate pentru obținerea unor altor categorii de capabilități.

Implementarea noului cadru de lucru tehnologic în organizații poate oferi avantaje considerabile care permit optimizarea fluxurilor organizaționale, eficientizarea proceselor, scăderea costurilor și creșterea competitivității. Prin acestea, în cadrul unei organizații, tehnologia își depășește condiția clasică de suport a activităților desfășurate evoluând într-un element cu potențial catalizator dacă este implementată și utilizată corespunzător. În aceste condiții securizarea informației și a sistemelor informaționale se constituie ca o direcție de importanță strategică pentru organizație și necesită identificarea și utilizarea de instrumente adecvate pentru managementul acesteia.

În cadrul tezei de doctorat am abordat domeniul securizării informației în cadrul mediilor cloud computing subliniind atât necesitatea securizării activelor informaționale dar și importanța identificării unor mecanisme sustenabile, corelate și adaptate la necesitățile și posibilitățile organizației. În acest sens adoptarea unor tehnici bazate pe o arhitectură de management a riscului poate oferi instrumente pentru identificarea mecanismelor optime de securizare a informației și care să fie în concordanță cu obiectivele organizației.

Securitatea informațională este un proces dinamic care trebuie să răspundă nevoilor, vulnerabilităților, amenințărilor, precum și schimbărilor constante care au loc în mediul de operare. O abordare cuprinzătoare combină elemente tehnologice, oameni și procese prin utilizarea unui mecanism structurat care integrează securitatea informației și activitatea de management a riscurilor.

Importanța informației pentru organizațiile moderne a determinat creșterea fenomenului infracțional cibernetic și implicarea unor noi tipuri de actori cu motivații complexe. Identificând vulnerabilitățile unei tehnologii imature și beneficiind de cantități mari de resurse la dispoziție aceștia au manifestat adaptabilitate ridicată modificându-și rapid strategiile și tehnicile de acțiune în vederea depășirii mecanismelor de protecție utilizate de sistemele de protecție.

În acest sens în teză am efectuat un studiu pentru a identifica dacă instrumentele specifice strategiilor clasice de protecție a sistemelor informaționale mai pot face față cu succes provocărilor tehnologice moderne. Studiul de caz având ca obiect de cercetare infrastructura cloud computing din cadrul Institutului de Cercetare, Dezvoltare și Inovare – Produse High-Tech pentru Dezvoltare Durabilă (ICDI-Pro-DD) al Universității Transilvania a identificat faptul că deși instrumentele erau aplicate corespunzător totuși acestea nu reușeau să asigure securitatea resurselor concomitent cu furnizarea către utilizatori a maximului de capabilități pe care tehnologia le poate oferi.

Evoluția rapidă a fenomenului cibernetic infracțional și "succesele" repurtate de acesta sunt datorate și imposibilității instrumentelor specifice strategiei clasice de a face față dinamismului, mobilității, flexibilității, cantității, varietății, complexității ridicate a sistemelor informaționale bazate pe tehnologii cloud computing. Securizarea mediilor informaționale moderne necesită reconsiderarea strategiei utilizate și dezvoltarea unor instrumente/inițiative

într-o arhitectură modernă care să asigure securitatea datelor, păstrarea capabilităților tehnologiilor și care să fie economic sustenabilă.

O altă direcție importantă de cercetare în cadrul tezei a fost aceea a automatizării obscurizării informației. Procesul clasic de obscurizare a datelor se bazează pe elementul uman pentru realizarea operațiunilor de clasificare a acestora lucru care induce numeroase limitări operaționale și costuri nejustificate. Dezvoltările tehnologice în domeniul procesării limbajului natural și accesul ușor la cantități considerabile de resurse informaționale, necesare acestor procese, creează oportunitatea automatizării prelucrării informațiilor. În acest fel limitările induse de factorul uman pot fi eliminate iar sistemele bazate pe automatizarea obscurizării datelor pot răspunde mult mai bine necesităților mediilor de lucru moderne.

Aplicația dezvoltată în acest sens are la bază un element de învățare automată a conceptelor și un modul de prelucrare a limbajului natural. Analizele desfășurate au scos în evidență faptul că o astfel de abordare poate fi integrată într-un sistem de securizare al datelor bazat pe managementul riscului. Din cauza faptului că sistemul necesită investiții mai ridicate pentru punerea în funcțiune el se pretează organizațiilor care au o orientare pe termen lung. Totuși și celelalte tipuri de organizații ar putea integra un astfel de sistem dacă ar opta pentru utilizarea acestei capabilități sub forma unui serviciu. Aplicația a fost concepută pentru maximă compatibilitate cu mediile cloud computing, ea putând fi ușor integrată în cadrul organizațional și perturbând la un nivel minim fluxurile operaționale.

Sistemele informaționale moderne trebuie să facă față unor cantități mari de informații și să asigure capabilități care acum câteva decenii erau de neconceput. Posibilitățile pe care tehnologiile moderne le oferă permit orchestrarea resurselor în arhitecturi diverse cu grade de complexitate din ce în ce mai ridicate. Paradoxal, tocmai aceste capabilități avansate constituie și elementul care frânează adopția lor de către utilizatori. Păstrarea confidențialității, integrității și disponibilității datelor în mediile informaționale moderne crește în dificultate o dată cu creșterea complexității acestor sisteme. Securizarea datelor în aceste sisteme se constituie ca un element critic care condiționează succesul sau eșecul organizațiilor.

6.2 Contribuții originale

Obiectivele de ordin teoretic și practic propuse și descrise în primul capitol au fost îndeplinite în întregime, astfel:

Obiectivul O1 a fost îndeplinit prin următoarele realizări și contribuții originale:

- S-a realizat o analiză complexă a mediului de securitate specific tehnologiilor cloud computing, identificându-se limitările tehnologiilor actuale de securizare a datelor;
- S-au identificat riscurile de securitate specifice mediului de manipulare a datelor cloud computing, evidențiindu-se spectrul nou de factori de risc datorat utilizării unui mediu de manipulare a informației bazat pe capabilități computaționale externalizate.

Obiectivul O2 a fost îndeplinit prin următoarele realizări și contribuții originale:

- S-a realizat o analiză a principalelor strategii clasice de protejare a activelor informaționale ale unei organizații, identificându-se limitările posibilităților de utilizare și a eficacității acestora;
- S-a realizat un studiu de caz al infrastructurii cloud computing din cadrul Institutului de Cercetare, Dezvoltare și Inovare – Produse High-Tech pentru Dezvoltare Durabilă (ICDI-Pro-DD) al Universității Transilvania. S-a identificat spectrul de necesități de securitate, specifice unui mediu de lucru dinamic, mobil, bazat pe partajerea resurselor, de la distanță și s-a analizat modul în care strategia clasică de protecție a datelor este în măsură să asigure nevoile de securitate a datelor în acest mediu.

Obiectivul O3 a fost îndeplinit prin următoarele realizări și contribuții originale:

- S-au propus și analizat o serie de măsuri, de nivel strategic, pentru îmbunătățirea securității datelor dar care sunt adaptate nevoilor specifice ale mediilor informaționale bazate pe tehnologii cloud computing.

Obiectivul O4 a fost îndeplinit prin următoarele realizări și contribuții originale:

- S-au identificat limitările mecanismelor clasice de obscurizare a informației bazate pe criptare și mascare;
- S-a identificat potențialul de utilizare a token-izării și avantajele utilizării acesteia ca mecanism de obscurizare a datelor în mediile dinamice cu acces diferențiat la resurse, atât din punct de vedere al costurilor cât și al beneficiilor operaționale.

Obiectivul O5 a fost îndeplinit prin următoarele realizări și contribuții originale:

- S-a realizat o analiză a limitărilor sistemelor actuale de clasificare a datelor;
- S-a propus și dezvoltat un model de obscurizare a datelor bazat pe sisteme automate de prelucrare a limbajului natural;
- S-a implementat și testat modelul propus. În vederea realizării acestui lucru, s-a utilizat pentru partea de procesare componente ale platformei IBM Bluemix, iar pentru interacțiunea cu utilizatorul o interfață web dezvoltată pentru a pune în evidența capabilitățile cloud computing.

Obiectivul O6 a fost îndeplinit prin următoarele realizări și contribuții originale:

- S-a realizat un studiu comparativ a costurilor pentru sistemul clasic și cel propus în vederea evidențierii avantajelor modelului dezvoltat;
- S-a efectuat o analiză comparativă a managementului riscurilor de securitate pentru sistemul clasic și cel propus pentru a compensa limitările analizei costurilor.

6.3 Direcții viitoare de cercetare

Urmare a analizei rezultatelor obținute pe parcursul cercetărilor efectuate în prezenta teză de doctorat, am identificat o serie de noi direcții care ar putea constitui subiectul unor proiecte de cercetare ulterioare:

- Îmbunătățirea modelelor matematice de cuantificare a investițiilor în domeniul securității sistemelor informaționale, în momentul de față acestea fiind în general limitate la evaluare informației procesate și a probabilității de compromitere a acesteia. Deoarece tehnologia a devenit o componentă catalizatoare a proceselor organizaționale adoptarea acestui tip de model limitează posibilitatea cuantificării corecte a riscului compromiterii resurselor informaționale;
- Dezvoltarea sistemului propus de obscurizare a informațiilor prin integrarea unor algoritmi mai copleși bazați pe metadate, analiza emoțiilor etc. Astfel, procesul de clasificare a informațiilor poate obține fiabilități ridicate prin considerarea unor elemente mai complexe precum intenția, starea de spirit, canalul de transmitere a informației, calitatea sursei informației etc.;
- Studierea posibilității integrării în sistemul automatizat de clasificare, a informațiilor în format audio, imagine sau video. Ținând cont de cantitatea foarte mare de informație de acest gen precum și de dezvoltările tehnologice în procesarea acestor tipuri de formate dezvoltarea unei astfel de capabilități se constituie ca o necesitate reală a mediului informațional actual.
- Dezvoltarea și studierea aplicabilității unui sistem automat de management a informațiilor bazat pe modulul de obscurizare a informațiilor propus în prezenta lucrare. Avantajele automatizării obscurizării informației din cadrul sistemelor informaționale moderne pot fi puse în valoare de un sistem care să administreze independent informațiile și care să fie transparent pentru utilizator. În acest fel organizațiile pot beneficia de

avantajele tehnologice specifice mediilor cloud computing într-o arhitectură operațională sustenabilă dezvoltată pe managementul riscului;

- Dezvoltarea inițiativelor de securizare a mediilor informaționale moderne și realizarea unor analize avansate cu privire la capabilitățile acestora. O astfel de analiză poate avea aplicabilitate imediată în identificarea și dezvoltarea unor strategii moderne de management a activelor tehnologice ale unei organizații care să permită utilizarea, într-un mediu securizat, a întregului spectru de capabilități pe care sistemele le pot oferi;

6.4 Diseminarea rezultatelor prin lucrări elaborate pe durata pregătirii doctoratului

Rezultatele activității de cercetare, desfășurate pe durata studiilor doctorale, au fost diseminate și validate atât prin participări în cadrul unor conferințe internaționale cât și prin publicarea de articole în volume și reviste de specialitate naționale și internaționale. Dintre acestea șase au fost publicate ca prim autor iar două ca și coautor, astfel:

a) Lucrări publicate la conferințe cotate ISI WoS:
   1. **OGÎGĂU-NEAMȚIU, F.,** Antonoaie, C., „*Securing Data in Online Learning Systems by Automated Classification*", 14th International Scientific Conference „Elearning and Software for Education", București, 2018, DOI 10.12753/2066-026X-18-000;

b) Lucrări publicate în jurnale BDI/B+:
   1. **OGÎGĂU-NEAMȚIU, F.,** „*Cryptographic key management in cloud computing"***,** Proceedings of the 10th International Scientific Conference "Defense Resources Management in the 21st Century", 2015, Brașov, Romania, pp. 225-229, ISSN: 2248 – 2245;
   2. **OGÎGĂU-NEAMȚIU, F.,** „*Tokenization as a Data Security Technique*", National Defence University Scientific Quarterly, Nr. 2 (103), 2016, Varșovia, pp. 124-135, ISSN 0867–2245;
   3. **OGÎGĂU-NEAMȚIU,** F., MORARU, S. A., KRISTALY D. C., „*A Data Defense Strategy For Modern Business Environment*", International Journal of Advanced Research in Computer Science (IJARCS), Vol 9, No 1, 2018, India, ISSN: 0976-5697;
   4. **OGÎGĂU-NEAMȚIU,** F., „*Automating the Data Security Process*", Journal of Defense Resources Management, Vol. 8, Issue 2(15), 2017, Brașov, Romania, pp. 91-100, ISSN: 2068-940;
   5. **OGÎGĂU-NEAMȚIU,** F., MOGA, H., „*A Cyber Threat Model of a Nation Cyber Infrastructure based on Goel-Okumoto Port Approach*", Revista Academiei Forţelor Terestre Nr. 1 (89)/2018, pp. 75-87, ISSN 2247-840X.

c) Lucrări publicate în volume de specialitate
   1. **OGÎGĂU-NEAMȚIU,** F., MOGA, H., BOȘCOIANU, E., „Profilul psihologic al războinicului cibernetic și hackerului non statal bazat pe matricea de decizie polieuristică", în volumul „Managementul Situațiilor de Risc în Contextual Crizelor de Securitate", editura Academiei Forțelor Terestre „Nicolae Bălcescu", Sibiu, 2017, pp. 78-137, ISBN 978-973-153-277-6;
   2. MOGA, H., **OGÎGĂU-NEAMȚIU,** F., BOȘCOIANU, E., „Modelarea amenințării interstatale utilizând evaluarea polieuristică a deciziilor", în volumul „Managementul Situațiilor de Risc în Contextual Crizelor de Securitate", editura Academiei Forțelor Terestre „Nicolae Bălcescu", Sibiu, 2017, pp. 138-178, ISBN 978-973-153-277-6.

Bibliografie selectivă

Alonso, S. (2016, December 30). Computer network defense operations, disrupting the enemy's attack. Preluat de pe CYBER SECURITY: https://cyber-ir.com/2015/08/23/computer-network-defense-operations-disrupting-the-enemies-attack/

Armbrust M., F. A. (2010). A view of cloud computing. Communications of the ACM, Vol. 53, No. 4,., 50-58.

Armbrust, M. F. (2009). Above the Clouds: A Berkeley View of Cloud. EECS Department. University of California, Berkeley. Preluat pe February 20, 2016, de pe https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

Ashley Chonka, Y. n. (2011). Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks.

Baeza-Yates, R. &.-N. (1999). Modern information retrieval (Vol. 463). New York: ACM press.

Betz, D. J. (2017). Cyberspace and the State: Towards a Strategy for Cyber-Power. New York: Routledge.

Boulding, K. E. (1962). Conflict and Defense: A General Theory.

Care, J., & Litan, A. (2016). Hype Cycle for Application Security,. Gartner.

Christopher D. Manning, P. R. (2008). Introduction to Information Retrieval. Cambridge University Press. Preluat de pe https://nlp.stanford.edu/IR-book/pdf/irbookonlinereading.pdf

Cleveland, F. (2008). Cyber security issues for Advanced Metering Infrasttructure (AMI). Institute of Electrical and Electronics Engineers Xplore. doi:10.1109/PES.2008.4596535

Craggs, B. &. (2017). Smart cyber-physical systems: beyond usable security to security ergonomics by design. In Proceedings of the 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems, pp. 22-25.

Dasgupta S., P. C. (2008). Algorithms. New York: McGraw-Hill.

Dimensional Research . (2015). THE STATE OF DATA PRIVACY IN 2015 A SURVEY OF IT PROFESSIONALS.

Durairaj M., K. P. (2014). A Study On Virtualization Techniques And Challenges In Cloud Computing,. International Journal Of Scientific & Technology Research(Volume 3, Issue 11).

Geer Jr, D. E. (2008, September 28). Complexity is the enemy. ieee seCurity & PrivaCy, Volume: 6, Issue: 6, 88-88.

Goetsch, K. (2014). eCommerce in the Cloud. Sebastopol, USA: O'Reilly Media, Inc.

Grabosky, P. (2014). The Evolution of Cybercrime, 2004-2014. RegNet Working Paper, No. 58,.

Grama, B. &. (2017). Change, Resistance to Change and Organizational Cynicism. Studies in Business and Economics, 11(3), 47-54. doi:10.1515/sbe-2016-0034

Guvernul României. (2002). Hotărâre de guvern nr. 585/2002 art 3.

H.Weber, R. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review, 23-30. doi:https://doi.org/10.1016/j.clsr.2009.11.008

International Data Group. (2016). Enterprise Cloud Computing Survey.

Jan Kallberg, B. T. (2013). From Cyber Terrorism to State Actors' Covert Cyber Operations. În Strategic Intelligence Management (pg. 229–233). doi:https://doi.org/10.1016/B978-0-12-407191-9.00019-3

Jonathan Levin, L. E. (2014). The Data Revolution and Economic Analysis. În Innovation Policy and the Economy, Volume 14 (pg. 1-24). University of Chicago Press.

Kent, A. B. (1955). Machine literature searching VIII. Operational criteria for designing information retrieval systems. Journal of the Association for Information Science and Technology, 6(2), 93-101.

MacKey David J. (2003). Information Theory, Inference and Learning Algorithms. Cambridge: Cambridge University Press.

Maha Tebaa, S. E. (2013). Secure Cloud Computing through Homomorphic Encryption. International Journal of Advancements in Computing Technology (IJACT), 29-38.

Marie Baezner, P. R. (2017). Cyber and Information warfare in the. Zürich: Center for Security Studies.

Mell P., G. T. (2011). The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-145.

Microsoft. (2018, ianuarie 12). the-osi-model-s-seven-layers-defined-and-functions-explained. Preluat de pe www.microsoft.com: https://support.microsoft.com/en-us/help/103884/the-osi-model-s-seven-layers-defined-and-functions-explained

Miller, E. H. (2010). A Multiple-Replica Remote Data Possession Checking Protocol with Public Verifiability. Second International Symposium on Data, Privacy, and E-Commerce.

Nillson N. (1998). Introduction to Machine Learning: an early draft of a proposed textbook. Stanford.

OGÎGĂU-NEAMȚIU, F. M. (2018). A Cyber Threat Model of a Nation Cyber Infrastructure based on Goel-Okumoto Port Approach. Revista Academiei Forţelor Terestre Nr. 1 (89)/2018, 75-87. Preluat de pe http://www.armyacademy.ro/rev1_2018.php

Oxford Dictionary. (2018, February 13). Preluat de pe Definition of encryption in English:: https://en.oxforddictionaries.com/definition/encryption

Panmore Institute. (2016, Septemeber 9). The CIA thriad. Preluat de pe http://panmore.com/the-cia-triad-confidentiality-integrity-availability

PCI Security Standards Council. (2018, 02 02). PCI_DSS_v3-2. Preluat de pe pcisecuritystandards.org: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

R. Chandramouli, M. I. (2013, September). Cryptographic Key Management. Preluat de pe National Institute of Standards and Technology, USA: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7956.pdf

Rhoton, J. (2009). Cloud Computing Explained: Implementation Handbook for Enterprises. Milton Keynes, UK: Recursive Press.

Rouse, M. (2017, Septembrie). What is data masking? Preluat de pe Information security information: http://searchsecurity.techtarget.com/definition/data-masking

Schneier, B. (2008, October 1). Security Is a State of Mind. Dr. Dobb's Journal.

Securelink. (2016). Managing Cloud Data Security in Regulated Industries for 2016. Preluat pe November 26, 2017, de pe https://www.securelink.com/newhotness/wp-content/uploads/2015/12/WP_ManagingDataSecurity.pdf

Seref Sagiroglu, D. S. (2013). Big data: A review. Collaboration Technologies and Systems (CTS), 2013 International Conference on. San Diego, USa: IEEE. doi:10.1109/CTS.2013.6567202

Shenk, J. (2013). Layered Security: Why It Works . SANS Institute.

Sosinsky, B. (2011). Cloud Computing Bible. Indianapolis, USA: Wiley Publishing, Inc.

Stackify. (2017). 35 Leading PaaS Providers. Preluat pe Noiembrie 5, 2017, de pe https://stackify.com/top-paas-providers/

REZUMAT / ABSTRACT

Cercetări privind securizarea informației în sistemele cloud computing
Contributions on information security in cloud computing systems

Conducător științific,
Prof. dr. ing. Sorin Aurel MORARU

Doctorand,
Florin OGÎGĂU-NEAMȚIU

Cuvinte cheie: information technology, data security, automation, strategy, tokenization

Rezumat

Teza de doctorat abordează problematica securizării mediilor informaționale bazate pe tehnologii cloud computing. Abordarea are la bază, pe de o parte, caracterul critic al informației și al sistemelor de tehnologia informației pentru organizațiile moderne, dar și necesitatea ca procesul securizării acesteia să fie unul sustenabil care să nu limiteze capabilitățile tehnologiilor sau performanța organizației. Cercetarea de față a scos în evidență faptul că noua artitectură de livrare a capabilităților tehnologice combinată cu viteza și gradul de integrare a acesteia în procesele organizaționale și în viețile oamenilor necesită abordări inovatoare în ceea ce privește instrumentele de nivel tactic, operațional și strategic utilizate pentru securizarea mediilor. Securitatea informațională este un proces dinamic care trebuie să răspundă nevoilor, vulnerabilităților, amenințărilor, precum și schimbărilor constante care au loc în mediul de operare. Securizarea datelor în medii cu un ridicat caracter dinamic suferă din cauza limitărilor impuse de operatorul uman și, în acest context, automatizarea obscurizării datelor poate surmonta aceste limitări. Lucrarea scoate în evidență faptul că securitatea datelor și a infrastructurilor în mediile cloud computing trebuie fundamentată într-un cadru holistic de management al riscului care să țină cont de date, amenințări, vulnerabilități, dar și de impactul pe care eventualele măsuri de protecție le-ar avea asupra organizațiilor și proceselor derulate de acestea.

Abstract

The PhD thesis addresses the issue of securing information environments based on cloud computing technologies. The approach is based, on the one hand, on the critical nature of information and information technology systems for modern organizations, but also on the need for the process of securing it to be a sustainable one that does not limit the capabilities of the technology or the performance of the organization. This research has highlighted that the new architecture used to deliver technological capabilities, combined with its speed and degree of integration into organizational processes and people's lives, requires innovative approaches and tools at tactical, operational and strategic levels used for securing environments. Information security is a dynamic process that needs to address the needs, vulnerabilities, threats, and constant changes that take place in the operating environment. Securing data in high dynamic environments suffers from the limitations imposed by the human operator, and in this context automated data obscuration can overcome these limitations. The paper highlights the fact that data and infrastructure security in cloud computing environments must be managed in a holistic risk management framework that takes into account data, threats, vulnerabilities, and the impact that any protective measures would have on the organizations and its processes.

CURRICULUM VITAE

Informaţii Personale	Florin OGÎGĂU-NEAMȚIU
Experiență profesională	
Perioada	martie 2010 – prezent
Funcția sau postul ocupat	Șef Compartiment Informatizare și INFOSEC
Numele angajatorului	Departamentul Regional de Studii pentru Managementul Resurselor de Apărare, Brașov
Perioada	iulie 2008 – martie 2010
Funcția sau postul ocupat	Responsabil INFOSEC/ administrator rețea
Numele angajatorului	Ministerul Apărării Naționale, Brașov
Perioada	iulie 2002 – iulie 2008
Funcția sau postul ocupat	Șef microstructură
Numele angajatorului	Ministerul Apărării Naționale, Brașov
Educație și formare	2016 – curs "Chief Information Officer", College of Information and Cyberspace, Washington D.C. (S.U.A.); 2008 - Diplomă de licență, specializarea "Informatică", Facultatea de matematică și informatică a Universității ”Transilvania”, Brașov (România); 2002 - Diplomă de licență în "Managementul organizației" specializarea "Știință militară", Academia Forțelor Aeriene “Henri Coandă”, Brașov (România);
Limbi străine	Engleză – foarte bine Germană – intermediar Franceză – intermediar
Competențe și abilități organizatorice	Capacitate de coordonare a echipei, orientat pe rezultate, abilități bune de analiză a competențelor oamenilor și de a desemna sarcinile în funcție de aptitudinile lor, capacitatea de a lucra sub presiune și de a putea lua decizii în medii cu factori necunoscuți cu termene scurte, abilități de a lucra într-un mediu solicitant, cu situații extrem de dinamice și stresante;
Competențe sociale	Perseverent, loial, bun comunicator, adaptabil, conștiincios
Altele	Reprezentant al DRESMARA în cadrul cadrul grupului de lucru ”Invățământ Distribuit la Distanță” din cadrul centrelor NATO/PTEC; Membru în colectivul de cercetare ”Procedură de testare şi evaluare a securităţii reţelelor fără fir”, Planul sectorial de cercetare și dezvoltare al Ministerului Apărării Naționale, pozitia 13, 2013; Membru în colectivul de cercetare ”Realizarea unui program de simulare a sistemului de conducere a focului GUN*STAR NIGHT din cadrul complexului antiaerian 2x35 mm Oerlikon”, Planul Sectorial de Cercetare-Dezvoltare al MApN pe anul 2017.

Universitatea Transilvania din Brașov

CURRICULUM VITAE

Personal Information	Florin OGÎGĂU-NEAMȚIU
Professional experience	
Dates	March 2010 – present
Occupied position	Head of Information and INFOSEC Branch
Employer	Regional Department of Defense Resources Management Studies, Brașov
Dates	July 2008 – March 2010
Occupied position	INFOSEC/network administrator
Employer	Ministry of National Defense, Brașov
Dates	July 2002 – July 2008
Occupied position	Head of team
Employer	Ministry of National Defense, Brașov
Education	2016 – "Chief Information Officer" course, College of Information and Cyberspace, Washington D.C. (USA); 2008 – Licensed in Informatics, Faculty of Mathematics and Informatics, ”Transilvania” University, Brașov (România); 2002 – Licensed in "Organizational Management", specialization "Military Science", Air Force Academy “Henri Coandă”, Brașov (România);
Foreign languages	English – advanced German – medium French – medium
Managerial competences	High leadership skills, result oriented, good capacities to analyze team members abilities and allocate tasks based on them, good capacity to work in stressful environments in dynamic and demanding conditions, to make decisions in high incertitude environments and with short deadlines.
Social abilities	Tenacious, loyal, good communicator, adaptable, rigorous
Other	DRESMARA representative in ”Advanced distributed learning Group” of NATO/PTEC (Partnership and Training Education Centers) ; Team member in the research group ”Procedure for Testing and Evaluation of the Wireless Networks Security“ , Research and Development Sectorial Plan of the Ministry of National Defense, position 13, 2013; Team member in the research group “Development of a simulation program for the GUN*STAR NIGHT fire control of the 2x35 mm Oerlikon air defense system”, Research and Development Sectorial Plan of the Ministry of National Defense, 2017.