Aspecte privind securitatea la nivelul SLA în serviciile de Cloud computing

Dragoș BARBU[1,2], Alexandru SIPICĂ[1], Ionuț CANDET[1]

[1]Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București

[2]Academia de Studii Economice București, Școala Doctorală de Informatică Economică

dragos.barbu@ici.ro, alexandru.sipica@ici.ro, ionut.candet@ici.ro

Rezumat: Lucrarea de față își propune să identifice importanța securității la nivelul SLA (Service Level Agreement) în condiția utilizării scăzute a serviciilor de Cloud Computing la nivelul economiei. Articolul prezintă în prima parte deficiențele în adopția serviciilor de cloud, prezentând la nivel statistic gradul de adopție pe țări și ramuri de activitate. În partea a doua, este prezentat conceptul de SLA (documentul care guvernează relația client–furnizor cloud computing), precum și cele mai importante criterii pentru dezvoltarea unui SLA. În vederea furnizării de servicii cu un grad ridicat de încredere sunt prezentate cele mai importante metrici privind asigurarea securității la nivelul SLA. În ultima parte, în vederea creșterii încrederii în serviciile de cloud, sunt propuse un set de metrici care pot fi incluse în documentele de SLA (Disponibilitatea şi timpul de întreţinere, lista de servicii şi resurse care sunt oferite de către furnizor către clienţi, timpul de răspuns al aplicaţiei, programul de notificare în avans al modificărilor în reţea care pot afecta utilizatorii, timpul de răspuns al biroului de asistenţă pentru diferitele categorii de probleme, consecinţele în caz de încălcare a acordului).

Cuvinte cheie: Cloud Computing, securitate, SLA, metrici de securitate.

The SLA security issues in cloud computing services

Abstract: This paper aims to identify the importance of security at the SLA level (Service Level Agreement), given the low utilization of Cloud Computing services at the economy level. The article presents in the first part the deficiencies in the adoption of cloud services, presenting at statistical level the degree of adoption by countries and branches of activity. In the second part, we present the concept of SLA (the document that governs the client-provider cloud computing relationship) as well as the most important criteria for the development of an SLA. In order to provide services with a high degree of trust, the most important metrics regarding security assurance are presented at the SLA level. Finally, in order to increase trust in cloud services, a set of metrics can be proposed that can be included in SLA documents (Availability and maintenance time, list of services and resources that are provided by the provider to the clients, application response, advance notification program of network changes that may affect users, support desk response time for different problem categories, consequences in case of breach of agreement).

Keywords: Cloud Computing, security, SLA, security metrics.

1. Introducere

Incidentele de securitate cibernetică (Strategia României pentru Cyber Security, 2013) și atacurile cibernetice majore cu care s-au confruntat unele state și organizații internaționale în ultimii ani au determinat, la nivel internațional, înțelegerea necesității adoptării unor strategii și politici în domeniul securității informatice. Astfel, există strategii naționale de securitate cibernetică, cum ar fi cele din Estonia, Statele Unite, Marea Britanie, Germania și Franța, care susțin necesitatea dezvoltării în continuare a capabilităților lor de combatere a atacurilor cibernetice și care stabilesc cadrul de acțiune și cooperare între guverne, entități și ONG-uri pentru a atenua consecințele. Conform acestor strategii, eforturile statelor vizează implementarea unor măsuri de securitate care să conducă la creșterea nivelului de protecție a infrastructurii cibernetice, în special a celor care sprijină infrastructurile critice naționale.

Problematica propusă în cadrul articolului de față face parte dintr-un proiect de cercetare elaborat în vederea îmbunătățirii serviciilor de cloud computing. Standardele de calitate pentru cloud computing permit elaborarea unei strategii și a unui cadru de reglementare specific, care să

definească terminologii, modele structurale, rolurile și responsabilitățile părților implicate, să stabilească criteriile de securitate, performanță și funcționalitate a serviciilor cloud, precum și a modalităților de utilizare și evaluare a acestora.

Pe măsură ce sporește importanța informațiilor, impactul negativ al pierderii acestora la nivel organizațional crește exponențial. Efectele sunt predictibile și costisitoare, incluzând:

- eficiență redusă;
- scăderea productivității;
- creșterea stresului și frustrării angajaților;
- venituri mai mici.

În încercarea de a evalua serviciile de cloud este necesară alegerea unor criterii de măsurare, indicatori și metrici care joacă un rol esențial în procesul de evaluare. Sunt propuse diverse metrici de evaluare, care acoperă principalele aspecte ale cloud computing: performanță, efecte economice, securitate.

2. Dificultăți în implementarea serviciilor de cloud

Confidențialitatea și securitatea reprezintă cele mai importante obstacole pentru implementarea cloud-ului în sectorul public, indiferent dacă confidențialitatea cloud-ului este principalul motor al inițiativei (spre exemplu, în inițiativa germană *trusted cloud*), sau cazul în care confidențialitatea și securitatea reprezintă un obstacol în calea implementării unei aplicații specifice (cazul experienței franceze care a remarcat faptul că neîncrederea față de cloud este dependentă de problemele de confidențialitate, în ciuda implementării inițiativei cloud).

Aspecte ce pot fi considerate dificultăți în asigurarea calității serviciilor de cloud sunt:

- *problemele financiare* - de exemplu, determinarea costurilor reale comparativ cu beneficiile preconizate, luând în considerare costul total al sistemelor potențiale de back-up etc. Ca și caz particular, costurile asociate cu implementarea funcționalităților serviciilor cloud sau integrarea acestora în proceduri sunt insuficient cunoscute în comparație cu cele ale serviciilor convenționale IT;
- *aspecte tehnice* – acest tip de dificultăți este menționat în special de Italia care descrie astfel de probleme ca fiind legate de lipsa maturității tehnologiilor. Cu toate acestea, alte țări, cum ar fi Portugalia, au subliniat faptul că tehnicile și tehnologiile, nu au fost o problemă majoră, deoarece cloud computing-ul a reprezentat un instrument nou și există, de obicei, costuri legate de adoptarea de noi tehnici, oricare ar fi acestea.
- *probleme de reglementare* – spre exemplu, experiența Italiei arată că principala dificultate în absorbția cloud-ului în sectorul public este legată de aspectele legale care împiedică partajarea serviciilor în cadrul diferitelor administrații publice. Drept urmare s-a constatat că în astfel de cazuri este necesară încheierea unor acorduri interne. În mai multe țări (cum ar fi Austria), este de asemenea interzisă salvarea anumitor date în centre cloud cu locația în străinătate - din motive legate de securitatea națională.
- *SLA și lipsa de practici în elaborarea unor astfel de acorduri* – anumiți furnizori de servicii cloud oferă contracte standard de bază pentru dezvoltarea cloud-urilor; aceste contracte nu acoperă corespunzător nevoile și cererile clienților cu niveluri mai ridicate ale solicitărilor de securitate;
- *probleme legislative* – furnizorii de servicii cloud lucrează adesea cu subcontractori, ceea ce face ca problemele juridice să fie câteodată mai complicate (chiar dacă, contractul se încheie între administrație și CSP (Cloud Solution Provider), subcontractanții trebuie să respecte aceleași reguli privind, securitatea, SLA sau schimbul de date, angajat prin contract).

La nivel European, multe dintre inițiativele analizate au fost afectate de dificultăți și diferențe de natură culturală precum și de insuficienta capacitate a organizațiilor interne de a gestiona schimbările. În majoritatea cazurilor, introducerea cloud-ului necesită un nou proces de gestionare și achiziție a TIC, precum și diverse schimbări în competențele TIC și a posturilor din sectorul public (în cazul Franței este de subliniat impactul asupra resurselor umane unde serviciile cloud automatizează unele dintre sarcinile care erau efectuate anterior de către personal) (figura 1).

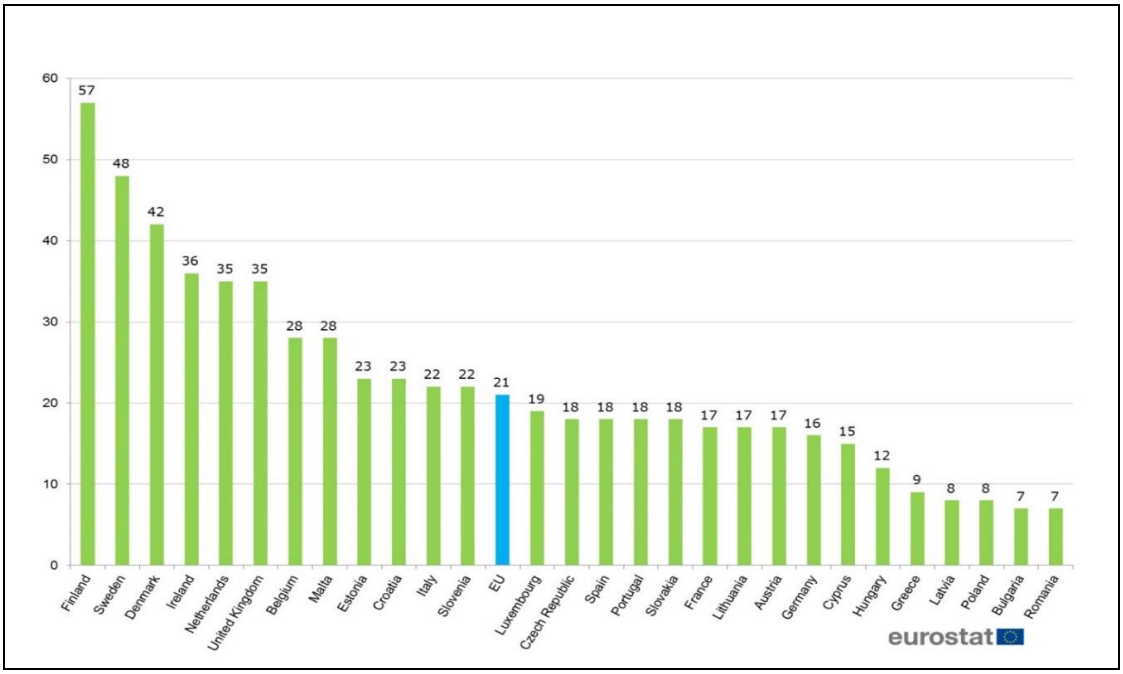


Figura 1. Adopția serviciilor de Cloud Coputing la nivelul Uniunii Europene în 2017 (Eurostat 2017)

Preocupările privind confidențialitatea și securitatea datelor reprezintă factori majori în percepțiile pe care utilizatorii și personalul din sectorul public le au legat de cloud computing, constituind o barieră în adoptarea de inițiative la nivel național. Bariere de ordin cultural se regăsesc în majoritatea țărilor analizate, indiferent de nivelul lor de implementare a cloud-ului. În acest sens este necesară prezentarea unei liste a principalelor dificultăți identificate la implementarea cloud în statele UE (tabelul 1).

Tabelul 1. Principalele bariere ale inițiativelor și aplicațiilor Cloud

Nr. crt.	Țară	Securitate și confidențialitate	Reglementare	Financiare	Technologice	SLA	Culturale
1	**UK**	x	x	-	x	-	x
2	**Italia**	x	x	-	x	x	x
3	**Olanda**	x	x	x	x	x	-
4	**Franța**	x	-		x	-	x
5	**Danemarca**	x	x	x	x	-	x
6	**Germania**	x	x		-	-	-
7	**Spania**	-	-	-	x	x	x
8	**Portugalia**	x	-	-	-	x	x
9	**Belgia**	x	x		x	x	-
10	**Austria**	x	x	x	x	x	x

Prelucrat după (Bonneau V. 2013)

3. Conceptul de SLA

În cadrul *Practical Guide to Cloud Service Agreements (version 2)*, acordurile la nivel de servicii cloud (Cloud service agreements, CSA) sunt definite ca un set de documente sau acorduri care conțin termenii care guvernează relația dintre clientul cloud şi furnizorul de servicii cloud.

SLA-urile descriu pentru ambele părți implicate (atât client, cât și furnizor de cloud), așteptările acționând ca o foaie de parcurs pentru schimbarea serviciului cloud. De fapt, la fel cum un proiect IT necesită o foaie de parcurs care cuprinde un set de rezultate clar definite, un SLA este, de asemenea, esențial pentru lucrul cu infrastructura cloud. De fapt, pentru a dezvolta un SLA coerent și eficient trebuie menționată o listă de criterii importante (Chraibi, M. et al., 2017).

Câteva dintre cele mai importante criterii sunt:

- *disponibilitate*: descrie procentul disponibilității serviciului convenit în cazul zilelor lucrătoare și a celor nelucrătoare. De exemplu: 99,9% în timpul zilelor lucrătoare, 98,5% în timpul nopții /weekend;
- *performanță*: descrie timpul maxim de răspuns pentru un anumit serviciu;
- *securitatea/confidențialitatea* datelor: acest element este legat de confidențialitatea, integritatea, disponibilitatea și responsabilitatea datelor stocate în cadrul cloud-ului. Un exemplu privind securitatea este criptarea tuturor datelor stocate și transmise;
- *așteptările privind recuperarea în caz de dezastru*: acest element descrie angajamentul asumat de furnizorul de cloud pentru a asigura recuperarea datelor în caz de dezastru, fapt care ar putea afecta centrul principal de date;
- *localizarea datelor*: acest element descrie locația unde sunt stocate datele. Această regulă ar trebui să fie în concordanță cu legislația locală;
- *accesul la date*: această regulă definește modul în care clientul va accesa datele sale. Un exemplu al acestei reguli ar fi următorul: datele recuperabile de la furnizor în format lizibil;
- *portabilitatea datelor*: acest element descrie identitatea unui alt furnizor care poate deține datele clientului ori de câte ori furnizorul principal întâlnește o problemă. De fapt, este posibil ca furnizorul de cloud să nu menționeze niciun alt furnizor de cloud;
- *procesul de gestionare a schimbării*: această parte se referă la procesele pe care un serviciu trebuie să le treacă pentru a fi actualizate sau pentru a adăuga noi funcționalități;
- *strategia de ieșire*: această parte descrie cât de netedă este ieșirea din centrul de date al furnizorului de servicii cloud.

4. Metricile de securitate pentru serviciile SLA

În literatura de specialitate sunt identificate două categorii majore de metrici care pot fi exprimate în cadrul SLA. Prima categorie conține *metrici pentru evaluarea calității serviciilor oferite de către CSP*, în timp ce cea de-a doua categorie conține *metrici care sunt folosite pentru a evalua securitatea mediului oferită de CSP*.

În ambele categorii am putea subdiviza măsurătorile pe baza nivelului de servicii oferit de CSP: Software-ul ca serviciu (SaaS), Stocarea ca serviciu, Platforma ca serviciu (PaaS) şi Infrastructura ca serviciu (IaaS).

În Figura 1 sunt clasificate metricile care se pot evalua atunci când se ia în considerare calitatea serviciilor oferite de CSP. Pentru clienți, aspectul economic este cel mai important criteriu

în selecția furnizorului de cloud. Diferiții furnizori de servicii cloud oferă o varietate de opțiuni cu costuri diferite.

Furnizorul de servicii cloud oferă diferite mașini virtuale în funcție de planurile și cerințele clienților.

Clienții compară toate opțiunile disponibile și selectează cel mai economic furnizor de servicii și planul care îndeplinește cerințele lor. În Figura 2 sunt clasificate metricile care se pot evalua atunci când se în considerare calitatea serviciilor oferite de CSP.

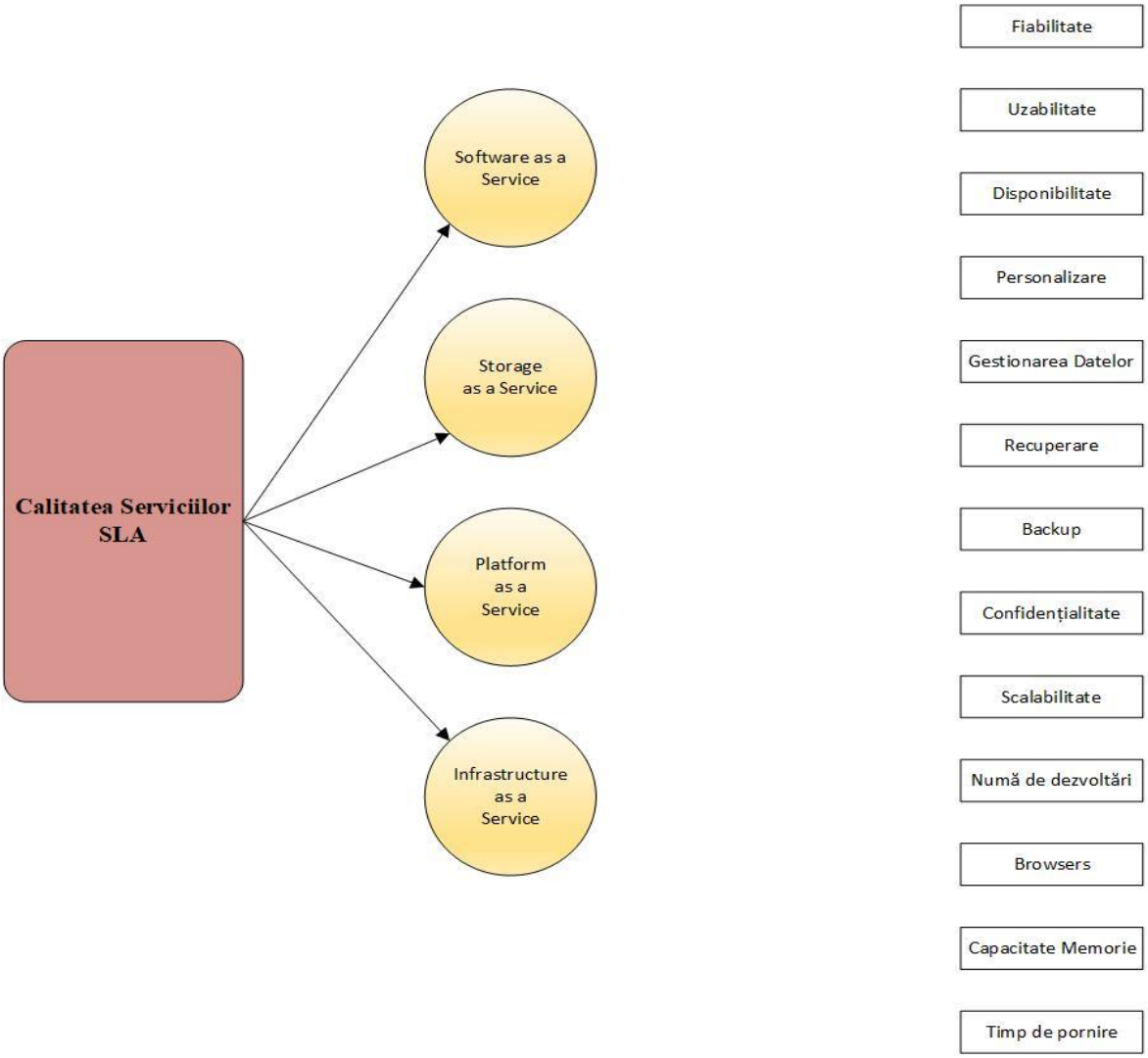


Figura 2. Categorii de metrici pentru evaluarea serviciilor CSP (adaptat Chraibi, M. et al., 2017)

Deoarece securitatea este unul dintre aspectele cele mai importante pe care clienții le iau în considerare înainte de a lua decizia de a transfera gestionarea datelor și serviciilor lor către cloud, în Figura 3 sunt identificate diferite metrici care trebuie exprimate într-un SLA pentru a asigura clienții de securitatea activelor lor.

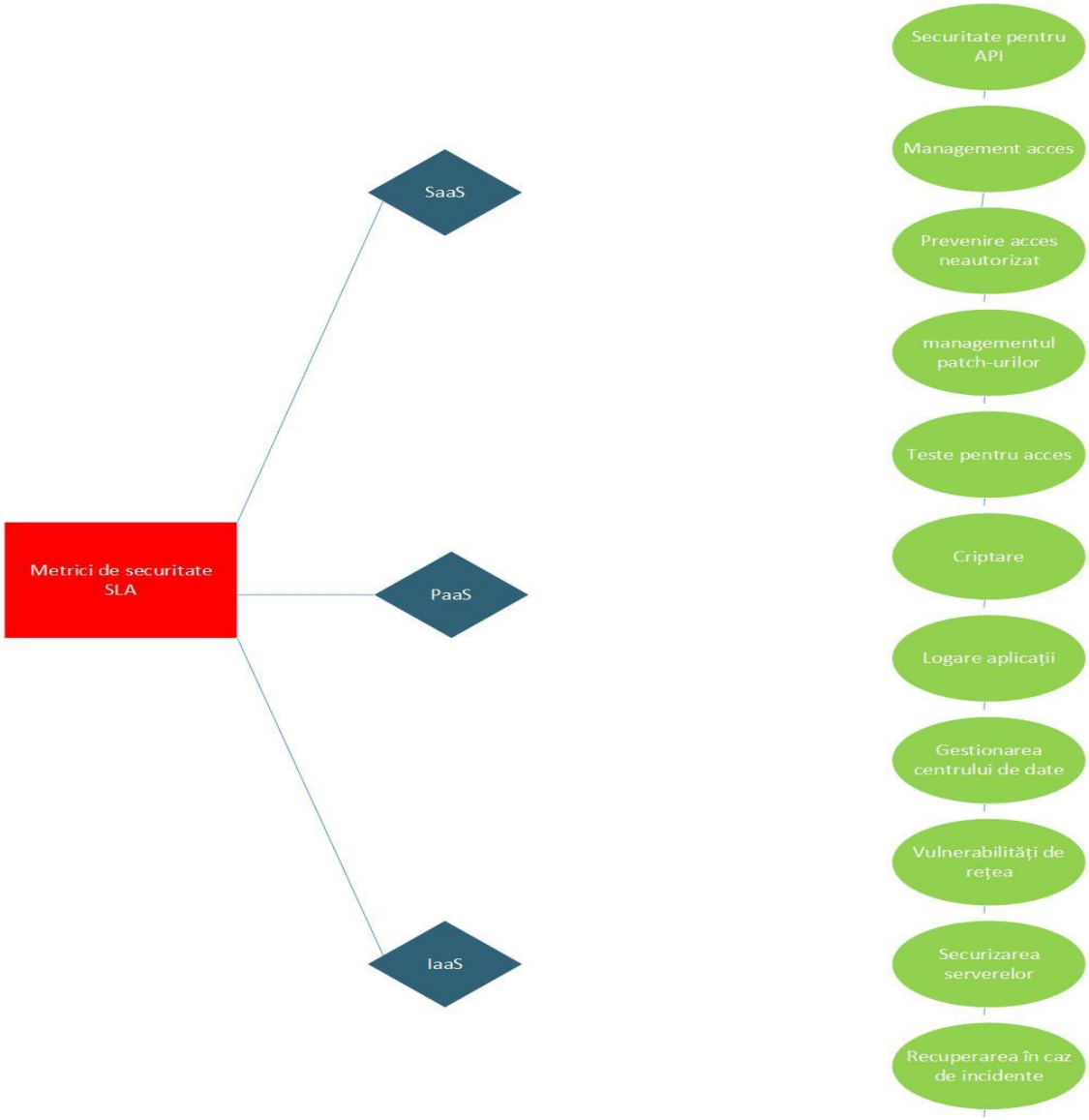


Figura 3. Metrici SLA (adaptat Chraibi, M. et al., 2017)

Securitatea informațiilor și confidențialitatea sunt probleme cruciale în mediul cloud. În cloud computing, serviciile sunt accesate de clienți prin intermediul internetului. Dar internetul poate fi o rețea nesigură în anumite condiții. Astfel, există întotdeauna preocupări legate de securitate în timpul stocării și partajării datelor confidențiale ale companiei. Caracteristici cum ar fi securitatea datelor şi autentificarea sunt aspecte de securitate identificate de mulți cercetători și sunt explicate în Tabelul 2.

Tabelul 2. Metrici de securitate

Caracteristici	Descriere	Metrici
Autentificare	Autentificarea înseamnă, de obicei, verificarea faptului dacă utilizatorul este autentificat sau nu. Numai utilizatorii autentificați au dreptul de a accesa datele.	• Eficacitate • Sensibilitate • Confidențialitate
Securitatea datelor	Furnizorul Cloud oferă un diferite opțiuni pentru securizarea datelor din cloud cu costuri diferite. Clienții trebuie să selecteze planul în funcție de nivelul de securitate necesar pentru a-și asigura datele în cloud.	• Latența comunicării prin SSL • Aplicabilitatea SSL • Capacitatea de audit

5. Evaluarea serviciilor de SLA

Vulnerabilitățile (Cârnu E. C. et al., 2018), în general sunt erori care pot induce breșe de securitate. O vulnerabilitate software este o eroare care poate fi folosită direct de un hacker pentru a avea acces la un sistem sau la o rețea. Concretizarea încrederii stabilite între clienții și furnizorii de servicii cloud apare sub forma unui document legal numit Acord la Nivel de Servicii (SLA). SLA include calitatea serviciilor, capacitatea resurselor, scalabilitatea, obligațiile și consecințele în caz de încălcări ale acordului. (Chandana et al., 2017) identifică următoarele metrici care pot fi incluse în documentele de tip SLA:

- disponibilitatea și timpul de întreținere: procentajul serviciilor disponibile pe unitatea de timp;
- lista de servicii și resurse care sunt oferite de către furnizor către clienți;
- timpul de răspuns al aplicației;
- programul de notificare în avans al modificărilor în rețea care pot afecta utilizatorii;
- timpul de răspuns al centrului de asistență pentru diferitele categorii de probleme;
- consecințele în caz de încălcare a acordului.

(Lamb et al., 2014) au prezentat o abordare care descrie diferite tipuri de modele de cloud computing existente în prezent și modul în care acestea gestionează serviciile. Sistemele actuale de cloud nu ignoră restricțiile SLA, ci sunt proiectate să suporte un singur tip de SLA. SLA include în general timpul total de întreținere a sistemului și o serie de metrici de răspuns. Dacă dintr-un anumit motiv furnizorul de cloud nu mai poate respecta termenii descriși, intervine o strategie de compensare adresată clienților afectați.

Problemele de securitate (Vevera V. A. et al., 2018) reflectă, de multe ori, o lipsă a know-how-ului dezvoltatorilor implicați. TIC este un domeniu în care cunoștințele devin depășite foarte rapid, iar programele de formare și calificare, realizate în mod continuu, sunt o condiție primordială pentru menținerea angajaților TIC și pentru productivitatea acestora. Conceptele multiple SLA permit furnizorilor să diferențieze nivelurile de servicii disponibile. Arhitecturile moderne suportă disponibilitatea și timpul de întreținere, precum și parametrii de latență, lățime de bandă etc. Acest tip de SLA prevede sancțiuni atunci când condițiile SLA sunt încălcate. (Luna et al., 2017) propun evaluarea cantitativă la nivel de securitate a furnizorilor de servicii cloud (Cloud Service Providers - CSPs) bazată pe secSLA (Security Level Agreements) pentru a se potrivi cu cerințele clienților. Folosind această evaluare, CSP-urile sunt clasificate (conform secSLA) pentru a se potrivi mai bine cu cerințele clienților. Sunt propuse două tehnici de evaluare, și anume QPT (Quantitative Policy Trees) și QHP (Quantitative Hierarchical Process) pentru evaluarea cantitativă și analiza nivelului de securitate bazat pe secSLA furnizat de CSP-uri. Aceste tehnici pot contribui la îmbunătățirea specificațiilor privind cerințele de securitate, introducând o metodologie flexibilă și simplă care să le permită clienților să identifice și să reprezinte nevoile lor specifice de securitate. QPT utilizează o agregare logică a cuantificatorilor de securitate, în timp ce QHP se bazează pe tehnici de optimizare multi-variabile luând în considerare diferitele elemente ale unui secSLA. În general, cele două tehnici, evaluarea secSLA și clasarea CSP-urilor se efectuează în etape progresive QPT și QHP, așa cum se arată în figura 4.

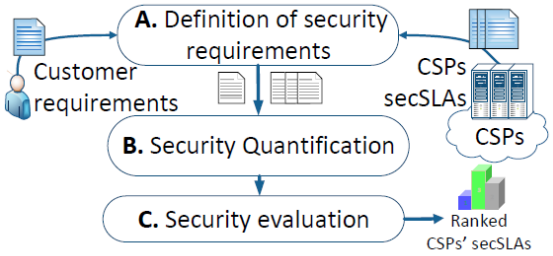


Figura 4. Etapele evaluării cantitative secSLA (după Luna et al., 2017)

Organizația Internațională de Standardizare (ISO) și Comisia Electrotehnică Internațională (IEC), în standardul ISO/IEC 9126 revizuit ulterior la ISO/IEC 25010: 2011, au identificat diferitele criterii de evaluare a calității unui software: funcționalitate, fiabilitate, utilizabilitate, eficiență, mentenabilitate și portabilitate (ISO/IEC 25010:2011).

6. Concluzii

Conceptul de SLA oferă criterii care trebuie luate în analiză la dezvoltarea serviciilor de Trusted Cloud Computing;

În cadrul articolului sunt identificate 6 metrici ce măsoară securitatea la nivelul SLA (eficacitate, sensibilitate, confidențialitate, latența comunicării prin SSL, aplicabilitatea SSL, capacitatea de audit) care au două caracteristici esențiale și anume: autentificare și securitatea datelor.

În ceea ce privește evaluarea vulnerabilităților, articolul identifică șase metrici esențiale care pot fi introduse în pachetul de documente oferit clienților pentru a crește gradul de încredere în serviciile de cloud (Trusted Cloud). Pentru rezolvarea problemelor de securitate, furnizorii de cloud vor trebui să includă și să îmbunătățească în permanență modalitățile de asigurare a securității datelor.

În prezent, flexibilitatea mai mare a Cloud Computing-ului în comparație cu externalizarea tradițională este adesea contrabalansată de siguranța redusă a clientului, cauzată de contractele insuficient de precise și de echilibrate cu furnizorii de Cloud Computing. Tehnologiile Cloud Computing vor sta la baza unei noi etape în dezvoltarea managementului în istoria informaticii.

Confirmare

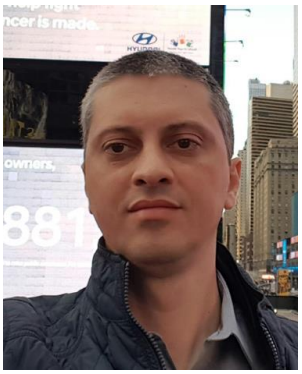
Acest articol a fost susținut în cadrul *Simpozionului Slove Muscelene*, ediția a XI-a, desfășurat în perioada 18-19 iulie 2019 la Câmpulung Muscel.

BIBLIOGRAFIE

1. Bonneau, V. (2013). *Analysis of cloud best practices and pilots for the public sector*. ISBN:978-92-79-33897-7, 2013.
2. Cîrnu, E. C., Rotună, C. I., Vevera, A. V., Boncea, R. (2018). *Measures to Mitigate Cyber-security Risks and Vulnerabilities in Service-Oriented Architecture*. Studies in Informatics and Control, 27(3) 359-368, September 2018, ISSN: 1220-1766, eISSN: 1841-429X, 2018, 359-368.
3. Chandana, O. R., Brunda, B. V., Rajeshwari, B. S. (2017). *A Study on Service Level Agreement Management Techniques in Cloud*. International Journal, 5(5).
4. Chraibi, M. et al. (2017). *Policy Based Context Aware Service Level Agreement (SLA) Management in the Cloud*. In CLOUD COMPUTING 2017: The 8th International Conference on Cloud Computing, GRIDs, and Virtualization, pp. 122-128.
5. Lamb, C. C., Heilman, G. L. (2014). *Service Level Agreement Complexity Processing Concerns for Standalone and Aggregate SLAs*. Department of Electrical and computer Engineering. The University of New Mexico, 27th July 2014.
6. Luna, J., Taha, A., Trapero, R., Suri, N. (2017). *Quantitative reasoning about cloud security using service level agreements*. IEEE Transactions on Cloud Computing, 5(3), 457-471.
7. *** (SQuaRE) – *System and software quality models*. BS ISO/IEC 25010:2011, 2011.
8. *** *Strategia României pentru Cyber Security*, 2013, documentul poate fi consultat la adresa: https://cert.ro/vezi/document/NCSS-Ro.

9. Vevera, V. A., Albescu, A. R. (2018). *Factorul uman vs. securitatea cibernetică*. Romanian Journal of Information Technology and Automatic Control, Revista Română de Informatică și Automatică, Vol. 28, No. 4, 2018, 67-74.

10. *** Eurostat.2017 https://ec.europa.eu/eurostat.



Dragoş Cătălin BARBU este doctorand la Universitatea de Studii Economice din București și deține un masterat la Universitatea din București, Facultatea de Matematică și Informatică. În prezent este Cercetător Științific superior III și şef al departamentului Cloud Computing la Institutul Național de Cercetare-Dezvoltare în Informatică - ICI București. De asemenea, este lector asociat la Facultatea de Matematică și Informatică - Universitatea din București. Expertiza sa profesională include limbaje de programare C / C++ și Java, baze de date relaţionale, medii integrate de dezvoltare (Visual Studio, NetBeans, Eclipse). Din 2004 a fost implicat în următoarele proiecte finanțate de UE: Similar și ARiSE (FP6), UsiXML (Eureka), SPOCS (CIP-ICT PSP), TOOP (H2020), IdealIST2018. Este de asemenea membru al Consiliului Științific al ICI București din 2017 și președintele Comitetului Tehnic de Specialiști (TCS) - parte a Comitetului Tehnico-Economic (TCE) - entitate guvernamentală a Ministerului Comunicațiilor și Societății Informaționale în procesul de elaborare, monitorizare și implementare a politicii guvernamentale. Este autor a 20 de lucrări de revistă și 14 lucrări de conferință, un capitol de carte și o carte în domeniul securității cibernetice.

Dragoş Cătălin BARBU is a PhD candidate at the Bucharest University of Economic Studies and he holds a M.Sc. from the University of Bucharest, Faculty of Mathematics and Computer Science. He is currently working as a Senior Scientific Researcher III and Head of the Cloud Computing Department at the National Institute for Research and Development in Informatics - ICI Bucharest. He is also an associate lecturer at the Faculty of Mathematics and Computer Science - University of Bucharest. His professional expertise includes C/C++ and Java programming, relational databases, integrated development environments (Visual Studio, NetBeans, Eclipse). Since 2004 he has been involved in the following EU funded projects: Similar and ARiSE (FP6), UsiXML (Eureka), SPOCS (CIP-ICT PSP), TOOP (H2020), IdealIST2018. Mr. Barbu is also a member of the Scientific Council of ICI Bucharest since 2017 and the President of the Technical Committee of Specialists (TCS) - part of the Technical - Economical Committee (TCE) - governmental entity that assists the Ministry for Communications and Information Society in the process of government policy elaboration, monitoring and implementation. He is author/ co-author of 20 journal papers and 14 conference papers, one book chapter and one book in the cyber-security domain.

Alexandru SIPICĂ a absolvit Facultatea de Management în anul 2005. Este doctor la UAMV București. În prezent este Cercetător Științific gradul III la ICI București. Din 2016 este membru și secretar al Consiliului Științific ICI București. Principalele sale domenii de interes sunt Cloud Computing și Project Management. Este implicat în proiecte de cercetare specifice societății informaționale. Cercetarea sa a fost publicată în articole de jurnal și în conferințe specializate TIC.

Alexandru SIPICĂ graduated from the Faculty of Management in 2005 and UAMV Bucharest. He currently is a Scientific Researcher III at ICI Bucharest. Since 2016 he is a member and secretary of the ICI Bucharest Scientific Council. His main areas of interest are Cloud Computing, Project Management. He is involved in research projects specific to the information society. His research has been published in journal articles and specialized ICT conferences.

Ionuț CANDET a absolvit Universitatea din București specializarea Managementul Informațiilor și al Documentelor în anul 2014. În prezent este Asistent Cercetare la ICI București. Din 2018 este șef Birou Permanență în cadrul Serviciului Cloud Computing. Principalele sale domenii de interes sunt Cloud Computing și Datacenter. Este implicat în proiecte de cercetare specifice societății informaționale. Rezultatele activității sale de cercetare a fost publicat în articole de reviste și în conferințe specializate TIC.

Ionuț CANDET is graduated on 2014 from University of Bucharest, in Information and Document Management. Currently he is a Research Assistant at ICI Bucharest. Since 2018 he has been head of the Permanent Office within the Cloud Computing Service. Its main areas of interest are Cloud Computing and Datacenter. He is involved in research projects specific to the information society. The results of his research activity have been published in journal articles and in specialized ICT conferences.