



GHID
Securitatea în Cloud

Ghid realizat de către:



Asociația Națională
pentru
Securitatea
Sistemelor Informatice

Pagină albă

Cuprins

1.	Introducere.....	4
1.1	Ce înseamnă Cloud Computing	4
1.2	Tipuri de Cloud	4
1.3	Servicii de tip Cloud	5
2.	Cloud Computing: Caracteristici, Evoluții, Bariere de adoptare.....	6
2.1	Caracteristici.....	6
2.2	Evoluții.....	7
2.3	Reglementari și recomandări la nivel UE	8
2.4	Bariere de adoptare	11
2.4.1	Constituirea unui cadru de reglementare specific	12
2.4.2	Securitatea	12
2.4.3	Confidențialitatea.....	13
2.4.4	Încrederea	13
2.4.5	Blocarea serviciilor și standardele	13
2.4.6	Alte probleme.....	13
3.	Impact pentru sectorul privat	14
3.1	Impact la nivelul sectorului financiar	14
3.2	Impact la nivelul sectorului educațional.....	16
3.3	Impact la nivelul sectorului telecomunicațiilor	19
3.4	Impact la nivelul sistemului de sănătate	20
4.	Securitatea în Cloud	22
4.1	Vulnerabilități	22
4.1.1	Încălcarea securității datelor.....	23
4.1.2	Pierderea datelor.....	23
4.1.3	Piratarea conturilor sau a serviciilor	23
4.1.4	Interfete și API nesigure	24
4.1.5	Blocarea serviciilor (DoS, DDos)	24
4.1.6	Insuficienta investigare și implicare (due–diligence)	24
4.1.7	Probleme cu tehnologiile distribuite	25
4.2	Asigurarea conformității în cloud.....	26
4.3	Riscuri și preocupări privind platformele Cloud	26
4.4	Recomandări	30
4.4.1	Guvernanța și Managementul de Risc al Organizației	30
4.4.2	Interoperabilitate și portabilitate.....	33

4.4.3	Securitate, continuitatea afacerii, și recuperarea după dezastre	34
4.4.4	Arhitectura și Proceduri operaționale în Data Center.....	35
4.5	Auditare și atestare	36
Anexa nr. 1 -	Caracteristici	38
Anexa nr. 2 -	Analiza SWOT	40
Anexa nr. 3	Studii suport pentru utilizarea Cloud-ului în România.....	41

1. Introducere

Comisia Europeană a lansat în martie 2010 Strategia Europa 2020 pentru ieșirea din criză și pregătirea economiei UE pentru provocările deceniului următor. Europa 2020 conturează o perspectivă care înglobează realizarea unui grad înalt de ocupare a forței de muncă, crearea unei economii cu emisii scăzute de carbon, productivitate și coeziune socială, obiective care urmează a fi atinse prin acțiuni concrete la nivelul UE și la nivel național.

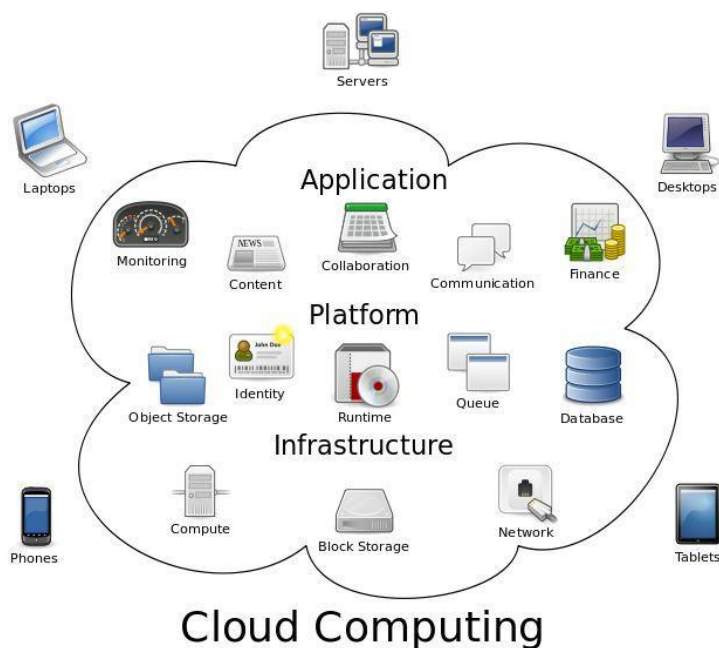
Agenda Digitală pentru Europa este una dintre cele șapte inițiative-pilot ale Strategiei Europa 2020 și are ca scop definirea rolului motor esențial pe care utilizarea tehnologiei informației și comunicațiilor (TIC) va trebui să-l joace în realizarea obiectivelor Europei pentru 2020.

Dezvoltarea astăzi a cloud computing-ului are același impact revoluționar pe care l-a avut dezvoltarea rețelelor electrice și de transport cu un secol în urmă.

Aplicarea pe scară largă și utilizarea mai eficace a tehnologiilor de cloud computing vor permite guvernelor să abordeze provocările fundamentale cu care se confruntă și vor oferi cetățenilor o mai bună calitate a vieții, datorită accesului mai ușor la serviciile publice.

1.1 Ce înseamnă Cloud Computing

Cloud Computing este un concept modern, un model de servicii de acces prin Internet la sisteme distribuite de resurse de calcul configurabile la cerere (Ex: servere, stocare de date, aplicații și servicii) care pot fi puse rapid la dispoziție cu eforturi minime de management și intervenție din partea clientului și a furnizorului. Accesul se poate face de oriunde, convenabil, fără ca utilizatorul să aibă nevoie să știe configurația sistemelor care furnizează aceste servicii. Mai simplu spus, aplicațiile și datele rulează și sunt stocate în altă parte decât pe serverele și stațiile utilizatorului, acesta accesându-le de la distanță (pe Internet, dar nu neaparat).



1.2 Tipuri de Cloud

Cloud privat descrie o infrastructură IT, prevăzută pentru utilizarea exclusivă de către o singură organizație care cuprinde mai mulți consumatori (Ex: business units). Infrastructura IT se află la sediul organizației sau gestionarea acesteia este externalizată la un terț ('on-premises' sau 'off-premises'). Un cloud privat poate fi comparat cu un centru de date convențional - diferența fiind că soluțiile tehnologice sunt puse în aplicare

pentru a optimiza utilizarea resurselor disponibile și de a spori aceste resurse prin investiții mici, care sunt făcute într-un mod treptat în timp

Cloud public este o infrastructură deținută, administrată și operată de către un furnizor de servicii specializat, organizație comercială, academică, guvernamentală sau o combinație a acestora. Serviciile pot fi accesate prin intermediul internetului, iar furnizorul de servicii are un rol esențial în ceea ce privește protecția eficientă a datelor angajate în sistemele sale.

Cloud de comunitate este o infrastructură de tip cloud prevăzută pentru utilizarea exclusivă de către o comunitate specifică de consumatori din organizații care au preocupări sau interese comune (de exemplu școli, cercetători, dezvoltatori de software). Aceasta poate fi deținută, administrată și operată de către una sau mai multe dintre organizațiile din comunitate, o terță parte sau o combinație a acestora și poate exista fizic în interiorul sau în afara organizației.

Cloud Hybrid, așa-numitul "**cloud intermediar**", descrie o infrastructură de tip cloud ca o combinație de două sau mai multe infrastructuri Cloud distincte (Cloud de comunitate, privat sau public), care rămân entități unice, dar sunt legate împreună de o tehnologie proprietară sau standardizată, care permite portabilitatea datelor și aplicațiilor la cerere (un exemplu de utilizare este echilibrarea utilizării resurselor în cazul vârfurilor de solicitare).

1.3 Servicii de tip Cloud

În funcție de cerințele utilizatorilor, există mai multe soluții de cloud computing disponibile pe piață, acestea pot fi grupate în trei categorii principale sau "modele de servicii". Aceste modele se aplică, de obicei, la ambele soluții cloud privat și public:

IaaS (Infrastructure as a Service): un furnizor închiriază o infrastructură tehnologică, adică servere virtuale la distanță, care pot înlocui înlocui sistemele IT de la sediul companiei sau pot fi folosite alături de sistemele existente. Astfel de furnizori sunt de obicei jucătorii de pe piața de specialitate și se bazează de fapt pe o infrastructură fizică complexă care se întinde în mai multe zone geografice.

SaaS (Software as a Service): un furnizor oferă prin intermediul de servicii web, diverse aplicații și le pune la dispoziția utilizatorilor finali. Aceste servicii sunt adesea menite să înlocuiască aplicații convenționale instalate de utilizatori pe sistemele lor locale. Acesta este cazul de exemplu al aplicațiilor tipice de birou bazate pe web, cum ar fi foi de calcul, instrumente de procesare de text, registre computerizate și agende, calendare partajate, poștă electronică, etc.

PaaS (Platform as a Service): un furnizor oferă soluții de dezvoltare avansată și găzduire de aplicații. Aceste servicii sunt de obicei adresate companiilor pentru a dezvolta și găzdui soluții proprietare pe bază de cerere pentru a satisface cerințele interne și / sau pentru a oferi servicii către terți. La fel, serviciile livrate de un furnizor de PaaS fac inutilă pentru utilizator necesitatea de hardware sau software suplimentar specific, la nivel intern.

IaaS include întreaga stivă de resurse de infrastructură și facilități (energie electrică, soluții de răcire, etc) pentru platformele hardware găzduite. Aceasta include capacitatea de a abstractiza (sau nu) resursele, precum și de a livra conectivitate fizică și logică a acestor resurse. În cele din urmă, IaaS oferă un set de API-uri care permit forme de management și alte tipuri de interacțiune cu infrastructura pentru consumatori.

PaaS se află deasupra IaaS și adaugă un nivel suplimentar de integrare cu framework-urile de dezvoltare de aplicații, capacități de middleware, și funcții, cum ar fi baze de date, stive de interogări, care permit dezvoltatorilor să construiască aplicații, și ale căror limbaje de programare și instrumente sunt suportate.

SaaS la rândul său, este construit pe IaaS și PaaS și oferă un mediu de operare de sine stătător folosit pentru a furniza întreaga experiență a utilizatorului, inclusiv conținutul, prezentarea, cererea și capacități de management.

Prin urmare, ar trebui să fie clar că există compromisuri importante pentru fiecare model în termeni de caracteristici integrate, de complexitate vs deschidere (extensibilitate), și de securitate. Compromisuri între cele trei modele de implementare cloud includ:

- În general, SaaS oferă cele mai integrate funcționalități, cu cea mai mică posibilitate de extensibilitate și un nivel relativ ridicat de securitate integrat (furnizorul poartă o parte importantă de responsabilitate pentru securitate).
- PaaS permite dezvoltatorilor să construiască propriile aplicații în zona superioară a platformei. Ca urmare, tinde să fie mai extensibil decât SaaS. Acest compromis se extinde la elementele de securitate, dar oferă tocmai datorită flexibilității posibilitatea integrării unui strat de securitate suplimentar.
- IaaS oferă cea mai multă extensibilitate. Acest lucru înseamnă că, în general, capacitățile de securitate și funcționalitățile nu trec dincolo de protejarea infrastructurii în sine. Acest model presupune că sistemele de operare, aplicațiile și conținutul vor fi gestionate și securizate de către consumatorul de astfel de servicii.

Organizații de reglementare și standardizare:

Cloud Security Alliance (CSA)

Cloud Security Alliance (CSA) este o organizație non-profit, cu misiunea de a promova utilizarea celor mai bune practici pentru furnizarea și asigurarea securității în Cloud Computing, și de a oferi educație cu privire la utilizarea de cloud computing. Cloud Security Alliance este condusă de o coalitie largă de practicieni din industrie, corporații, asociații și alte părți interesate.

ISACA

ISACA este o asociație independentă non-profit, la nivel mondial. ISACA se angajează în dezvoltarea, adoptarea și utilizarea la nivel global a cunoștințelor și a practicilor pentru sistemele informatice de vârf.

Național Institute of Standards and Technology (NIST)

Fondată în 1901, NIST este o agenție federală non-reglementare în cadrul Departamentului de Comerț al SUA. Misiunea NIST este de a promova inovația și competitivitatea industrială prin avansarea științei, a standardelor și tehnologiilor în moduri care sporesc securitatea economică și îmbunătățesc calitatea vieții noastre.

Article 29 Working Party – European Comision

Article 29 Working Party este un grup de lucru pentru protecția datelor ce a fost instituit în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal .

European Cloud Partnership

Parteneriatul Cloud European (ECP) reunește industria și sectorul public pentru a stabili o piață unică digitală pentru cloud computing în Europa.

Acesta a fost stabilit în cadrul [European Cloud Strategy](#).

2. Cloud Computing: Caracteristici, Evoluții, Bariere de adoptare

2.1 Caracteristici

Deoarece noțiunea „cloud” nu se referă la o anumită tehnologie, ci la o paradigmă în general, este obligatoriu să se clarifice unele aspecte.

Această secțiune stabilește capacitățile concrete asociate cu cloud computing, care sunt considerate esențiale (necesare în orice mediu cloud) și relevante. Putem distinge între capacități non-funcționale, economice și tehnologice adresate sau care vor fi adresate de către sistemele cloud.

Aspectele non-funcționale se referă la calitățile sau proprietățile unui sistem. Acestea pot fi realizate și interpretate în mai multe moduri ceea ce duce în mod tipic la probleme mari de compatibilitate și interoperabilitate între furnizori, fiecare furnizor având propriile metode de satisfacere a cerințelor. Aspectele nonfuncționale sunt unul dintre motivele pentru care „cloud” diferă atât de mult în interpretare.

Considerațiile economice sunt unul dintre motivele cheie pentru introducerea sistemelor cloud în mediul de afaceri. Interesul particular apare în reducerea costurilor și a efortului prin externalizare și/sau automatizarea managementului resurselor esențiale. După cum s-a observat în prima secțiune, aspectele relevante ce trebuie avute în vedere sunt asociate cu delimitarea dintre pierderea controlului și reducerea efortului. Cu privire la găzduirea pe infrastructuri „cloud” private, câștigul prin reducerea costurilor trebuie echilibrat în mod atent cu efortul ridicat de a construi și rula un astfel de sistem.

În mod evident, provocările tehnologice apar implicit din aspectele economice și nonfuncționale. În opoziție cu aceste aspecte, provocările tehnologice presupun o realizare specifică. În plus față de aceste provocări implicite, se pot identifica aspecte tehnologice suplimentare care vor fi adresate de sistemul cloud, parțial ca o condiție prealabilă de a realiza unele dintre aspectele de nivel ridicat, dar parțial deoarece sunt asociate direct cu anumite caracteristici ale sistemelor cloud.

Caracteristicile cheie ale cloud computing-ului pot fi analizate din prisma a trei aspecte: non-funcționale, economice, tehnologice, aspecte prezentate în **Anexa nr. 1**

2.2 Evoluții

Tendința spre cloud computing a început la finalul anilor 80 cu un concept de grid computing, când pentru prima dată un număr mare de sisteme au fost dedicate rezolvării unei singure probleme, de obicei din domeniul cercetării, necesitând resurse excepționale de calcul paralel. În Europa, rețelele optice de distanțe lungi sunt utilizate pentru a lega multe universități într-un mare computing grid pentru ca resursele să fie partajate și scalate pentru calcule științifice complexe.

Grid computing a asigurat un mediu virtual de resurse de calcul, dar diferă de cloud computing. Grid computing se referă în special la dedicarea mai multor computere pentru a soluționa o anumită problemă individuală sau pentru a rula o anumită aplicație. Cloud computing, pe de altă parte, se referă la folosirea mai multor resurse, inclusiv resurse computaționale, pentru a asigura un „serviciu” unitar către utilizatorul final. De obicei un grid este un cluster de servere pe care o sarcină mare poate fi divizată în sarcini mai mici pentru a rula în paralel. Din acest punct de vedere, un grid poate fi vizualizat ca un server virtual.

Într-un mediu cloud, resursele extinse de IT și de afaceri, precum servere, stocare, rețea, aplicații și procese pot fi puse la dispoziția sarcinilor de lucru. În plus, în timp ce un cloud poate asigura și susține un grid, un cloud poate susține și medii non-grid, precum arhitectura Web three-tier care rulează aplicațiile Web tradiționale sau Web 2.0.

În anii 90, conceptul de virtualizare a fost extins dincolo de serverele virtuale la niveluri mai ridicate de abstractizare – oferind pentru prima dată platforme virtuale, stocare și resurse de rețea și apoi la nivel aplicație, aplicații virtuale, care nu se bazează pe o infrastructură specifică. Puterea de calcul existentă a oferit clusterelor ca platforme virtuale de calcul pentru modele noi de business.

Mai recent, modelul „software ca serviciu” (SaaS) a ridicat nivelul de virtualizare la nivelul de aplicație, cu un model business de tarifyare nu prin resursele consumate, ci prin valoarea aplicației pentru abonați. Este un model emergent prin care utilizatorii pot avea acces la aplicațiile lor de oriunde, în orice moment, prin dispozitivele lor conectate. Aceste aplicații rezidă în centre de date masiv scalabile unde resursele de calcul pot fi furnizate dinamic.

Companiile pot alege să partajeze aceste resurse utilizând clouds privați sau publici, în funcție de nevoile specifice. Cloud-urile publice expun serviciile clienților, afacerilor și consumatorilor pe Internet. Cloud-urile private sunt în general limitate la utilizarea în cadrul unei companii în spatele unui firewall și astfel sunt mai puțin expuse. Puterea unui cloud este în gestionarea infrastructurii sale, permisă prin maturitatea și progresul tehnologiei de virtualizare pentru a gestiona și utiliza mai bine resursele de susținere prin provizionare

automată, re-imaging, reechilibrarea sarcinilor de lucru, cereri sistematice de modificare și o platformă dinamică, sigură și flexibilă.

Deoarece din ce în ce mai multe întreprinderi adaugă cloud computing, nivelul aplicațiilor migrează spre misiuni mai critice, iar SaaS va fi un pilon al strategiilor IT.

Un număr de companii au construit capacități de calcul bazate pe centre de date enorme în toată lumea pentru a susține ofertele de servicii web (căutare, mesagerie instant, comerț electronic). Cu această infrastructură de calcul, aceste companii sunt deja în poziția de a oferi aplicații software pe bază cloud.

Soluțiile software precum aplicațiile ERP (Enterprise Resource Planning - planificarea resurselor întreprinderii), au fost disponibile până acum numai întreprinderilor mari cu bugete IT consistente. Totuși, companiile care vând astfel de soluții pot acum să le ofere acum și întreprinderilor mici și mijlocii făcând aplicațiile lor foarte complexe și foarte scumpe disponibile ca servicii software online. Capacitatea SaaS de a oferi aplicații scumpe la prețuri convenabile va continua să se accelereze.

Nu în ultimul rând, trebuie avut în vedere faptul că la nivelul Uniunii Europene sunt constituite grupuri de lucru privind susținerea și adoptarea modelului Cloud Computing în administrația publică și în economie în general. De asemenea, sub tutela Comisiei Europene a fost elaborată și publicată în Septembrie 2012 Strategia Europeană privind Cloud Computing. Această strategie promovează adoptarea rapidă a modelului Cloud Computing în toate sectoarele economiei. Mai mult decât atât, o serie de țări membre ale Uniunii Europene au realizat deja pași consistenti în implementarea și operarea modelului Cloud Computing pentru serviciile guvernamentale.

2.3 Reglementari și recomandări la nivel UE

În septembrie 2012, Comisia Europeană a adoptat o strategie pentru „Valorificarea cloud computingului în Europa”. Strategia subliniază acțiunile pentru asigurarea unui câștig net de 2,5 milioane de noi locuri de muncă în Europa și o creștere anuală de 160 miliarde a PIB-ului UE (circa 1%), până în 2020. Strategia este concepută pentru a accelera și crește utilizarea cloud computing-ului în economie. Această strategie a fost rezultatul unei analize a politicii generale, a peisajului de reglementare și tehnologic și o consultare a părților interesate, pentru a identifica ce este necesar să se realizeze pentru a valorifica la maximum potențialul pe care cloud-ul îl poate oferi. Acest document stabilește acțiunile cele mai importante și urgente și reprezintă un angajament politic al Comisiei care servește drept apel pentru ca părțile interesate să participe la implementarea acestor acțiuni.

Autoritățile publice au un rol important de jucat în crearea unui mediu cloud de încredere în Europa. Acestea au posibilitatea de a-și utiliza poziția de achizitor major pentru a promova dezvoltarea și adoptarea cloud computing-ului în Europa, pe baza tehnologiilor deschise și a platformelor sigure. Stabilirea unui cadru clar și solid pentru adoptarea cloud-ului de către sectorul public le va oferi utilizatorilor internaționali siguranța unui acces fiabil și va face din Europa un pol activ al inovării în materie de servicii cloud. În plus, adoptarea unor soluții de cloud fiabile de către achizitorii publici ar putea încuraja IMM-urile să adopte și ele acest tip de soluții.

De asemenea, există îngrijorări legate de faptul că impactul economic al cloud computing-ului nu își va atinge întregul potențial decât dacă tehnologia este adoptată atât de autoritățile publice, cât și de întreprinderile mici și mijlocii (IMM-uri). În ambele cazuri, până în prezent adoptarea este limitată din cauza dificultății de a evalua riscurile adoptării cloud-ului.

În vederea atingerii acestor obiective, Comisia Europeană va lansa trei acțiuni specifice în domeniul cloudului:

- Acțiunea-cheie 1: deschiderea unui drum prin jungla standardelor
- Acțiunea-cheie 2: clauze contractuale și condiții sigure și echitabile
- Acțiunea-cheie 3: instituirea unui parteneriat european pentru cloud pentru a face din sectorul public un motor de inovare și dezvoltare.

Acțiunea-cheie 1 – deschiderea unui drum prin jungla standardelor

O utilizare pe scară mai largă a standardelor, certificarea serviciilor cloud pentru a demonstra că respectă aceste standarde și aprobarea certificatelor de către autoritățile de reglementare, ca probă a respectării obligațiilor legale, vor contribui la avântul cloudului.

În prezent, vânzătorii individuali sunt tentați să lupte pentru obținerea unei poziții dominante prin inducerea captivității clienților și descurajarea abordărilor standardizate, la nivel de sector. În pofida numeroaselor eforturi de standardizare conduse, în cea mai mare parte de furnizori, cloud-urile se pot dezvolta într-o direcție care nu presupune interoperabilitate, portabilitatea datelor și reversibilitate, adică tocmai caracteristicile esențiale pentru evitarea captivității clienților.

Standardele pentru cloud vor avea efect și asupra părților interesate din afara sectorului TIC, în special asupra IMM-urilor și a utilizatorilor și consumatorilor din sectorul public. Astfel de utilizatori sunt rareori în măsură să evalueze corectitudinea declarațiilor furnizorilor privind aplicarea standardelor, interoperabilitatea cloudurilor sau ușurința cu care datele pot fi deplasate de la un furnizor la altul. Din acest motiv, este necesară o certificare independentă, care suscită încredere.

Au fost deja demarate acțiuni de standardizare și de certificare a cloud computing-ului. Administrația Federală Institutul Național de Standarde și Tehnologie din SUA (U.S. National Institute for Standards and Technology - NIST) a publicat o serie de documente, inclusiv un set de definiții acceptate pe scară largă. Institutul European de Standardizare în Telecomunicații (ETSI) a instituit un grup „cloud” pentru a evalua nevoile de standardizare în materie de cloud și conformitatea cu standardele de interoperabilitate. Este clar că va fi nevoie de inițiative suplimentare vizând stabilirea de standarde. Cu toate acestea, prioritatea actuală constă în implementarea standardelor existente pentru a crește încrederea în cloud computing prin intermediul unor pachete de servicii comparabile. Pe lângă identificarea standardelor respective, este necesară o certificare a conformității.

Numeroase organizații (și, cu siguranță, toate marile organizații) au nevoie de o certificare a conformității sistemelor lor informațice cu cerințe juridice și de audit și doresc ca aplicațiile și sistemele lor să fie interoperabile. Comisia:

- va promova ofertele de servicii de cloud fiabile și de încredere, însărcinând ETSI să elaboreze până în 2013, prin cooperare transparentă și deschisă cu părțile interesate, o hartă detaliată a standardelor necesare (printre altele, pentru securitate, interoperabilitate, portabilitatea datelor și reversibilitate).
- va crește încrederea în serviciile de cloud computing prin recunoașterea, la nivelul UE, a specificațiilor tehnice pentru protecția datelor cu caracter personal și a datelor cu caracter sensibil în general, în domeniul TIC, în conformitate cu noul regulament privind standardizarea europeană
- va lucra împreună cu ENISA și alte organisme relevante pentru a sprijini dezvoltarea de sisteme de certificare voluntară la nivelul UE, în domeniul cloud computingului (inclusiv în ceea ce privește protecția datelor), și crearea unei liste a acestor sisteme până în 2014.
- va aborda problemele ecologice pe care le pune creșterea utilizării cloudului, convenind cu sectorul vizat criterii armonizate de măsurare a consumului de energie, a consumului de apă și a emisiilor de carbon ale serviciilor de cloud până în 2014.

Acțiunea-cheie 2: Clauze contractuale și condiții sigure și echitabile

De regulă, în domeniul informaticii, acordurile de externalizare făceau obiectul unei negocieri și vizau stocarea datelor, instalațiile de procesare și servicii definite și descrise în detaliu de la început. Pe de altă parte, contractele de cloud computing creează în esență un cadru în care utilizatorul are acces la capacități informațice cu o scalabilitate și flexibilitate infinită, în funcție de necesitățile sale. Cu toate acestea, în prezent, flexibilitatea mai mare a cloud computingului în comparație cu externalizarea tradițională este adesea contrabalansată de siguranța redusă a clientului, cauzată de contractele insuficient de specifice și de echilibrate cu furnizorii de cloud.

Din cauza complexității și a incertitudinii cadrului juridic aferent, furnizorii de servicii de cloud utilizează deseori contracte complexe sau acorduri privind nivelul serviciilor care au clauze extinse de declinare a răspunderii. Utilizarea contractelor standard de tipul „dacă îți convine bine, dacă nu, nu” (take-it-or-leave-it) îi permite furnizorului să facă economii, însă adesea utilizatorul, și în special utilizatorul final, găsește condițiile inacceptabile. Astfel de contracte pot impune de asemenea alegerea legislației aplicabile sau pot interzice

recuperarea datelor. Chiar și întreprinderile mai mari nu au decât puțină putere de negociere și, deseori, contractele nu prevăd răspunderea pentru integritatea sau confidențialitatea datelor, ori pentru continuitatea serviciului.

În ceea ce-i privește pe utilizatorii profesioniști, elaborarea clauzelor contractuale tip pentru acordurile privind nivelul serviciului în domeniul cloud computingului s-a dovedit a fi una dintre problemele cele mai sensibile în cadrul procesului de consultare. Acordurile privind nivelul serviciului determină relația dintre furnizorul de cloud și utilizatorii profesionali și se află la baza încrederii pe care utilizatorii serviciilor de cloud o pot avea în capacitatea unui furnizor de cloud de a furniza servicii.

În ceea ce-i privește pe consumatori și întreprinderile mici, Comisia a prezentat, în cadrul acțiunilor din Agenda digitală vizând creșterea încrederii în mediul digital, o propunere de regulament privind legislația europeană comună în materie de vânzări, care abordează multe dintre obstacolele generate de diferențele dintre legislațiile naționale, punând la dispoziția părților contractante un set de reguli uniforme. Propunerea conține norme adaptate la furnizarea de „conținut digital” care acoperă anumite aspecte ale cloud computingului.

Pentru chestiunile care nu țin de legislația europeană comună în materie de vânzări, sunt necesare acțiuni complementare specifice pentru a garanta că celelalte aspecte contractuale relevante pentru serviciile de cloud computing pot fi de asemenea acoperite printr-un instrument opțional similar. Aceste acțiuni complementare trebuie să acopere aspecte precum conservarea datelor după încetarea contractului, divulgarea și integritatea datelor, amplasarea și transferul datelor, răspunderea directă și indirectă, dreptul de proprietate asupra datelor, modificarea serviciului de către furnizorii de cloud și subcontractarea.

Deși legislația UE existentă protejează utilizatorii serviciilor de cloud, adesea consumatorii nu își cunosc drepturile și, în special, care sunt legile și jurisdicțiile aplicabile în materie civilă și comercială, în special când este vorba de chestiuni care țin de dreptul contractual.

În cursul consultării, elaborarea de condiții contractuale tip a fost identificată ca soluție pentru depășirea acestor probleme. Utilizatorii industriali și furnizorii și-au exprimat opțiunea pentru acorduri de autoreglementare sau standardizare. În ceea ce privește contractele cu consumatorii și întreprinderile mici, pentru a crea contracte clare și echitabile în materie de cloud computing, poate fi necesar să se elaboreze condiții și clauze contractuale tip bazate pe un instrument opțional de drept contractual. Identificarea și diseminarea celor mai bune practici privind clauzele contractuale-tip vor accelera adoptarea tehnologiei de cloud computing, prin creșterea încrederii potențialilor clienți.

Luarea unor măsuri adecvate cu privire la clauzele contractuale poate de asemenea contribui la asigurarea protecției datelor, care este un aspect de o importanță crucială. După cum s-a menționat mai sus, propunerea de regulament privind protecția datelor cu caracter personal va garanta un nivel ridicat de protecție a persoanelor fizice, prin asigurarea continuității protecției atunci când datele sunt transferate în afara UE și a SEE, în special prin clauze contractuale tip aplicabile transferurilor internaționale de date și prin crearea condițiilor necesare pentru adoptarea unor norme corporative obligatorii propice cloud computingului. Aceste modificări vor garanta că normele UE în materie de protecție a datelor iau în considerare realitățile geografice și tehnice ale cloud computingului. Până la sfârșitul anului 2013, Comisia:

- va elabora, împreună cu părțile interesate, clauze contractuale tip pentru acordurile privind nivelul serviciului aplicabile contractelor dintre furnizorii de cloud și utilizatorii de cloud profesionali, luând în considerare acquis-ul UE în curs de elaborare în acest domeniu.
- va propune, conform comunicării privind legislația europeană comună în materie de vânzări, condiții și clauze contractuale tip consumatorilor și întreprinderilor mici pentru aspectele care țin de propunerea în cauză.
- Va avea ca obiectiv standardizarea termenilor contractuali și a condițiilor cheie, oferind cele mai bune practici în materie de clauze contractuale pentru serviciile de cloud în ceea ce privește aspectele legate de furnizarea de „conținut digital”.
- va însărcina un grup de experți, creat în acest scop și cuprinzând reprezentanți ai sectorului, să definească, până la sfârșitul anului 2013, pentru acele aspecte ale cloud computingului care nu țin de legislația europeană comună în materie de vânzări, clauze contractuale și condiții pentru consumatori și întreprinderile mici, pe baza unui instrument opțional similar.

- va facilita participarea Europei la creșterea globală a cloud computingului prin: revizuirea clauzelor contractuale tip aplicabile transferului de date cu caracter personal către țări terțe și adaptarea acestora la serviciile de cloud, după necesități, și prin invitarea autorităților naționale de protecție a datelor să aprobe norme corporative obligatorii pentru furnizorii de cloud.
- va colabora cu industria de profil pentru a conveni asupra unui cod de conduită pentru furnizorii de cloud computing pentru a sprijini o aplicare uniformă a normelor de protecție a datelor, care poate fi transmis grupului de lucru „articolul 29” pentru avizare, în vederea asigurării certitudinii juridice și a coerenței dintre codul de conduită și legislația UE.

Acțiunea cheie 3 – Promovarea rolului de lider al sectorului public prin Parteneriatul european pentru cloud

Sectorului public îi revine un rol important în configurarea pieței de cloud computing. În calitate de cel mai mare cumpărător din UE de servicii informatice, sectorul public poate stabili cerințe stricte privind caracteristicile, performanța, securitatea, interoperabilitatea și portabilitatea datelor, precum și de conformitate cu exigențele tehnice. Acesta poate, de asemenea, să stabilească cerințe de certificare. Câteva state membre au lansat inițiative naționale, cum ar fi Andromede în Franța, G-Cloud în Regatul Unit și Trusted Cloud în Germania. Dar din cauză că piața sectorului public este fragmentată, cerințele acestuia au un impact redus, integrarea serviciilor este scăzută, iar cetățenii nu obțin cel mai bun raport calitate-preț. Gruparea cerințelor publice ar putea crește eficiența, iar cerințele sectoriale comune (de exemplu, privind e-sănătatea, îngrijirile sociale, asistența pentru autonomie la domiciliu și serviciile de e-guvernare cum ar fi datele deschise) ar putea reduce costurile și ar permite interoperabilitatea.

Sectorul privat ar beneficia, de asemenea, de servicii de mai bună calitate, de concurență sporită, de standardizare rapidă și de o mai mare interoperabilitate, precum și de oportunități de piață pentru IMM-urile din sectorul tehnologiei avansate.

Drept urmare, în acest an, Comisia creează un Parteneriat european pentru cloud, cu scopul de a oferi un cadru pentru inițiativele similare lansate la nivelul statelor membre. Acest parteneriat va reuni experți ai întreprinderilor vizate și utilizatori din sectorul public, care vor elabora, într-un mod deschis și complet transparent, cerințe comune privind achizițiile publice în domeniul cloud computingului. Parteneriatul nu are ca obiectiv crearea unei infrastructuri fizice de cloud computing. Prin cerințele privind achizițiile, care vor fi promovate de statele membre participante și de autoritățile publice în vederea utilizării pe întreg teritoriul UE, obiectivul este mai degrabă de a garanta că oferta comercială din Europa este adaptată nevoilor europene. Parteneriatul va permite de asemenea să se evite fragmentarea și să se garanteze că utilizarea cloudului public este interoperabilă și sigură, securizată, ecologică și pe deplin conformă cu normele europene, de exemplu în domeniul protecției datelor și al securității. Sub supravegherea unui comitet director, parteneriatul va regrupa autorități publice și consorții de întreprinderi care vor colabora pentru a pune în aplicare o acțiune de achiziție pre-comercială destinată:

- să identifice cerințele sectorului public în materie de cloud computing; să elaboreze specificații pentru achizițiile din domeniul IT și să conducă la obținerea unor implementări de referință pentru demonstrarea conformității și a performanței.
- să avanseze în direcția achizițiilor comune de servicii de cloud computing, efectuate de către organismele publice pe baza noilor cerințe comune ale utilizatorilor.
- să elaboreze și să aplice alte măsuri care necesită o coordonare cu părțile interesate, astfel cum se prevede în prezentul document.

2.4 Bariere de adoptare

Barierile majore pentru adoptarea cloud computingului sunt lipsa unui cadru de reglementare specific și îngrijorările cu privire la securitate și confidențialitate. Asigurarea unui comportament de încredere al clienților și al furnizorilor este un aspect important. Securitatea a fost întotdeauna o problemă importantă a managerilor IT, iar protecția informațiilor personale, științifice, comerciale și a proprietății intelectuale trebuie să fie asigurată de către furnizorii de servicii cloud.

O metodă universal valabilă pentru a asigura ultimele tehnologii de securitate, confidențialitate și încredere nu este nici adecvată, nici posibilă. Fiecare modalitate de utilizare a tehnologiei cloud computing trebuie să fie

evaluată critic și cu mare atenție și luată în considerare în ceea ce privește amenințările identificate, riscurile și cerințele de soluționare a conflictelor.

Pentru a consolida contribuția lor la informațiile reglementate și sensibile, furnizorii de servicii cloud trebuie să definească limitele și responsabilitățile, observând ce funcții și politici de securitate și de management al informațiilor asigură ei, și ce management al informațiilor și ce securitate trebuie asigurate în plus de către client sau alt furnizor de servicii partener. În mod tipic, acordurile de nivel de servicii (SLA) trebuie să reflecte această împărțire.

2.4.1 Constituirea unui cadru de reglementare specific

Lipsa unui cadru de reglementare specific generează reticență în privința adoptării conceptului de Cloud Computing, mai ales la nivelul instituțiilor publice. La nivelul organizațiilor private limitele de autoritate în privința opțiunilor legate de soluții tehnice și tehnologii permit o mai mare flexibilitate, deci o adoptare mai rapidă a soluțiilor și conceptelor noi. Pe de altă parte, în sectorul public limitele de autoritate date de structura ierarhică centralizată fac necesară inițiativa și coordonarea la nivel central.

Principalul mod de exprimare a inițiativei și coordonării la nivel central în privința cloudului este elaborarea unei strategii și a unui cadru de reglementare specific, care:

- să definească și să delimiteze rolurile entităților implicate; un aspect esențial în definirea acestor roluri este definirea rolului de evaluator și auditor al serviciilor de tip cloud guvernamental, rol atribuit guvernului
- să definească criteriile de securitate, performanță și funcționalitate care trebuie satisfăcute în furnizarea de servicii de tip cloud; aceste criterii trebuie, pe de o parte, să asigure încrederea în aceste servicii, iar pe de altă parte să asigure costuri eficiente ale serviciilor prin crearea unui mediu competitiv pentru furnizorii de astfel de servicii;
- să definească modalitatea de utilizare a serviciilor de tip cloud;

2.4.2 Securitatea

Un număr de aplicații curente de cloud computing presupun servicii oferite către consumatori finali, inclusiv e-mail și rețele sociale. Aceste servicii colectează și stochează volume mari de terabytes de informații personale, în centrele de date în toate țările din lume. Protecția datelor personale și gestionarea problemelor de confidențialitate pot determina succesul sau eșecul multor servicii cloud.

Problemele de securitate și de confidențialitate sunt complicate de amplasarea datelor în mai multe jurisdicții diferite cu niveluri diferite de protecție. Interceptarea și alte activități de supraveghere ale agențiilor guvernamentale reprezintă o altă problemă. Au existat instanțe în trecut când activitățile de strângere de informații au fost la limita spionajului comercial. Pe de altă parte, accesul legitim al agențiilor de aplicare a legii poate fi dificil. Protecția proprietății intelectuale, mai ales în ceea ce privește protecția drepturilor de autor, va pune și aceasta probleme. Au existat deja încercări de a face companiile de servicii de Internet (ISP) responsabile pentru împiedicarea partajării neautorizate de materiale protejate de drepturile de autor. Nu este încă clar cum vor fi soluționate aceste probleme în mediul cloud.

Asigurarea securității informațiilor în mediul cloud computingului impune trei niveluri de securitate: securitatea rețelei, securitatea serverului și securitatea aplicației. Aceste nevoi de securitate sunt prezente și în infrastructura internă și sunt afectate direct de politicile de acces și fluxurile de lucru ale unei entități care își deține și gestionează resursele. Când o entitate trece pe cloud computing, apar provocări de securitate la fiecare dintre cele trei niveluri, cât și cele care privesc operarea activității economice și persoanele implicate în managementul sistemului. Deși aceste provocări de securitate sunt exacerbate prin cloud computing, nu sunt produse de acesta.

Criptarea nu este o soluție completă, pentru că datele trebuie să fie decriptate în anumite situații – astfel încât să se poată prelucra și să se poată duce la îndeplinire funcțiile normale de management de date, de indexare și de sortare. Astfel, deși datele în tranzit și datele stocate sunt efectiv criptate, nevoia de a decripta, în general de furnizorul de servicii cloud, poate fi o problemă de securitate.

Totuși serviciile cloud pot fi securizate prin filtrarea e-mailurilor (inclusiv back-up și spam), filtrarea conținutului web și gestionarea vulnerabilităților, toate acestea îmbunătățind securitatea. Unele amenințări sunt mai bine tratate de centrele de date de dimensiuni mari (de exemplu atacuri de tipul Distributed Denial of Service, care presupun încercări de a împiedica un sit de internet sau un serviciu să funcționeze). Aplicațiile care rulează în cloud sunt mai puțin vulnerabile la astfel de atacuri.

Managementul identității și al accesului și politicile asociate pentru utilizarea serviciilor cloud trebuie să fie echivalente practicilor curente de la nivelul întreprinderilor și să asigure capacitatea de a interopera cu aceste aplicații existente.

2.4.3 Confidențialitatea

Legile și reglementările cu privire la confidențialitate și protecția datelor, precum acelea ale țărilor din Uniunea Europeană și Programul US Safe Harbor, necesită cunoașterea locației datelor stocate în orice moment. Datele pot fi stocate în mai multe copii, în mai multe jurisdicții cu diverse tipuri de legislație cu privire la confidențialitate și protecția datelor. Aceasta este o problemă particulară pentru agențiile guvernamentale care procesează informațiile personale. Această problemă poate încuraja unii furnizori de servicii cloud să își situeze centrele de date în jurisdicții cu cerințe juridice minime (posibil în afara Europei și a SUA). Totuși utilizatorii de servicii cloud pot avea nevoie de protecția juridică asigurată de o legislație puternică cu privire la protecția datelor cu caracter personal.

Din nou, integrând comportamentul convenit între furnizor și client, demonstrând unul altuia pentru fiecare tranzacție că acordul este menținut, dar și un registru care poate fi controlat din exterior, va naște încredere și susținere în utilizarea serviciilor cloud.

2.4.4 Încrederea

În ultimă instanță totuși, asimilarea serviciilor cloud depinde de încrederea pe care clientul și furnizorii o au unii față de ceilalți. Încrederea trebuie să fie aplicabilă legal sau pe baza standardelor dacă activează în practică. Încrederea în cloud computing trebuie să utilizeze o metodă integrată care se construiește pe ideile care susțin Acordurile de nivel de servicii (SLAs):

- Acordul asupra politicilor pentru partajarea informațiilor înainte de orice interacțiune între client și furnizorii de servicii cloud. Acest lucru se poate face prin utilizarea de contracte sau SLA care definesc accesul la serviciile specializate sau politici de control al accesului.
- Dovezi riguroase ale comportamentului convenit (definit în SLA) între furnizorul de servicii cloud și clienții lui pe durata interacțiunilor critice și după ce s-a ajuns la acorduri cu privire la politici.
- Asigurarea că arhive verificabile și controlabile din exterior cu privire la „buna conduită” sunt păstrate, de la început până la sfârșit.

Luate separat, aceste măsuri sporesc încrederea părților. Numai atunci când toate cele trei componente sunt corelate, se atinge un sistem în care se poate avea cu adevărat încredere.

2.4.5 Blocarea serviciilor și standardele

Blocarea serviciilor este o problemă pentru unii utilizatori. Din cauza lipsei de standardizare, consumatorii nu pot extrage cu ușurință propriile date și programe și merge spre un alt furnizor din cloud. Succesul internetului se datorează adopției standardelor deschise și dezvoltării de software open source. Pentru ca cloud computing să fie un succes, guvernele trebuie să promoveze standarde internaționale deschise pentru Cloud, astfel încât utilizatorii să poată schimba furnizorii de servicii Cloud cu costuri și riscuri minime.

2.4.6 Alte probleme

S-au exprimat preocupări cu privire la:

- Congestia transferurilor de date – pe măsură ce aplicațiile devin mai intense din punctul de vedere al datelor și computația este distribuită în cloud, nevoia de a muta volume largi de date poate crește;

- Costurile traficului de rețea – unele organizații au modele de cost care restrâng sau sancționează accesul la facilitățile externe și din străinătate;
- Pierderea datelor – dacă un serviciu cloud pierde date, aceasta este o problemă majoră pentru utilizatorii care se bazează pe serviciu;
- Incapacitatea consumatorilor de a se redresa după o problemă majoră.

3. Impact pentru sectorul privat

3.1 Impact la nivelul sectorului financiar

Industria serviciilor financiare continuă să adopte *Cloud Computing*-ul. Nu se pot nega avantajele mutării în cloud – costuri reduse, scalabilitate și flexibilitate mai mare, mobilitate crescută și implementare mai rapidă etc.

Cerința de protejare a informațiilor clienților, încă reprezintă o barieră pentru multe firme. Faptul că înregistrările și informațiile clienților trebuie securizate și păstrate confidențial cauzează mari dificultăți acestei industrii. Ar trebui precizată necesitatea companiilor de a proteja înregistrările clienților împotriva oricăror amenințări sau cât și a acceselor neautorizate care ar putea afecta sau cauza inconveniențe clienților în cauză.

Studiul Ernst & Young denumit **2012 Global Information Security Survey** a arătat că 59% dintre respondenți au spus că folosesc sau planifică să folosească servicii de cloud. Cu toate acestea, peste 33% nu au întreprins nicio măsură pentru administrarea sau diminuarea riscurilor de securitate.

Provocările pe care le introduce cloud computing-ul influențează industria serviciilor financiare în următoarele moduri:

- Companiile sunt reticente, considerând posibilitatea compromiterii datelor dintr-un cloud public precum și posibilitatea monetizării acestor date (de clienți) de către furnizorii de cloud. De exemplu, angajați din trezorerie (traders) din diferite companii de profil ar fi foarte circumspecți în a-și ține strategiile de tranzacționare într-un cloud, temându-se de faptul că un competitor de pe același cloud ar putea obține acces la ele. Similar, manageri de portofolii și analiști de risc sunt reticenți cu privire la detalii de alocarea a activelor sau a strategiilor de referință a relansării a unei companii.
- De vreme ce companiile de servicii financiare operează într-un mediu ultra reglementat, orice pierdere sau compromitere a datelor clienților sau oricare din scenariile de mai sus poate avea implicații și repercursiuni reputaționale și poate duce la procese colective din partea clienților.
- Managerii IT sunt de asemenea îngrijorați în ceea ce privește disponibilitatea aplicațiilor menținute în cloud. Furnizorii de servicii de tip cloud computing asigură serviciile în niște condiții standard, acestea neputând fi negociate efectiv de către un client, tinzând a fi evident în beneficiul furnizorilor, inclusiv oferind clienților doar garanții limitate. Imaginați-vă un scenariu în care un furnizor de servicii cloud computing șterge datele clienților sau oprește un serviciu sau o aplicație pe o perioadă de zile sau săptămâni, dintr-un motiv de încălcare a contractului, cum ar fi neplata temporară. Acest tip de scenariu ar crea multe probleme pentru o companie care nu ar avea pârghii reale de negociere într-un astfel de scenariu.
- Dependența de tehnologia furnizorului este un alt motiv de îngrijorare. Marea majoritate a furnizorilor de servicii cloud computing asigură accesul la resurse prin tehnologii proprii, interfețe patentate ale aplicațiilor, serviciilor web sau instrumente proprii de linie de comandă. Dacă o companie dorește să își schimbe furnizorul de servicii cloud computing, acest lucru ar presupune costuri ridicate doar pentru modificarea către noile interfețe și tehnologii, costuri care anulează tocmai avantajele utilizării acestui tip de serviciu.

Proprietatea Intelectuală

Companiile care și-au implementat servicii de cloud computing au observat cazuri în care diferite persoane au obținut acces neautorizat la datele aflate sub incidența Proprietății Intelectuale. Țintirea acestui tip de active valoroase are o tendință crescătoare. Cel mai probabil vom identifica în viitor metode suplimentare de tip atacuri persistente avansate (APTs – Advanced Persistent Threats) împotriva multor companii. Dat fiind

cantitatea mare de date ale clienților, industria de servicii financiare este o țintă viabilă și atractivă. Din această cauză, Proprietatea Intelectuală este mină de aur pentru hackeri.

Un atac reușit de acest tip, lansat împotriva serviciilor de cloud computing poate afecta la modul cel mai serios Proprietatea Intelectuală – și reputația companiilor. Au fost cazuri în care angajați au căzut victime și au permis ca încălcări de mare anvergură să se întâmple; aceștia au fost bine intenționați dar neștiutori. Mai mult decât atât, există întotdeauna pericolul unor atacuri intenționate din interior. Dacă un angajat lucrând la un furnizor de servicii de cloud computing decide să vândă date ale unui client celui care oferă mai mult, acest lucru ar determina un incident costisitor și jenant de compromitere a datelor pentru respectivul client.

Necunoașterea nu este acceptabilă

Ca și consumator de cloud computing, trebuie înțelese responsabilitățile ce revin clientului și să se țină cont că a te baza doar pe furnizorul de servicii de cloud computing nu este suficient. Multe organizații în necunoaștință de cauză se bazează pe acordurile privind nivelurile serviciilor (SLA - Service-level Agreement) cu furnizorul de servicii și presupun că aceștia sunt responsabili de securitatea datelor lor. Nu este acceptabil pentru o companie de servicii financiare să invoce necunoașterea acestor aspecte și să impute un incident către furnizorul de servicii.

Acum, că datele despre clienți și informația în general, pot fi oriunde într-un cloud digital, nu mai este îndeajuns să se ia în considerare aspectele de securitate doar prin prisma infrastructurii.

Conformitatea prin criptare

Companiile de servicii financiare ar trebui să folosească metode de criptare pentru a reduce riscul dezvăluirii și alterării datelor sensibile aflate în repaos sau în tranzit. Aceasta este una din cele mai bune metode de a menține informația în condiții de siguranță față de hackeri. Folosind această metodă, o pereche secretă de coduri digitale numită „cheie” este folosită pentru a cripta datele. Fără această cheie, datele nu pot fi decriptate.

Criptarea, protejează datele importante împotriva „ochilor curioși”, indiferent unde este informația stocată. Entitățile care încearcă să evite modul uzual de acces al datelor și protocoalele companiilor, vor obține astfel doar informații criptate.

Criptarea nu trebuie să aibă un efect negativ asupra utilizatorilor legitimi sau asupra clienților acestora, astfel încât aceștia să poată obține informațiile fără probleme. Însă, aceasta în sine reprezintă o problemă. Cine mai exact ar trebui să dețină cheile de criptare?

Gestionarea cheilor de criptare

Deseori, furnizorii de servicii de cloud computing care criptează datele clienților, dețin cheile de criptare. Cu toate acestea, revenim la situația expusă mai devreme. Dacă un hacker sau un angajat nemulțumit fură cheile, aceștia au acces la informații în formă necriptată.

Pentru a ajuta la rezolvarea acestei situații, *Gartner* recomandă clienților să rețină, să gestioneze local cheile de criptare și să se asigure că acestea sunt schimbate și distruse în mod corespunzător pentru a le menține secrete în timp.

Mai sunt și alte considerente de luat în calcul pentru industria financiară, atunci când adoptă o strategie de tip cloud computing. În primul rând, informația trebuie definită ca fiind de prim rang în interiorul cloud-ului. Mai presus de orice, informația trebuie protejată. Când se stabilesc strategiile pentru protejarea informației, trebuie luate în calcul cerințele de reglementare și trebuie faptul că cerințele referitoare la exportul datelor și restricțiile de rezidență sunt respectate.

Administrarea a astfel de cerințe poate fi descurajatoare pentru multe companii care nu au expertiză în cloud computing sau securitatea informațiilor. Lucrul cu un terț de încredere poate ajuta la acoperirea nevoilor, în același timp maximizând inovația și competitivitatea furnizată de către cloud.

Aceste recomandări vă vor ajuta la eliminarea îngrijorărilor legate de confidențialitatea și integritatea datelor pe măsură ce, îmbrățișând cloud-ul, migrați datele și aplicațiile. Cu cât petreceți mai puțin timp cu îngrijorările legate de securitate, cu atât puteți petrece mai mult timp cu strategiile de afaceri.

Un sondaj Internațional Data Group din 2010 a relevat că:

- 6% dintre CIO interpeleți au afirmat că reducerea de costuri este o prioritate critică de business pentru viitor în cadrul board-ului
- 62% au afirmat că optimizarea resurselor și a proceselor de afaceri vor fi o prioritate
- 67% au prevăzut îmbunătățirea timpului de marketing pentru produse și servicii la fel de critică în anii următori.

O companie de servicii financiare care se bazează puternic pe serviciile IT poate beneficia de cloud computing în ciuda obiecțiilor menționate mai sus. Reducerile de cost percepute, ușurința scalării, un timp mai rapid de ajungere către piață și implementare a sistemelor, virtualizarea datelor din întreaga întreprindere ca și serviciu, standardizarea tehnologiei enterprise și abilitatea de a accesa date și aplicații de oriunde sunt toți factori critici care pot conduce companiile de servicii financiare la adoptarea cloud computing-ului.

Pentru companiile de servicii financiare există nenumărate oportunități de a beneficia de avantajele cloud computing, prin migrarea diferitelor aplicații în cloud. Aplicațiile auxiliare (non-core), precum cele pentru anumite procese de business - de recrutare, de facturare, de managementul deplasărilor, pot – și trebuie – în mod simplu mutate în cloud. Un număr de operațiuni de infrastructură, precum managementul centrului de date, stocarea acelor date și recuperarea lor în caz de dezastru, ar trebui de asemenea să se mute în cloud după o evaluare minuțioasă a ofertelor diversilor venditori și luând în calcul și flexibilitatea furnizorilor de cloud în documentarea contractelor. Deși foarte puține companii folosesc acum cloud computing pentru aplicațiile lor de bază, diferite arhitecturi de găzduire de tip IaaS ale furnizorilor de cloud, vor face ca mai multe companii să își mute aplicațiile în mediul cloud. De fapt, soluțiile principale, precum procesele de tip batch care rulează pe durata întregii zile, aplicațiile de analiză și raportare reprezintă prin caracteristicile lor, candidații perfecți pentru cloud computing.

3.2 Impact la nivelul sectorului educațional

Instituțiile din sectorul educațional adoptă sistemul Cloud, la fel cum o fac și celelalte organizații. Peste tot în lume, universitățile studiază serviciile Cloud computing prin cooptarea oamenilor de știință, dar și prin intermediul colaborărilor interuniversitare, străduindu-se să găsească calea cea mai potrivită de a folosi aceste servicii, date fiind preocupările legate de securitate. Drept urmare, putem vedea un interes crescut și o investiție pe măsură în soluții tip Cloud privat, dar și de interes public, specifice sectorului educațional. Compania Forrester a avut discuții cu directori IT axate pe gradul de adoptare a sistemului Cloud de către universități din S.U.A., Anglia, Australia, Noua Zeelandă și India, în primul rând legate de învățare, cooperare și cercetare iar, în al doilea rând, de administrare.

Rezultate cheie

În urma discuțiilor avute, Forrester a identificat cinci elemente cheie:

- Funcționalitatea, scalabilitatea și agilitatea sunt cele mai valoroase caracteristici ale unui sistem Cloud. Toți cei intervievați erau de părere că nu puteau construi un sistem funcțional fără să fi ieșit în pierdere din punct de vedere al costurilor asigurând aceeași viteză ca și furnizorii de Cloud și, în același timp, să redimensioneze resursele proporțional cu nevoile instituționale. În plus, implementările Cloud permit angajaților IT să-și concentreze eforturile pentru a lucra în mod direct cu departamentele academice și să aloce personal pentru alte nevoi tehnologice critice instituțiilor.
- Responsabilizarea angajatului și „punerea în umbră” a IT-ului sunt factori cheie în adoptarea unui sistem Cloud. Accesul direct al consumatorului la serviciile Cloud au făcut posibil ca profesorii cu spirit practic să acționeze în calitate de resursă IT și să creeze propriile lor sisteme Cloud prin intermediu serviciilor, ceea ce a furnizat infrastructură și aplicații într-un mod mai rapid și mai eficient din punct de vedere al costurilor decât prin intermediul centrului IT. Drept urmare, putem

vedea cum multe departamente, dar și angajați ai universităților simt nevoia să utilizeze aceste servicii.

- Liderii mari din domeniul IT preferă sisteme de Cloud private. Fie că sunt pentru cercetare sau pentru colaborare, acest tip de sisteme sunt preferate pentru educație. Toate universitățile intervievate si-au manifestat reținerea în a încredința orice fel de „proprietate intelectuală” sau date care ar putea fi prelucrate, unui serviciu terț.
- Universitățile au interese solide vizavi de Cloud-ul comunitar. În aceeași măsură în care colaborarea între universități continuă să crească ca și importanță, la fel crește și dorința de a-și uni eforturile sau de a participa împreună la același serviciu Cloud. Cel mai important lucru din interesul pentru acest model a fost acela de a sprijini cercetarea și procesul de învățare.
- Învățământul superior IT nu are încredere în securitatea sistemelor Cloud. Liderii IT ai universităților își exprimă neliniștea în legătură cu „proprietatea intelectuală” și datele studenților care ar putea ajunge pe mâini greșite; astfel, securitatea este pe primul loc ca motiv de respingere a sistemului Cloud. Facultatea cât și angajații IT au fost cu toții deschiși asupra înțelegerii mai bune a securității Cloud și au arătat bunăvoință de a folosi servicii Cloud, presupunând că furnizorul poate da asigurările potrivite.
- Universitățile vor parteneriate flexibile și de lungă durată cu furnizorii. Liderii IT ai universităților așteaptă ca furnizorul să înțeleagă învățământul superior, să fie expert în implementarea Cloud, să ofere sugestii și bune practici, dar și să fie deschis la dezvoltarea unei relații furnizor/universitate, în care fiecare parte are ceva de învățat de la cealaltă. Această relație trebuie să fie îndeajuns de flexibilă încât să permită schimbări și dezvoltări educaționale și de tehnologie pe perioada contractului.

Tehnologia Cloud se face cunoscută învățământului superior – cu anumite rețineri.

Acesul rapid la resurse, ajutorul obținut ușor și rapid și un model economic în care se plătește doar pentru ceea ce ai nevoie, toate acestea se fac simțite în lumea educației superioare care devine tot mai competitivă. Astfel, nu e deloc surprinzător faptul că serviciile Cloud au pătruns pe această piață foarte rapid. Forrester Consulting a descoperit că majoritatea marilor instituții de învățământ superior, experimentează serviciile Cloud după modelul celor folosite de marile companii. Adoptarea timpurie este de cele mai multe ori determinată de profesori și alți membri ai personalului având o gândire vizionară și o minte liberă și care, ei înșiși, pot presta servicii pentru un anumit curs sau proiect. Adoptarea formală de către personalul IT al universităților întârzie din cauza preocupărilor legate de siguranța „proprietății intelectuale”. Instituțiile își doresc mai multă flexibilitate în utilizarea tehnologiilor, dar sunt foarte preocupate de securitatea datelor, mai ales când este vorba de un sistem Cloud public - de fapt, de orice alt mediu găzduit. IT-ul formal acceptă mai degrabă soluții de tip Cloud privat care furnizează date dintr-un centru intern sau dintr-o platforma Cloud comunitar extinsă.

Instituțiile pro-Cloud demonstrează anumite caracteristici

Majoritatea marilor instituțiilor de învățământ superior studiază tehnologiile Cloud pe diferite nivele de interes.

Acelea care sunt cele mai favorabile sistemului Cloud demonstrează anumite caracteristici :

- *Cunoștințele și experiența liderului IT.* Universitățile care lucrează cel mai mult cu sistemul Cloud au un CIO sau un director IT care înțelege avantajele tehnologiei Cloud și are o experiență directă legată de lucrul cu un astfel de sistem. În multe cazuri, acești lideri au lucrat în sistemul corporatist înainte a de fi fost angajați într-un mediu universitar în care au cunoscut cerințele studenților. Aici, prioritatea lor este de a face cunoscută personalului, valoarea tehnologiei Cloud. Pentru a convinge, creează programe pilot pe care le fac cunoscute și altor departamente, împărțind studii de piață și evaluând rezultatele pentru procesul de învățare, robustețea tehnologiei și perspectivele celui care îndrumă.
- *Natura instituției.* Unele instituții au programe puternice de studiu în domenii foarte tehnice, beneficiind astfel la maxim de avantajele unor investiții importante în tehnologia Cloud. Studiile noastre arată că profesorii bine informați și deschiși în domeniul tehnologiei, sunt de departe cei mai buni candidați pentru punerea la punct a unui sistem Cloud pentru proiectele și acțiunile academice.

Această tehnologie poate ușura punerea la punct a unor instrumente pe care studenții și profesorii să le folosească pentru proiectele propuse pe parcursul unui curs și facilitează eliberarea resurselor la sfârșitul cursului.

- **Locația geografică.** Instituțiile S.U.A. par a fi mult mai avansate în ceea ce privește acceptarea și folosirea serviciilor și soluțiilor Cloud. Se pare că aceste instituții au un avans mult mai mare în descoperirea provocărilor și a eventualelor capcane oferite de Cloud, dar și în educarea factorilor de decizie din cadrul facultății sau al universității vis-a-vis de beneficiile aduse de Cloud. Lipsa de cunoștințe și de înțelegere cu privire la caracteristicile mediului Cloud a afectat instituțiile din majoritatea zonelor geografice în care am efectuat interviuri. Aceste diferențe nu sunt o piedică în calea instituțiilor în a descoperii tehnologia Cloud, dar fac progrese într-un ritm lent și precaut și în același timp păstrează contactul cu reușitele și provocările altor instituții.

Terminologia Cloud este adesea o provocare

În cadrul instituțiilor există confuzie în legătură cu ceea ce reprezintă Cloud. Forrester definește Cloud computing ca un sistem standardizat care include servicii, programe informatice sau acces la informații furnizate ca un serviciu de sine stătător pentru a cărui utilizare se plătește. Există trei nivele în structura Cloud:

- serviciul software (Software-as-a-service, **SaaS**)
- serviciul de infrastructură (infrastructure-as-a-service, **IaaS**)
- serviciul platformă (platform-as-a-service, **PaaS**).

Forrester definește cinci modele pentru dezvoltarea sistemelor Cloud:

- public
- privat intern
- privat găzduit virtual
- hibrid
- comunitar

Instituțiile de învățământ superior preferă modelul privat intern în centrele lor de date. Majoritatea instituțiilor cu care Forrester Consulting a avut discuții, folosesc un fel de formă hibrid, păstrând informațiile despre studenți pe servere proprii, iar email-urile și documentele legate de cercetare într-un sistem Cloud. Deoarece instituțiile colaborează, se așteaptă ca și platforma Cloud să crească, mai ales în ceea ce privește instituțiile de cercetare și cele care oferă cursuri de învățare online.

Universitățile explorează un spectru larg de tehnologii cloud

Instituțiile de învățământ superior nu sunt novice în tehnologiile Cloud. Unele dintre ele deja au avut un fel de tehnologie *Cloud* în ultimii cinci ani sau mai mult. Încrederea lor în platformele *Cloud* variază, lucru ce afectează dorința de a utiliza anumite tehnologii de Cloud, dar toate instituțiile explorează posibilitățile și au planuri de a adopta asta în zone diferite. Există următoarele puncte de vedere despre platformele Cloud:

- Platformele *Cloud* sunt utilizate pe scară largă. Utilizarea cea mai consistentă a tehnologiilor de tip *Cloud* de către toate universitățile intervievate a fost utilizarea de soluții SaaS pentru studenți, cum ar fi servicii de email. Alte utilizări comune - din nou, cea mai mare parte tot de tip SaaS - au avut la baza preocupări academice, cum ar fi laboratoare și mediile de colaborare folosite pentru o anumită perioadă de timp ca suport pentru anumite cursuri. Unele folosesc posibilități de urmărire, de colaborare și de gestionare, cum sunt platformele de tip *Cloud* eLearning, altele au preferat să-și configureze soluțiile respective pe serverele lor interne. Aceste utilizări de platforme *Cloud* publice se concentrează pe procesul de învățare, iar studenții sunt capabili să se conecteze utilizând toate dispozitivele lor.
- Departamentele IT în domeniul educațional preferă platforme *Cloud* private. Responsabilii IT din învățământul superior sunt foarte preocupați de drepturile pe proprietatea intelectuală și confidențialitatea datelor. Ca urmare, toți liderii IT ai instituțiilor au fost mult mai confortabili cu o platforma *Cloud* privat instalată și livrată printr-un centru de date din campusul universitar.
- Platformele *Cloud* publice și private vor fuziona în cele din urmă. În timp ce profesioniștii IT din educație preferă platforme *Cloud* privat, ei recunosc că acestea au limite și sunt deschise, astfel, la

completarea lor cu servicii de *Cloud* public. De exemplu, unele servicii necesită un volum ridicat de cereri și o funcționare fără întreruperi, cum ar fi optarea și înscrierea studenților la anumite cursuri, acestea fiind candidate perfecte pentru servicii *Cloud* public. Platformele hibride *Cloud* au, de asemenea, beneficii puternice în actul de predare, instituția putând suplimenta cu ușurință instruirea din clasă cu învățarea on-line.

- Platformele *Cloud* comunitare sunt populare în special pentru partajarea rezultatelor cercetărilor și articolelor. Unele universități lucrează împreună pentru a partaja spațiu de stocare și capacitățile de procesare. Grupuri de universități formează comunități pentru a facilita proiecte comune în care schimbul de informații este esențial.

Recomandari cheie

Având în vedere utilizarea tot mai susținută a serviciilor *Cloud* de către departamentele academice, precum și necesitatea de a schimba comportamentul departamentelor IT aliniindu-l criteriilor de agilitate și productivitate oferite de aceste servicii, liderii tehnici din departamentele IT ale instituțiilor din educație trebuie să-și concentreze eforturile asupra a trei domenii principale:

- 1) trecerea de la organizarea departamentului IT (Information Technology) către noțiunea de BT (Business Technology) pentru a consolida legăturile cu departamentele academice
- 2) trecerea infrastructurii interne către o platforma de *Cloud* privat
- 3) adoptarea unei platforme *Cloud* hibrid în viitor.

Specialiștii IT din învățământul superior trebuie să:

- recunoască faptul că departamentul IT nu mai este centrul de tehnologie al universității. Departamentul IT trebuie să devină mai orientat spre funcțional și să acționeze ca o resursă pentru departamentele academice și organizaționale ale universității. Astfel, acesta trebuie să dispună de relații puternice cu comunitatea academică și să migreze de la furnizarea de capabilități de tehnologie către o poziție de consiliere și consultanță cu privire la modul în care tehnologiile pot îmbunătăți misiunea academică.
- înceapă călătoria spre platformele *Cloud* privat cu o înțelegere a ceea ce face un *Cloud* privat. Virtualizarea nu este echivalentă cu o platformă *Cloud*. Acest lucru are implicații operaționale mai mari decât tehnologia în sine. Arhitectura platformei de *Cloud* privat ar trebui să fie în așa fel gândită încât să poată oferi o soluție care să ofere o experiență de utilizare similară cu soluțiile *Cloud* publice.
- verifice serviciile *Cloud*. Instituțiile trebuie să găsească metodele potrivite pentru a testa capabilitățile și performanțele platformei *Cloud* alese. Testele pot conține scenarii care să verifice securitatea soluției, rezistența la atacuri externe, protecția datelor, performanța etc.

Sursa: *"Cloud Bursts Into Higher Education" - A Forrester Consulting Thought Leadership Paper Commissioned By Cisco Systems*

3.3 Impact la nivelul sectorului telecomunicațiilor

O evoluție dramatică are loc în prezent în industria de telecomunicații. Operatorii de telefonie mobilă, fixă și broadband precum și furnizorii de servicii din întreaga lume operează pe infrastructuri de rețea de telecomunicații proprietare, învechite și costisitoare. Creșterea numărului și diversității de dispozitive mobile care accesează rețelele, nu numai pentru voce, ci și pentru multimedia și date, face ca traficul total să crească, în timp ce ARPU (*Average Revenue Per User*) a rămas constant sau chiar este în scădere. Cuplat cu faptul că pentru aceste rețele de telecomunicații au fost construite o multitudine de aplicații complexe, inflexibile, proprietare și specifice, precum și necesitatea de a servi cât mai multe companii, operatorii și furnizorii de echipamente trebuie să treacă de la un model tradițional, închis, către un cadru care este deschis, centrat pe consumator, care să permită dezvoltarea serviciilor mai rapid și cu costuri reduse.

Platformele *Cloud* sunt o continuare naturală a tendinței de virtualizare, tendință ce are o istorie care depășește 15 ani. Acest trend a ajuns acum la un punct critic în care se poate crea și livra valoare de business. Această valoare poate fi creată în trei direcții principale:

- Eficientizarea fluxurilor și serviciilor actuale
- Crearea de noi modele pentru furnizarea serviciilor curente
- Crearea în întregime de noi modele și servicii.

O mare varietate de jucători în domeniul telecomunicațiilor se grăbește să exploateze aceste oportunități de afaceri în ecosistemul *Cloud*. Furnizorii de top (Google și Amazon), integratorii de sistem, furnizorii de servicii și infrastructuri de *Cloud*, precum și alte companii, par dornici de a apuca o felie din plăcinta *Cloud*. De asemenea, furnizorii de servicii de comunicații (ISP) au recunoscut platformele *Cloud* ca sursă de noi venituri. O parte importantă dintre ei deja a făcut din serviciile de *Cloud* o parte integrantă din strategia lor de afaceri. Ca furnizori de rețele interconectate, companiile ISP au un avantaj unic față de alți jucători din piața *Cloud* și pot juca un rol-cheie în crearea de valoare pe partea tehnologiilor *Cloud*. Deși, doar câteva companii ISP generează o valoare semnificativă din servicii *Cloud*, acest lucru se va schimba dramatic în următorii ani. Companiile din domeniul telecomunicațiilor sunt în mod activ în căutarea de noi modele de servicii în *Cloud*.

Ceea ce noi numim acum *Cloud Computing* este rezultatul unei evoluții naturale din adoptarea pe scară largă a noțiunilor de virtualizare și arhitectură orientată spre servicii. Platformele *Cloud* sunt o evoluție în administrarea infrastructurii din centrele de date, în care conceptele au evoluat de la capacitatea de a gestiona hardware eterogen, software, aplicații - întâi în cadrul centrului de date, apoi la nivel de companie, iar acum cu platformele *Cloud*, la nivelul mai multor companii simultan. Platformele *Cloud* pot fi considerate ca un sistem de management recunoscut pentru capacitățile sale tehnologice, și este văzut de mulți ca un scop în sine. Din acest punct de vedere, *Cloud Computing* poate servi ca bun de larg consum pentru optimizarea IT.

Prin studiul nostru, am descoperit că firmele ISP - atât mari cât și cele mici, în toate zonele geografice – adoptă tehnologii *Cloud* ca o modalitate de a merge mai departe. Mai mult de trei sferturi dintre companiile ISP (în sondajul nostru) au indicat că au pilotat, adoptat sau implementat tehnologii *Cloud* în organizațiile lor. 94% dintre respondenți se așteaptă să facă acest lucru în următorii trei ani. Numărul de respondenți ISP care au implementat tehnologii sau platforme *Cloud* este de așteptat să crească brusc de la 11% în prezent la 41% în următorii trei ani.

Acest nivel de adoptare a platformelor *Cloud* nu se limitează la companiile ISP mari. Studiul de față a arătat că în timp ce un procent mai mare de companii ISP (cele cu venituri anuale mai mari de 20 de miliarde de USD), pilotează tehnologii *Cloud*, companiile ISP mici nu au rămas afară din joc. De fapt, 53% dintre companiile ISP cu venituri mai puțin de 1 miliard de dolari și 90% din cei cu venituri între 1 miliard USD și 20 de miliarde de USD, au adoptat *Cloud* într-o anumită măsură. În comparație cu organizații din alte industrii, companiile ISP investesc la rândul lor în servicii *Cloud* pentru a realiza noi surse de venit. Potrivit *Informa's Telecom Cloud Monitor*, numărul de companii ISP care oferă spre vânzare servicii *Cloud*, a crescut de la aproximativ 60 în 2009 la mai mult de 140 în primul trimestru al 2012. Mai mult, companiile ISP din întreaga lume au cheltuit aproape 14 miliarde de USD pe implementare de tehnologii *Cloud* în 2011. Prognozele pentru piața totală *Cloud* sunt foarte diverse, dar ele arată în mod constant că, în general, cheltuielile pe tehnologii *Cloud* sunt în creștere.

Sursa: The natural fit of Cloud with Telecommunications, IBM Global Business Services, Executive Report

3.4 Impact la nivelul sistemului de sănătate

În comparație cu alte industrii, sistemul de sănătate are o tehnologie care este subutilizată și care ar putea să contribuie la îmbunătățirea eficienței operaționale. Majoritatea sistemelor medicale se bazează pe arhivele medicale vechi, scrise pe hârtie.

Informațiile care sunt digitalizate nu sunt de obicei portabile, inhibând partajarea informațiilor în rândul diverșilor actori din domeniul sanitar. Utilizarea tehnologiei pentru a facilita colaborarea dintre medici și pacienți și între comunitățile medicale este limitată.

Industria sanitară trece spre un model de asigurare a îngrijirii medicale centrate pe informații, permis parțial de standardele deschise care susțin cooperarea, fluxurile de lucru cooperative și partajarea informațiilor. *Cloud Computingul* asigură o infrastructură care permite spitalelor, cabinetelor medicale, companiilor de asigurări și facilităților de cercetare să dețină resurse computaționale îmbunătățite, cu cheltuieli de capital mai reduse. *Cloud Computing-ul* satisface cerințele tehnologice cheie ale industriei medicale:

- permite accesul la cerere la bazele de date și facilitățile mari de stocare care nu sunt furnizate în mod tradițional în mediile IT.
- susține seturile mari de date pentru arhivele electronice din domeniul sănătății (EHR - Electronic Health Record), imaginile radiologice și datele genomice (o sarcină dificilă - de la departamentele IT are spitalelor).
- facilitează partajarea EHR între medicii autorizați și spitalele din diverse zone geografice, asigurând acces mai rapid la informații și reducând nevoia de a duplica testele.
- îmbunătățește capacitatea de a analiza și urmări informațiile (cu guvernanta adecvată a informațiilor), astfel încât datele cu privire la tratamente, costuri, performanță și studii de eficiență să fie analizate și utilizate.

Datele din sistemul sanitar au cerințe stringente de securitate, confidențialitate, disponibilitate pentru utilizatorii autorizați, trasabilitate de acces, reversibilitatea datelor și păstrare pe termen lung. De aceea, vânzătorii de *Cloud* trebuie să țină cont de acestea toate în timp ce respectă reglementările industriale și guvernamentale. Problemele de transformare a sistemelor IT în sisteme interoperabile au întârziat creșterea *Cloud Computingului* în industria sanitară.

Când se are în vedere o mutare către *Cloud Computing*, actorii din domeniul sanitar (cabinete medicale, facilități de cercetare, spitale etc.) trebuie să țină cont de tipul de aplicații care se mută în *Cloud* (aplicații clinice și neclinice). Aplicațiile clinice sunt formate din EHR, introducerea de date de către medici, și software pentru utilizare imagistică și farmacologică. Aplicațiile neclinice includ managementul ciclului de venituri, facturarea către pacienți, gestionarea statelor de plată, contabilizarea costurilor și gestionarea revendicărilor.

Actorii din sistemul de sănătate trebuie să aibă în vedere modelul serviciului *Cloud* (**IaaS** - Infrastructure as a Service, **PaaS** - Platform as a Service, sau **SaaS** - Software as a Service) care se adresează cel mai bine cerințelor business. În multe cazuri, **SaaS**, cu modelul business de plată la utilizare, va fi opțiunea economică cea mai atractivă, mai ales pentru cabinetele medicale mici, deoarece nevoia pentru personalul IT cu normă întreagă este eliminată împreună cu cheltuielile de capital asociate cu sistemul hardware, sistemele de operare și software. **PaaS** este opțiunea viabilă pentru instituțiile sanitare care au resurse de a dezvolta propriile soluții pe bază *Cloud*. Pentru instituțiile sanitare care caută o infrastructură mai scalabilă, **IaaS** oferă o soluție la cheie mai eficientă din punctul de vedere al costurilor care asigură scalabilitate cu flexibilitate, securitate, acorduri de nivel de servicii definite, salvarea și protecția datelor.

Beneficiile Cloud Computing pentru sistemul de sănătate

„Centricitatea pacientului” a devenit tendința cheie în furnizarea sistemului de sănătate și conduce la dezvoltarea constantă în adoptarea înregistrărilor medicale electronice (EMR), a înregistrărilor electronice privind sănătatea (EHR), a înregistrărilor personale privind sănătatea (PHR) și tehnologiilor legate de îngrijirea medicală integrată, siguranța pacientului, accesul punctelor de intervenție la informațiile demografice și clinice și suportul decizional clinic. Disponibilitatea datelor, fără a lua în considerare locația pacientului și a medicului, a devenit cheia atât pentru satisfacerea pacientului, cât și pentru rezultatele clinice îmbunătățite. Tehnologiile *Cloud* pot facilita în mod semnificativ această tendință.

Cloud Computing oferă beneficii semnificative pentru sectorul sistemului de sănătate: clinicile și spitalele solicită au acces rapid la sistemul computerizat și facilități mari de depozitare care nu sunt furnizate în configurațiile standard din domeniul IT. Mai mult decât atât, datele referitoare la sistemul de sănătate trebuie distribuite în diverse zone geografice, cauzând întârzieri semnificative în tratament și pierdere de timp. *Cloud-ul* înglobează toate aceste cerințe, furnizând astfel organizațiilor din sistemul de sănătate o șansă incredibilă de îmbunătățire a serviciilor pentru clienții și pacienții lor, de distribuire a informațiilor cu mai multă ușurință și de îmbunătățire a eficienței operaționale în același timp.

Cercetarea Clinică. Numeroși comercianți de produse farmaceutice încep să apeleze la *Cloud* pentru îmbunătățirea cercetării și dezvoltarea industriei de medicamente. Importanța din ce în ce mai mare a produselor biologice în procesul de cercetare fac din Cloud-based Computing „un aspect deosebit de important al R&D” – cercetare / dezvoltare. În prezent, companiile farmaceutice nu au capacitatea de a rula seturi mari de date - îndeosebi determinarea secvenței ADN - deoarece dimensiunea datelor poate depăși capacitatea calculatoarelor lor.

Înregistrări Medicale Electronice. Spitalele și medicii încep să ia în considerare evidențele medicale din bazele *Cloud* și serviciile de arhivare a imaginilor medicale, care sunt furnizate online. Obiectivul constă în descărcarea de sarcini a departamentelor IT ale spitalului și permiterea lor de a se concentra asupra susținerii altor elemente deosebit de importante (ex. adoptarea EMR și a sistemelor clinice îmbunătățite de susținere).

Telemedicină. Prin creșterea disponibilității tehnologiilor mobile și a dispozitivelor medicale inteligente, telemedicina s-a dezvoltat, incluzând nu numai tele-consultații și tele-operatii, dar și schimb de înregistrări medicale, videoconferințe și monitorizare la domiciliu.

Big Data. Organizațiile de sănătate revin la cloud computing pentru economisirea costurilor de stocare a hardware-ului pe plan local. Cloud-ul păstrează seturi mari de date pentru EHR-uri, imagini radiologice și date genomice pentru testările clinice ale medicamentelor. Încercarea de a distribui EHR în diverse zone geografice fără beneficiile de depozitare cloud, poate amâna tratarea pacienților.

Analitică. Cloud computing facilitează practica, iar informațiile și observațiile la scara populației sunt disponibile aproape în timp real. Această disponibilitate asigură cele mai actuale și complete observații, iar cunoștințele clinice sunt disponibile pentru susținerea deciziilor referitoare la furnizorul de servicii medicale și pentru a permite concentrarea asupra creării valorii legate de îmbunătățirea rezultatelor, mai degrabă decât asupra consumului. Informațiile cuprinse în Cloud pot fi, de asemenea, mai bine analizate și evaluate (prin guvernarea corectă a informațiilor) astfel încât datele referitoare la studiile privind tratamentele, costurile, performanța și eficacitatea, pot fi analizate și se poate conta pe acestea.

4. Securitatea în Cloud

4.1 Vulnerabilități

Pentru a identifica cele mai importante vulnerabilități legate de securitatea *Cloud*, CSA a efectuat un sondaj printre experții din domeniu. Pe baza acestui studiu s-a întocmit raportul final pentru anul 2013, raport în care au fost identificate următoarele nouă probleme critice ale securității *Cloud*, prezentate în ordinea severității lor:

- a) Compromiterea securității datelor
- b) Pierderea datelor
- c) Piratarea conturilor sau a serviciilor
- d) Nesiguranța API-urilor
- e) Blocarea serviciilor *Cloud*
- f) Persoane rău-intenționate din interiorul sistemului
- g) Abuz asupra serviciilor *Cloud*
- h) Insuficienta investigare și implicare (due-diligence)
- i) Probleme cu tehnologiile distribuite

Astfel, acest raport servește drept un ghid bine pus la punct de identificare a vulnerabilităților și care va ajuta atât utilizatorii cât și furnizorii *Cloud* în a lua decizii în cunoștință de cauză cu privire la diminuarea riscului într-un sistem *Cloud*. Acest studiu ar trebui să fie utilizat împreună cu ghidurile celor mai bune practici, "Ghidul de securitate pentru zone critice în *Cloud Computing V.3*" și "Securitatea văzută ca un Ghid de implementare a unui serviciu." Împreună, aceste documente vor oferi indicații prețioase pentru alcătuirea unor strategii complexe și adecvate securității *Cloud*.

4.1.1 Incălcarea securității datelor

Una dintre principalele preocupări ale oricărui CIO este că datele interne, sensitive și secrete ar putea ajunge în mâinile concurenței. Chiar dacă această problemă a existat și înainte de apariția calculatorului, tehnologia *Cloud* aduce cu ea numeroase alte căi de atac asupra informației. În noiembrie 2012, cercetătorii de la Universitatea din Carolina de Nord, Universitatea din Wisconsin și corporația RSA au lansat un document care descrie modul în care o mașină virtuală ar putea folosi un canal ascuns de informații pentru a extrage cheile private criptografice și a le folosi în alte mașini virtuale de pe același server fizic. În cele mai multe cazuri însă, un atacator nu va trebui să meargă atât de departe, adică până la compromiterea cheilor de criptare. Dacă un serviciu *Cloud* care deservește mai mulți clienți nu este proiectat corespunzător, atunci un „defect” sau o vulnerabilitate într-una din aplicațiile unui client ar putea permite escaladarea drepturilor de acces ale unui atacator nu doar la datele clientului respectiv, dar și a datelor altor clienți.

Consecințe

Deși atât pierderea cât și scurgerea de date reprezintă în egală măsură amenințări serioase pentru un sistem *Cloud*, din păcate măsurile pe care le putem lua pentru adresarea uneia ar putea-o agrava pe cealaltă. Mai exact, prin criptarea informațiilor se reduce impactul încălcării securității datelor, însă, în eventualitatea pierderii cheilor de decriptare se vor pierde de asemenea exact datele ce trebuiau protejate. În mod similar, dacă s-ar decide păstrarea unei copii locale necriptate a datelor pentru a reduce impactul unei astfel de pierderi, atunci ar crește șansele unei scurgeri a datelor.

4.1.2 Pierderea datelor

Atât pentru consumatori cât și pentru marile organizații, perspectiva pierderii permanente de informații este îngrijorătoare. Desigur, datele stocate în *Cloud* pot fi pierdute și din alte motive. Orice ștergere accidentală din partea furnizorului de *Cloud*, sau mai rău, un dezastru natural cum ar fi un incendiu sau un cutremur, ar putea duce la pierderi definitive ale datelor clienților, cu excepția cazului în care furnizorul păstrează copii ale acelor date.

În plus, sarcina de a evita pierderea informațiilor nu este doar a furnizorului. De exemplu, dacă un client își criptează datele înainte de a le stoca în *Cloud* și pierde cheia de decriptare, atunci acele date vor fi pierdute, iar vina este a clientului.

Consecințe

Conform noilor norme UE privind protecția datelor, distrugerea și coruperea datelor cu caracter personal sunt considerate forme de încălcare a securității datelor și necesită a fi notificate către organele competente.

În plus, multe dintre politicile de conformitate solicită organizațiilor să păstreze înregistrări sau alte documente de audit. În cazul în care o organizație stochează aceste date în *Cloud*, pierderea lor ar putea pune în pericol gradul de conformitate a organizației.

4.1.3 Piratarea conturilor sau a serviciilor

Deturnarea conturilor sau a serviciilor nu este ceva nou. Metode de atac precum phishing-ul, fraudă și exploatarea vulnerabilităților software sunt încă folosite și funcționează. Credențialele și parolele sunt adesea refolosite, ceea ce amplifică impactul unor astfel de atacuri. În acest context, soluțiile *Cloud* vin ca o nouă amenințare. Un atacator care obține acces la datele unei persoane sau unei organizații îi poate urmări activitățile și tranzacțiile, îi poate manipula datele, îi poate răspunde cu informații false și îi poate redirecționa clienții la site-uri ilegale. Astfel, un cont sau un serviciu piratat poate deveni un punct de plecare pentru a lansarea unor atacuri ulterioare.

În aprilie 2010, datorită unei vulnerabilități de securitate (Cross-Site Scripting – XSS), site-ul web Amazon a fost ținta unui atac ce a permis atacatorilor să obțină acces la credențialele site-ului. În 2009, multe sisteme Amazon au fost piratate și deturnate pentru a rula ca noduri de răspândire a botnetului Zeus.

Consecințe

Pirățiile de conturi și de servicii, de obicei reușite prin obținerea credențialelor de acces, rămân o amenințare de top. Astfel, atacatorii pot accesa de mai multe ori zonele critice ale serviciilor *Cloud*, permițându-le să compromită confidențialitatea, integritatea și disponibilitatea acestor servicii. Organizațiile ar trebui să fie conștiente de aceste tehnici, precum și de strategiile de protecție împotriva lor, pentru a limita daunele rezultate dintr-o astfel de breșă de securitate. Organizațiile ar trebui să interzică schimbul de credențiale între utilizatori și servicii, și să folosească tehnici puternice de autentificare acolo unde este posibil.

4.1.4 Interfețe și API nesigure

Furnizorii de *Cloud* propun un set de interfețe software (API) pe care clienții le folosesc pentru a interacționa și a gestiona serviciile *Cloud*. Prin urmare, securitatea și disponibilitatea serviciilor *Cloud* sunt dependente de securitatea acestor interfețe de bază. Începând cu autentificarea și controlul accesului și terminând cu criptarea și monitorizarea activității, aceste interfețe trebuie concepute astfel încât să protejeze atât împotriva accidentelor cât și a acțiunilor rău-voitore.

Mai mult, organizații și părți terțe se bazează adesea pe aceste interfețe pentru a oferi servicii de valoare clienților lor. Aceasta duce la o complexitate mărită a acestor interfețe; de asemenea, crește riscul deoarece organizațiile ar putea fi obligate să împartă credențialele cu terțe părți care implementează aceste API-uri.

Consecințe

În timp ce majoritatea furnizorilor fac eforturi pentru a garanta securitatea serviciului, este foarte important ca utilizatorii acelor servicii să înțeleagă implicațiile legate de securitate vizavi de folosirea, administrarea, orchestrarea și monitorizarea serviciilor *Cloud*.

4.1.5 Blocarea serviciilor (DoS, DDos)

Blocarea serviciilor este un atac menit să împiedice utilizatorii unui serviciu *Cloud* să acceseze propriile date sau aplicații. Prin forțarea serviciului să folosească cât mai multe resurse cum ar fi puterea procesorului, memoria, spațiul pe disc sau banda de rețea, atacatorul (sau atacatorii, dacă vorbim despre o blocare de serviciu distribuită) provoacă o încetinire considerabilă a sistemului, mergând până la lipsa unui răspuns, ceea ce duce la confuzia și chiar furia utilizatorului.

Deși atacurile de tip *DDoS* tind să genereze multa teamă și atenție din partea mass-media (mai ales când autorii acționează în numele unei idei politice – *hactivism*), acestea nu reprezintă singura formă de blocare a unui serviciu. Atacuri la nivel de aplicații pot ținti anumite vulnerabilități ale serverelor web, a celor de baze de date sau a altor resurse *Cloud* și, având avantajul dimensiunilor mici, în unele cazuri chiar mai mici de 100 de bytes, blochează serviciul.

Consecințe

Ca și consumatori, întreruperile serviciului nu doar ca devin frustrante, dar începem să ne întrebăm dacă, în ideea de a reduce costurile, chiar a meritat mutarea datelor importante în *Cloud*. Chiar mai rău, deoarece furnizorii de *Cloud* pot taxa clienții pe baza timpului de procesare și a spațiului folosit pe disc, există posibilitatea ca un eventual atac să determine sistemul folosit să folosească atât de mult timp pentru procesare încât să devină prea scump pentru client și atunci acesta va fi nevoit să-l oprească el însuși.

4.1.6 Insuficienta investigare și implicare (due-diligence)

Tehnologia *Cloud* s-a dovedit a fi un fel de “goana după aur”, în care multe organizații s-au grabit să găsească promisiunea unor costuri reduse, a unei eficiențe operaționale și a unei securități îmbunătățite. În timp ce toate acestea pot fi scopuri realiste pentru organizații care au resursele necesare pentru a adopta această tehnologie în mod corespunzător, prea multe companii s-au grabit să o adopte fără a o înțelege pe deplin.

Fără o bună înțelegere, aplicații sau servicii puse în *Cloud* și responsabilități operationale cum ar fi răspunsul la incidente, criptarea și monitorizarea securității, organizațiile ajung la nivele de risc necunoscute în moduri pe care nici ei înșiși nu le pot înțelege, dar care reprezintă de departe o abatere de la riscurile lor curente.

Consecințe

O organizație care se grăbește să adopte tehnologiile *Cloud* se expune unei serii de probleme. Probleme contractuale apar peste obligațiile privind răspunderea, creând astfel neînțelegeri între furnizorul serviciului și client. Expunerea în *Cloud* a aplicațiilor care depind de controale de securitate la nivel de rețea internă reprezintă un pericol atunci când acele controale dispar sau nu răspund așteptărilor clientului. Atunci când arhitecți nefamiliarizați cu sistemul *Cloud* proiectează aplicații pentru *Cloud*, apar probleme operaționale și de arhitectură.

Concluzia este ca organizațiile care doresc să utilizeze servicii *Cloud* trebuie să aibă resurse competente și să se asigure de o investigație, o înțelegere clară și o implicare constantă înainte de a lua această decizie.

4.1.7 Probleme cu tehnologiile distribuite

Furnizorii de servicii *Cloud* folosesc aceleași resurse (infrastructura, platformă, aplicații) pentru clienți multipli. Fie ca este vorba de componente de baza care alcătuiesc această infrastructură (ex. cache CPU, GPU, etc.) care nu sunt proiectate pentru o arhitectură multi-client (*IaaS*), de platforme redistribuite (*PaaS*) sau de aplicații multi-client (*SaaS*), amenințarea unor vulnerabilități comune există în toate modelele de livrare. Se recomandă o strategie de apărare bine pusă la punct și care trebuie să se desfășoare la nivel de resurse de calcul, stocare, rețea, aplicație și utilizator, fie că este vorba de un model de serviciu *IaaS*, *PaaS* sau *SaaS*. Secretul este acela că o singură vulnerabilitate sau greșeală de configurație poate compromite un întreg sistem *Cloud*.

Consecințe

Compromiterea unei componente a unei tehnologii comune mai multor clienți cum ar fi hipervizorul, o componenta a unei platforme sau o aplicație într-un mediu *SaaS*, înseamnă mai mult decât afectarea unui client. Această vulnerabilitate este periculoasă pentru că poate afecta un întreg sistem *Cloud*.

CA Technologies și Institutul Ponemon prezintă rezultatele studiului asupra securității *Cloud* ("*Security of Cloud Computing Providers Study*"). Această lucrare este a doua dintr-o serie de două părți despre situația securității în *Cloud*. Primul studiu aparut în mai 2010 se numea "Securitatea utilizatorilor *Cloud*" ("*Security of Cloud Computing Users*").

Sondajul a fost făcut pe 103 furnizori de servicii *Cloud* în SUA și 24 în șase țări europene, pentru un total de 127 de furnizori diferiți. Cei care au răspuns întrebărilor afirmă ca *SaaS* (55%) este serviciul *Cloud* cel mai folosit, urmat de *IaaS* (34%) și *PaaS* (11%).

65% dintre furnizorii de *Cloud* prezenți în acest studiu, au implementat resursele IT în *Cloud* public, 18% în *Cloud* privat și 18% sunt hibride.

Concluziile cele mai importante ale furnizorilor de *Cloud*

Un rezumat al celor mai importante rezultate ale studiului amintit mai sus:

- Majoritatea furnizorilor de *Cloud* intervievați nu văd securitatea serviciilor lor de *Cloud* ca un avantaj competitiv. Mai mult, nu consideră securitatea ca una dintre responsabilitățile cele mai importante și nu cred că produsele sau serviciile lor protejează și securizează în mod substanțial informațiile confidențiale ale clienților lor.
- Cei mai mulți furnizori de *Cloud* cred că securitatea *Cloud* este responsabilitatea clientului. De asemenea, spun că sistemele și aplicațiile lor nu sunt întotdeauna evaluate din punct de vedere al amenințărilor la adresa securității înainte de a fi furnizate clienților.

- Atenționare pentru cumpărători - în medie, furnizorii de tehnologii *Cloud* alocă cel mult 10% dintre resursele operaționale securității și cei mai mulți nu sunt convinși că cerințele legate de securitate din partea clienților sunt îndeplinite.
- Principalele motive pentru care clienții cumpără resurse *Cloud* sunt costurile reduse și dezvoltarea rapidă de aplicații. În schimb, securitatea îmbunătățită sau conformitatea cu reglementările nu reprezintă motive de a alege servicii *Cloud*.
- Cei mai mulți furnizori de *Cloud* prezenți la studiu recunosc faptul că nu au personal dedicat pentru supravegherea securității aplicațiilor, a infrastructurii sau a platformelor.
- Furnizorii de resurse *Cloud* private par să acorde o mai mare importanță și au un nivel mai ridicat de încredere în capacitatea organizației lor de a îndeplini obiectivele de securitate, față de furnizorii de servicii *Cloud* publice sau hybrid.
- În timp ce securitatea ca și serviciu oferit de *Cloud* este foarte puțin oferit clienților, aproximativ o treime dintre furnizorii de *Cloud* prezenți la studiu îl au în vedere ca viitoare sursă de venit undeva în următorii 2 ani.

4.2 Asigurarea conformității în cloud

Unele dintre problemele cheie care vor trebui abordate sunt:

- **Transparența.** Furnizorii de servicii trebuie să demonstreze existența unor controale eficiente și robuste de securitate, asigurând clienții că informațiile lor sunt asigurate în mod corect împotriva accesului neautorizat, modificării sau distrugerii lor. Întrebările cheie care ar trebui adresate pentru a decide sunt: Cât de multa transparență este suficientă? Ce trebuie să fie transparent? Va ajuta aceasta transparență răufăcătorii? Domenii-cheie în care transparența furnizorul este importantă includ: Ce angajați (de la furnizor) au acces la informațiile despre clienți? Este definită clar separarea funcțiilor între angajații furnizorului? Cum sunt separate (logic și fizic) informațiile între clienți? Ce controale sunt implementate pentru a preveni, detecta și reacționa la încălcarea regulilor descrise mai sus?
- **Confidențialitate.** Cu probleme de confidențialitate în creștere pe tot globul, este imperativ pentru furnizorii de servicii de cloud computing să demonstreze clienților capacitatea controalelor de confidențialitate implementate. Furnizorul trebuie să pună la dispoziție mai multe canale de comunicare înainte de începerea livrării serviciului. Aceste canale de comunicare trebuie să fie testate periodic în timpul operațiilor.
- **Conformitatea.** Cele mai multe organizații de astăzi trebuie să respecte o suită întreagă de legi, regulamente și standarde. Există îngrijorări legate de platformele de cloud computing, în sensul că datele nu pot fi stocate într-un singur loc și nu poate fi ușor de accesat. Este esențial să se asigure că, acestea pot fi accesate fără a compromite alte informații sau alți clienți, dacă datele sunt cerute de către autorități. Auditiuri executate de către autoritățile judiciare, de standardizare și de reglementare demonstrează că aceste cazuri pot exista. Atunci când se utilizează servicii de cloud nu există nici o garanție că o organizație poate obține informații atunci când este necesar, și unii furnizori chiar își rezervă dreptul de a nu prezenta anumite informații către autorități.
- **Transmiterea informațiilor.** Când informațiile pot fi stocate oriunde în platforma Cloud, locația fizică a informațiilor poate deveni o problemă pentru că locația fizică dictează competența și obligația legală. Legile țării privind informațiile de identificare personală variază foarte mult, ceea ce este permis într-o țară constituind o posibilă încălcare în alta.
- **Certificare.** Furnizorii de servicii de Cloud vor trebui să ofere o asigurare clienților lor, că ei fac lucrurile "corect". Asigurarea acestui lucru se obține prin auditiuri externe de la autorități independente, de aceea rapoarte ale acestor auditiuri sunt o parte vitală a oricărui program de certificare.

4.3 Riscuri și preocupări privind platformele Cloud

Multe dintre riscurile asociate frecvent cu platformele Cloud nu sunt noi, și pot fi întâlnite în multe din companiile de astăzi. Planificarea eficientă a activităților de gestionare a riscurilor este crucială în asigurarea faptului că informațiile sunt disponibile, în același timp și protejate.

Procese și procedurile de business trebuie să țină seama de securitate, și managerii de securitate a informațiilor trebuie să ajusteze politicile și procedurile organizațiilor lor pentru a satisface nevoile de

business. Având în vedere mediul de afaceri dinamic și concentrat pe globalizare, există foarte puține organizații care nu externalizează măcar o parte din activitatea lor. Angajarea într-o relație cu o terță parte nu înseamnă numai utilizarea serviciilor și tehnologiei furnizorului platformei de Cloud, dar, de asemenea, trebuie să se ia în considerare modul în care furnizorul funcționează, arhitectura soluțiilor oferite, precum și cultura și politicile organizaționale ale furnizorului. Câteva exemple de riscuri care trebuie să fie gestionate sunt:

- Organizațiile trebuie să fie foarte specifice în alegerea unui furnizor. Reputația, istoria și sustenabilitatea ar trebui să fie factori de luat în considerare. Sustenabilitatea este de o importanță deosebită pentru a se asigura că serviciile vor fi disponibile și datele pot fi urmărite.
- Furnizorul platformei Cloud își asumă de multe ori responsabilitatea pentru gestionarea informațiilor, care este o parte esențială. Imposibilitatea de a atinge un anumit nivel de calitate a serviciilor poate avea un impact major nu numai pentru confidențialitatea datelor, dar, de asemenea, pentru disponibilitatea lor, afectând grav fluxurile de operațiuni.
- Caracterul dinamic al tehnologiilor Cloud poate duce la confuzie cu privire la locul în care informațiile rezidă de fapt. Când este necesară regăsirea de informații, acest lucru poate crea întârzieri.
- Accesul terților la informații sensibile creează un risc de compromitere a informațiilor confidențiale. În cloud computing, acest lucru poate reprezenta o amenințare semnificativă la asigurarea protecției proprietății intelectuale și a secretelor comerciale.
- Platformele Cloud permit sistemelor să ofere nivele de high-availability de multe ori imposibil de a fi atinse în rețelele private, cu excepția cazurilor în care se investeste masiv. Dezavantajul constă în posibilitatea de mixare a informațiilor cu alți clienți Cloud, inclusiv cu concurenți. Respectarea regulamentelor și legilor în diferite regiuni geografice poate fi o provocare pentru organizații. În acest moment există puține precedente juridic în ceea ce privește asumarea răspunderii pentru platformele Cloud. Este extrem de important obținerea unei consilieri juridice adecvate pentru a se asigura că în contract se stipulează clar zonele în care furnizorul platformei Cloud este responsabil și răspunzător.
- Datorită naturii dinamice a platformelor Cloud, informațiile nu pot fi localizate imediat în caz de dezastre. Planurile de continuitate a afacerilor în caz de dezastru (DRP) trebuie să fie bine documentate și testate. Furnizorul de cloud trebuie să înțeleagă rolul pe care îl joacă în termeni de backup, de reacție la incidente și de recuperare a serviciilor. Obiectivele privind timpul de recuperare ar trebui să fie prevăzute în contract.

Strategii de adresare a riscurilor pe platforme Cloud

Aceste riscuri, precum și altele pe care o organizație le identifică, trebuie să fie gestionate în mod eficient. O organizație trebuie să pună la punct un program robust de management al riscului care să fie suficient de flexibil pentru a face față riscurilor. Într-un mediu în care confidențialitatea a devenit extrem de importantă pentru clienții enterprise, accesul neautorizat la datele din Cloud este o preocupare critică. Atunci când se semnează un contract cu un furnizor de servicii cloud, o organizație trebuie să aibă un inventar al datelor lor și să se asigure că sunt clasificate și etichetate în mod corespunzător. Acest lucru va ajuta în determinarea a ceea ce trebuie specificat în momentul elaborării unui acord de asigurare a nivelului de calitate a serviciilor (Service Level Agreement - SLA), - de obicei completează un contract de servicii - identificarea nevoilor de criptare a datelor transmise sau stocate, precum și controale suplimentare de informații sensibile sau de mare valoare pentru organizație.

Acordul de asigurare a nivelului de calitate a serviciilor (SLA) este cel care definește relația dintre organizație și furnizor de servicii cloud, fiind unul dintre cele mai eficiente instrumente pentru a asigura o protecție adecvată a informațiilor stocate în platforma Cloud. Contractul SLA este instrumentul prin care clienții pot specifica ce modele de control se vor utiliza și descrie așteptările în urma unui audit extern. Așteptările clare în ceea ce privește manipularea, utilizarea, stocarea și disponibilitatea de informații trebuie să fie specificat în SLA. În plus, cerințele de continuitate a afacerii și recuperare în urma dezastrelor (discutate anterior), vor trebui să fie comunicate în acest acord.

Protecția informațiilor va evolua ca urmare a unui acord SLA puternic, cuprinzător, care este susținut de un proces de asigurare la fel de puternic și cuprinzător. Structurarea unui SLA detaliat și complet, care include drepturi specifice pentru audit va ajuta organizația în gestionarea informațiilor sale odată ce acestea părăsesc organizația și sunt transportate, stocate sau prelucrate în Cloud.

Implementarea și utilizarea serviciilor Cloud trebuie să fie considerate nu numai în contextul "intern" vs. "extern", care se referă la locația fizică a bunurilor, resurselor și informațiilor, dar, de asemenea, prin definirea consumatorului serviciului și prin definirea responsabilului pentru guvernarea lor, de securitate, precum și conformitatea cu politicile și standardele.

Acest lucru nu vrea să sugereze că localizarea (în sau în afara premiselor) unui bun, a unei resurse sau a datelor nu afectează modul de tratare a securității și riscul unei organizații, ci pentru a sublinia că riscul, de asemenea, depinde de:

- Tipurile de bunuri, resurse și informații gestionate
- Cine le gestionează și cum
- Controalele selectate și modul în care acestea sunt integrate
- Probleme de conformitate

De exemplu, o soluție "LAMP" – explicație - instalată pe Amazon AWS EC2 ar fi clasificat ca o soluție publică, off-premise, o soluție IaaS gestionată de o terță parte, chiar dacă instanțele și aplicațiile / datele cuprinse în acestea au fost gestionate de către consumator sau de o terță parte. O soluție particularizată care deserveste mai multe departamente, instalată pe "Eucalyptus" sub controlul și managementul unei corporații, ar putea fi descrisă ca o aplicație privată, on-premise, auto-gestionată SaaS. Ambele exemple descriu elasticitatea și capacitatea de "self-service" a platformelor Cloud.

Tabelul de mai jos rezuma aceste puncte:

	Infrastructure Managed By ¹	Infrastructure Owned By ²	Infrastructure Located ³	Accessible and Consumed By ⁴
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Or Organization Third Party Provider	 Organization Third Party Provider	On-Premise Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

¹ Management includes: governance, operations, security, compliance, etc...

² Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment

³ Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control

⁴ Trusted consumers of service are those who are considered part of an organization's legal/contractual/policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

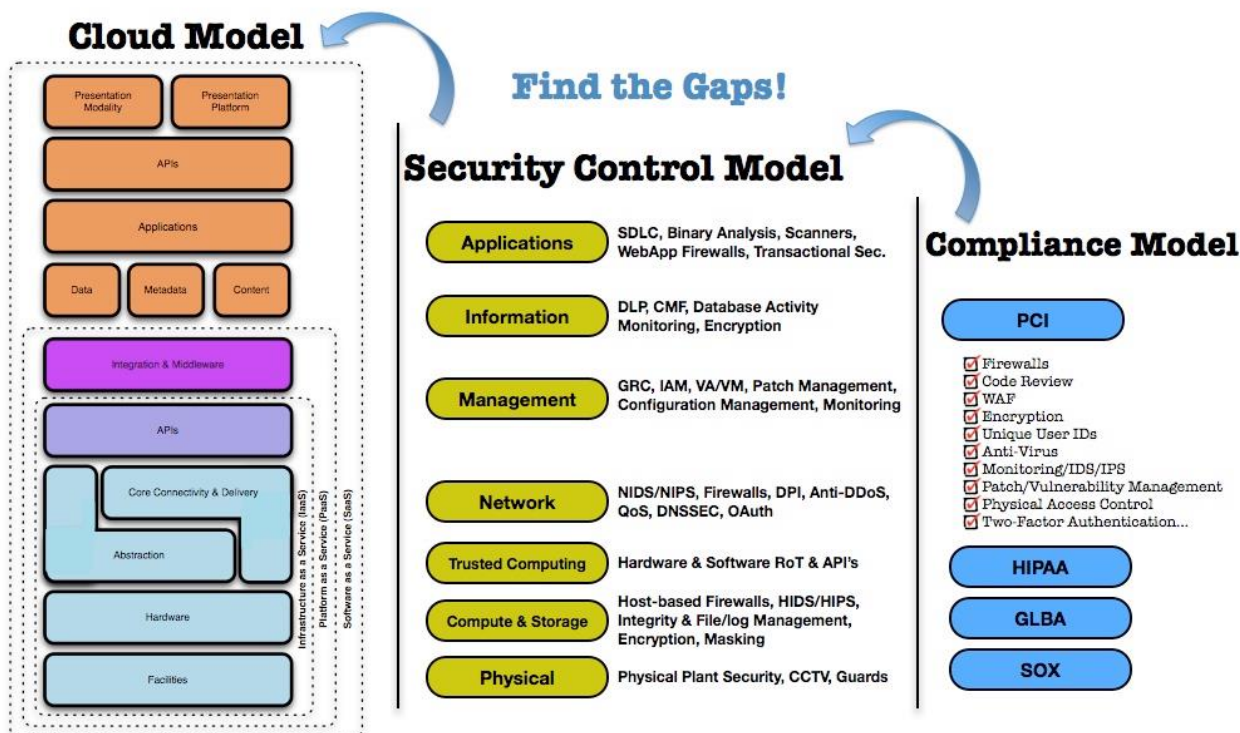
Referința: CSA Cloud Computing Security Guidance V2.1 pag. 22

Modelul Cloud Cube evidențiază provocările în a înțelege și a asigura modele de cloud cu standarde cum ar fi ISO/IEC 27002, standard ce oferă "... o serie de orientări și principii generale pentru inițierea, implementarea, menținerea și îmbunătățirea securității informațiilor în cadrul unei organizații."

ISO/IEC 27002, punctul 6.2 se concentrează pe obiectivele de control ale părților terțe și prevede: "... securitatea informațiilor organizației și securitatea prelucrării informațiilor nu trebuie să fie reduse prin introducerea de produse sau servicii externe..."

Ca atare, diferențele în metodele și responsabilitatea de a asigura securitatea datelor în cele trei modele de servicii Cloud evidențiază faptul că consumatorii de servicii Cloud se confruntă cu situații dificile. Dacă furnizorii de servicii Cloud nu pot demonstra ușor controalele de securitate, precum și măsura în care acestea sunt puse în aplicare pentru consumator, iar consumatorul știe care controale sunt necesare pentru a menține securitatea informațiilor lor, există un potențial imens pentru deciziile greșite și rezultatele negative. Acest lucru este critic. Primul pas este categorisirea serviciului Cloud oferit relativ la modelele arhitecturale Cloud. Apoi este posibilă determinarea arhitecturii de securitate, precum și alte cerințe de conformitate, ca un exercițiu de analiză și determinare a lucrurilor lipsă (gap-analysis sau analiza diferențială). Rezultatul acestei analize determină starea generală a serviciului din punct de vedere "securitate" și modul în care acesta răspunde cerințelor de protecție.

Figura de mai jos prezintă un exemplu de analiză a unui serviciu Cloud în compararea cu un catalog predefinit de controale de securitate, pentru a determina existența sau lipsa anumitor controale. Aceasta, la rândul său, poate fi comparat cu un set de norme sau un set de cerințe, cum ar fi PCI DSS.



Referinta: CSA Cloud Computing Security Guidance V2.1 pag. 23-24

Controalele de securitate în cloud computing sunt, în cea mai mare parte, similare cu controalele de securitate în orice mediu IT. Cu toate acestea, din cauza modelelor și arhitecturilor serviciilor Cloud, a modelelor operaționale diferite și a tehnologiilor utilizate, serviciile în Cloud computing pot prezenta riscuri diferite de soluțiile IT tradiționale.

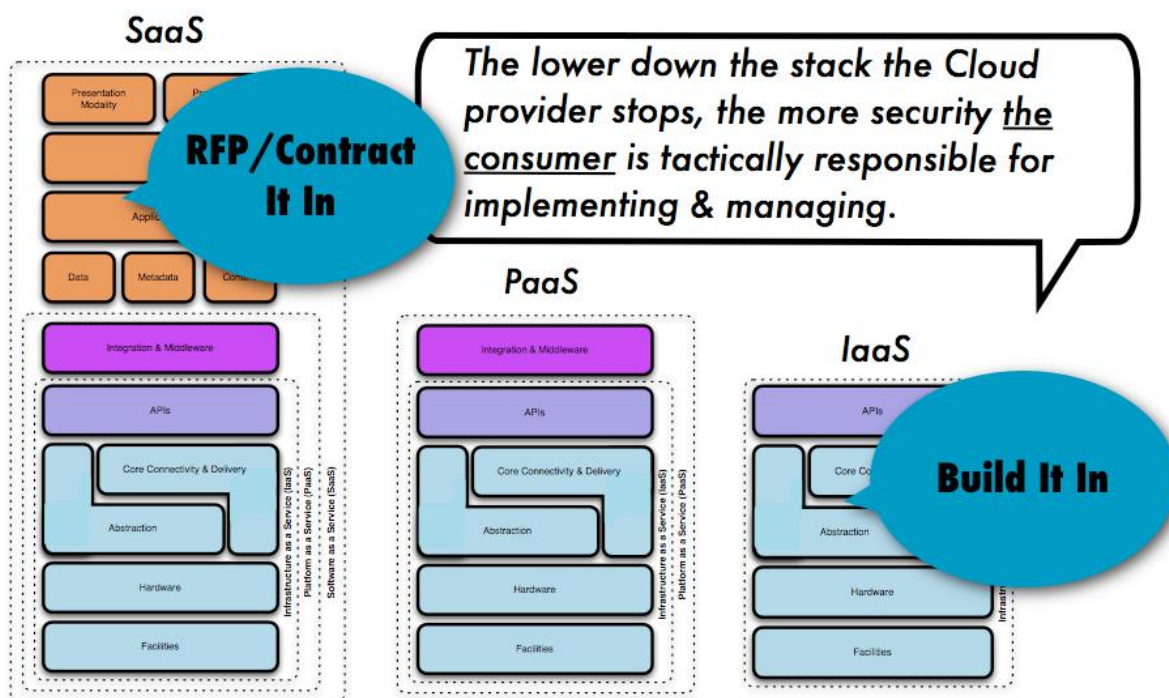
Politica de securitate a unei organizații este caracterizată prin maturitatea, eficiența, și completitudinea controalelor de securitate. Aceste controale sunt puse în aplicare pe mai multe niveluri, pornind de la securitatea locației (securitatea fizică), la infrastructura de rețea (de securitate de rețea), a sistemelor informatice (sistemul de securitate), până la securitatea datelor și a aplicațiilor (securitatea aplicațiilor). În plus, controalele sunt puse în aplicare și la nivelul persoanelor și proceselor, cum ar fi separarea atribuțiilor, respectiv managementul schimbării.

Unul dintre avantajele majore ale cloud computing este eficiența costurilor rezultată direct din economiile provenite din scalabilitatea soluțiilor, nivelul mare de reutilizare și standardizare. Pentru a aduce soluțiile lor la aceste randamente, furnizorii de servicii Cloud trebuie să ofere un nivel ridicat de flexibilitate pentru a putea adresa un segment cât mai mare din piață. Din păcate, integrarea securității în aceste soluții este adesea percepută ca o rigidizare a lor.

Această rigiditate se manifestă adesea în imposibilitatea de a obține paritatea în desfășurarea controlului de securitate în medii Cloud, comparativ cu mediile IT tradiționale. Acest lucru rezultă în mare parte din abstractizarea infrastructurii, precum și din lipsa de vizibilitate și de capacitatea de a integra mai multe controale de securitate familiare - mai ales la nivelul rețelei.

Figura de mai jos ilustrează aceste probleme: în mediile SaaS controalele de securitate și domeniul lor de aplicare sunt negociate în contractele de servicii, inclusiv aspecte legate de nivelul de calitate a serviciilor, de confidențialitate și de conformitate. Într-o oferta IaaS, în timp ce responsabilitatea pentru asigurarea

infrastructurii și nivelurile de abstractizare aparține furnizorului, restul nivelurilor (până la aplicație) este responsabilitatea consumatorului. PaaS oferă un echilibru între cele două, unde asigurarea platformei în sine cade în responsabilitatea furnizorului, dar asigurarea securității aplicațiilor dezvoltate pe platforma respectiva aparțin consumatorului.



Referinta: CSA Cloud Computing Security Guidance V2.1 pag. 26

4.4 Recomandări

4.4.1 Guvernanța și Managementul de Risc al Organizației

În cele ce urmează, prin *guvernanță* vom înțelege ansamblul unitar de activități conexe din domeniile *conducerii și controlului*.

Iar *guvernanța corporativă* este definită ca fiind un sistem de reglementări aprofundate prin care corporațiile sunt *conduse și controlate*, punând accent pe structurile interne și externe ale corporației, cu intenția de a monitoriza activitățile de management și de a reduce riscul apariției unor evenimente nedorite din interiorul corporației.

Guvernanța eficientă și Managementul de Risc al Organizației din cadrul mediilor Cloud Computing decurg din procesele continue perfecționate de guvernanță din domeniul securității informațiilor, ca parte a îndatoririlor generale de guvernanță corporativă, care se cuvin. Procesele perfecționate de guvernanță din domeniul securității informațiilor trebuie să ducă la programe de management al securității informațiilor care în mod permanent trebuie să fie extensibile în funcție de business, repetabile în cadrul organizației, măsurabile, menținute în funcțiune, perfecționate și să fie economice.

Chestiunile fundamentale de guvernanță și management de risc al organizației în Cloud Computing privesc identificarea și implementarea de structuri, procese și controale organizaționale adecvate, în scopul menținerii cu eficiență a conceptului GRC în domeniul securității informațiilor. GRC reprezintă ansamblul de activități strâns înrudite din sferele *Guvernanță-Risk Management- Conformitate*. Organizațiile trebuie de asemenea să asigure condiții corespunzătoare de securitate a informației pe tot lanțul informațional, cuprinzând inclusiv furnizori și clienți de servicii Cloud Computing, precum și furnizorii lor subcontractați care, pot exista în diverse *modele* de structuri de cloud.

Recomandări adresate guvernanței

✓ O parte din economiile realizate din servicii de Cloud Computing, trebuie investite în analiza minuțioasă a capacităților de securitate ale furnizorului, a utilizării de controale de securitate și aplicării în permanență de evaluări și audituri detaliate, pentru asigurarea îndeplinirii cerințelor de securitate.

✓ Atât clienții cât și furnizorii de servicii Cloud Computing, trebuie să dezvolte o guvernanta cât mai viguroasă în domeniul securității informațiilor, indiferent de modelul serviciului sau al modului de implementare a acestuia. Guvernanta din securitatea informației trebuie să ducă la colaborare dintre clienți și furnizori, pentru atingerea ȳintelor prestabilite în sprijinul desfășurării activităților organizației și îndeplinirii programelor de securitate a informației. Modelul adoptat pentru serviciu, permite reglarea rolurilor și responsabilităților guvernantei și managementului de risc (bazat pe controlul utilizatorului și furnizorului), în timp ce modelul de implementare poate determina responsabilitățile și perspectivele (bazat pe evaluarea riscului).

✓ Organizațiile clienților trebuie să aibă în vedere analiza proceselor și structurii guvernantei din domeniul securității informației, ca parte a atenției cuvenite față de furnizori. Procesele și capacitățile guvernantei de securitate ale furnizorului, trebuie să fie dimensionate pentru a asigura suficiență, performanță și consistență, proceselor de management al securității informațiilor clienților. Controalele privind securitatea informației la nivelul furnizorului, trebuie să fie în mod evident bazate pe analiza de risc și să sprijine vizibil aceste procese de management.

✓ Procesele și structurile guvernantei colaborative dintre clienți și furnizori trebuie să se dovedească necesare, atât ca parte a proiectării și dezvoltării furnizării de servicii, cât și pentru evaluarea de risc a serviciului.

✓ Departamentele de securitate trebuie să participe la stabilirea acordurilor SLA (Service Level Agreements) dintre furnizorii de servicii Cloud Computing și clienții acestora. De asemenea, trebuie să participe la stabilirea obligațiilor contractuale, pentru a se asigura că cerințele de securitate sunt impuse prin prevederile contractuale.

✓ Parametrii și standardele de apreciere a performanțelor și eficienței managementului securității informațiilor, trebuie să fie stabiliți înainte de pornirea funcționării în cloud. Cel puțin, organizațiile clientelare trebuie să înțeleagă și să se documenteze temeinic privind proprii lor parametri și felul cum aceștia se pot schimba când se va funcționa în cloud, caz în care, un furnizor poate să folosească parametri diferiți (posibil să fie chiar incompatibili !).

✓ Ori de câte ori este posibil, parametrii și standardele de securitate (în special cei legați de cerințe legale și de conformitate), trebuie să fie prevăzuți în acordurile SLAs și în contracte. Aceste standarde și acești parametri trebuie menționați în documente și trebuie să fie auditabili.

Recomandări privind Managementul de Risc al organizației

Așa cum se întâmplă la demararea oricărei activități noi, este important de urmat cele mai bune practici pentru realizarea managementului de risc. Aceste practici trebuie să fie proporționale cu modul particular de utilizare a serviciilor cloud care pot fi de la o slabă și sporadică procesare de date, până la procese critice care vehiculează informații sensibile de nivel înalt.

✓ Datorită lipsei de control fizic asupra infrastructurii multor sisteme Cloud Computing, acordurile SLA, cerințele contractuale și documentația furnizorului joacă un rol foarte important în managementul de risc, în comparație cu cazul tradițional al infrastructurilor proprietate ale organizațiilor.

✓ Datorită serviciilor diversificate oferite la cerere, precum și aspectelor *multi-tenant* specifice Cloud Computing-ului (*multi-tenant* este un principiu în arhitectura software în care, un singur program care rulează pe un sever servește simultan mai multe organizații client), formele tradiționale de audit și de evaluare nu sunt aplicabile sau pot avea rezultate incomplete. De exemplu, unii furnizori nu permit evaluarea vulnerabilităților și testarea penetrării, în timp ce alții limitează disponibilitatea rapoartelor de audit și monitorizarea activităților. Dacă astfel de informații sunt necesare unui utilizator conform politicii sale interne, acesta trebuie să caute alte evaluări alternative, sau unele excepții contractuale sau, în ultimă instanță, un alt furnizor, mai apropiat de cerințele sale din domeniul managementului riscurilor.

✓ În legătură cu utilizarea serviciilor cloud pentru funcțiuni critice unei organizații, managementul de risc trebuie să cuprindă identificarea și aprecierea valorilor organizației, identificarea și analiza amenințărilor și vulnerabilităților și impactul potențial al acestora asupra acelor valori (scenariul de incidente), probabilitatea evenimentelor/scenariilor, nivelurile și criteriile de acceptare ale riscului rezidual și dezvoltarea planurilor de tratare a riscului cu multiple opțiuni (control, anulare, transfer, acceptare). Rezultatul final al planurilor de tratare a riscurilor, trebuie să fie incluse în acordurile serviciilor achiziționate.

✓ Etapele de evaluare a riscurilor dintre furnizor și beneficiar trebuie să fie cuprinzătoare, cu consistență în privința criteriilor de analiză a impactului și în estimarea probabilității de apariție a evenimentelor. Utilizatorul

și furnizorul trebuie, în mod conjugat, să dezvolte scenariul de risc pentru serviciile cloud; acesta trebuie să fie intrinsec proiectului serviciului oferit de furnizor, precum și evaluării riscului de serviciu de cloud efectuată de utilizator.

✓ Inventarele valorilor organizației clientului trebuie să gestioneze serviciile de cloud care produc valoare și care se află sub controlul furnizorului.

✓ Serviciul, și nu furnizorul, trebuie să fie subiectul evaluării riscurilor. Utilizarea serviciilor cloud, și a modelelor de implementare, trebuie să răspundă obiectivelor managementului de risc al organizației, precum și obiectivelor activității acesteia.

✓ În cazul în care un furnizor se bazează pe un management al riscurilor necuprinzător și ineficient în asociere cu serviciile sale, clienții trebuie să evalueze cu atenție oportunitatea de a se folosi de serviciile furnizorului, precum și abilitățile utilizatorilor de compensare a posibilelor lipsurilor ale managementului riscurilor.

✓ Clienții serviciilor cloud, trebuie să cerceteze dacă propriul lor management a luat în considerare toleranța la risc cu privire la serviciile cloud și are în vedere acceptarea de risc rezidual în utilizarea serviciilor cloud.

Recomandări privind Managementul de Risc al Informațiilor

Managementul de Risc al Informațiilor - **MRI** constă în acceptarea expunerii inevitabile la risc, asociată cu capacitatea de a-l controla, pe baza toleranței la risc, acceptată de proprietarul informațiilor. În felul acesta, MRI este instrumentul principal al suportului decizional privind resursele IT, destinat să protejeze confidențialitatea, integritatea, disponibilitatea și autenticitatea valorilor informaționale.

✓ Se recomandă adoptarea unui model cadru pentru evaluarea MRI, și un model bine gândit de evaluare a eficienței MRI.

✓ Se recomandă stabilirea de cerințe contractuale adecvate și de controale, pentru colectarea datelor necesare luării deciziilor în analiza riscului informațional (de ex. felul cum este folosită informația, controlul accesului, controalele de securitate, securitatea locației, etc...)

✓ Se recomandă adoptarea unui proces de determinare a expunerii la risc, înainte de elaborarea cerințelor pentru un proiect Cloud Computing. Deși categoriile de informații necesare pentru înțelegerea nivelului de expunere și a capacităților de management sunt generale, parametri reali care stau ca probă și care pot fi colectați în condițiile serviciului, sunt specifici naturii modelului SPI de Cloud Computing. (Reamintim că modelul SPI înseamnă Software, Platform&Infrastructure luate ca Servicii).

✓ În cazul în care se utilizează modelul SaaS (Software as a Service), covârșitoarea majoritate a informațiilor, va trebui să fie asigurată de furnizorul serviciului. Organizațiile trebuie să structureze procese de obținere de informații analitice, necesare în obligațiile contractuale ale serviciului SaaS.

✓ În cazul în care se utilizează un furnizor de serviciu PaaS (Platform as a Service), se poate construi un sistem de culegere de informații la fel ca la SaaS, dar există și posibilitatea de a aduna informații din controale, precum și de a crea prevederi contractuale pentru testarea eficienței acestor controale.

✓ În cazul în care se utilizează un furnizor de serviciu IaaS (Infrastructure as a Service), trebuie asigurată transparența informației în modul de exprimare al contractului, pentru informațiile cerute de analiza de risc.

✓ Furnizorii de servicii cloud trebuie să includă parametri și controale pentru asistarea clienților în procesul de implementare a cerințelor lor din MRI.

Recomandări privind managementul entităților intermediare (third party)

✓ Clienții trebuie să perceapă serviciile cloud și securitatea în cloud ca o chestiune de securitate pe întreg lanțul de furnizare de servicii. În sensul că, în măsura în care este posibil, se fac verificări și evaluări pe tot lanțul care realizează serviciul (inclusiv conexiuni și externalizări ale furnizorului). Cu alte cuvinte, vorbim despre verificarea managementului tuturor entităților intermediare, subcontractate ale furnizorului.

✓ Evaluarea furnizorilor de servicii intermediare, trebuie avută în vedere în mod special în managementul incidentelor efectuat de furnizor, în politicile de recuperare după dezastru și de continuare a activității, în procese și proceduri; și neapărat trebuie să includă controlul încăperilor în care se face co-locare și salvări back-up. De asemenea, mai trebuie adăugat controlul evaluărilor interne ale furnizorului privind respectarea propriilor politici și proceduri, dar și evaluarea indicatorilor pe baza cărora, se măsoară performanța și eficiența controalelor furnizorului.

✓ Planul de recuperare după dezastru și de continuitate a activității utilizatorului, trebuie să includă scenarii de întrerupere a serviciilor furnizorului, de întrerupere a serviciilor intermediare care relaționează cu furnizorul, și a capacităților dependente de entități intermediare.

✓ Guvernanța privind securitatea informației la nivelul furnizorului, managementul riscurilor, procesele și structurile de verificare a conformității, trebuie să fie în mod cuprinzător evaluate, astfel:

o Este necesară o documentare clară despre felul cum facilitățile și serviciile sunt evaluate în raport cu riscurile, despre felul cum sunt auditate în privința punctelor slabe ale controlului, cât de des se fac aceste evaluări, și cum sunt atenuate slăbiciunile controlului în timp util.

o Este necesară definirea clară a felului în care furnizorul ia în considerare serviciile critice și factorii de succes în securitatea informației, indicatorii cheie de performanță, și felul în care toate acestea sunt măsurate în serviciile IT și în Managementul Securității Informațiilor.

o În scopul bunei cunoașteri a furnizorului, este necesară revizuirea cerințelor acestuia de legalitate, de reglementare, de activitate și contractuale; de asemenea, procesele sale de evaluare și comunicare.

o Din analiza contractului și a condițiilor de utilizare, trebuie identificate roluri, responsabilități și sarcini. Asigurarea controlului legalității, inclusiv includerea unei evaluări privind capacitatea de control al respectării prevederilor contractuale și al aplicării legii de jurisdicție străină sau aparținând unui stat comunitar.

o Este necesar de stabilit dacă elementele de bonitate – credibilitate ale furnizorului cuprind toate aspectele materiale ale relațiilor acestuia, cum ar fi situația lui financiară, reputația acestuia, verificările care i se fac, personalul-cheie, testele și planurile de recuperare după dezastru, ce fel de asigurare are, posibilitățile de comunicare și folosire de subcontractori.

4.4.2 Interoperabilitate și portabilitate

Organizațiile trebuie să abordeze tehnologia *cloud*, știind că ar putea în viitor să-și schimbe furnizorii. *Portabilitatea și interoperabilitatea* trebuie avute în vedere în avans, ca elemente ale managementului riscurilor și asigurării pe linie de securitate ale oricărui *program cloud*.

Datorită unei lipse generale de standarde de interoperabilitate, dar și din lipsă de cerință a pieței pentru aceste standarde, trecerea de la un furnizor de cloud la altul, poate fi un proces manual care să necesite multă muncă. Din perspectiva securității, una dintre principalele griji trebuie să fie menținerea consecvenței și seriozității controalelor de securitate, atunci când este schimbat mediul cloud.

Recomandări pentru toate soluțiile de cloud:

✓ Schimbarea furnizorilor de cloud este realmente în toate cazurile, o chestiune negativă pentru cel puțin una dintre părți, fapt care poate determina o reacție negativă neașteptată, de la vechiul furnizor de cloud.

✓ Trebuie luată în considerare mărimea depozitelor de date stocate la furnizorul de cloud. Cantitatea reală de date poate cauza întreruperea serviciului în timpul unei tranziții, sau o prelungire a timpului de tranziție, mai mare decât a fost anticipat. Mulți clienți au descoperit că folosind un curier care transportă hard discurile este o soluție mai rapidă decât transmisia electronică atunci când este vorba de depozite mari de date.

✓ Trebuie bine documentată arhitectura de securitate și configurația controalelor de securitate a componentelor individuale, așa încât, acestea să poată fi folosite în cadrul auditurilor interne, precum și pentru a facilita trecerea la un nou furnizor.

Recomandări pentru soluțiile IaaS de cloud (Infrastructure as a Service):

✓ Trebuie înțeles modul cum imaginile mașinilor virtuale pot fi capturate și portate la un nou furnizor de cloud, care ar putea să folosească tehnologii de virtualizare diferite.

✓ Trebuie identificat și eliminat (sau măcar de documentat), orice extensii specifice, aplicate de furnizor mediului de mașini virtuale.

✓ Trebuie înțeles care practici sunt implementate pentru a face sigură *deprovizionarea* corespunzătoare (deconfigurarea mașinilor dintr-un centru de date virtual) a imaginilor VM după ce o aplicație este portată de la un furnizor de cloud la altul.

✓ Trebuie înțelese practicile utilizate pentru dezafectarea discurilor și dispozitivelor de stocare.

✓ Trebuie înțelese dependențele bazate pe hardware / platforme și care trebuie să fie identificate, înainte de migrarea aplicațiilor / datelor.

✓ Trebuie solicitat acces la jurnalele de sistem, la evidența succesiunii evenimentelor, dar și la înregistrări de acces și financiare (facturi) de la furnizorul de cloud inițial.

- ✓ Trebuie identificate opțiunile necesare pentru a relua sau pentru a extinde serviciul cu furnizorul cloud initial, în parte sau în totalitate, pentru cazul în care, noul serviciu se dovedește a fi inferior.
- ✓ Trebuie stabilit dacă există funcții de management, interfețe, sau API-uri (interfețe software) utilizate dar care sunt incompatibile sau, sunt neimplementate de către noul furnizor.

Recomandări pentru soluțiile PaaS de cloud (Platform as a Service):

- ✓ Atunci când este posibil, se vor utiliza componente de platformă cu sintaxă standard, API-uri deschise, și standarde deschise.
- ✓ Trebuie înțeles care instrumente sunt disponibile pentru transferul sigur al datelor, pentru copii de rezervă și restaurare.
- ✓ Trebuie înțelese și documentate componentele aplicațiilor și modulele specifice furnizorului PaaS și e recomandabil să fie dezvoltată o arhitectură de aplicație structurată pe niveluri, pentru a minimiza accesul direct la modulele proprietare.
- ✓ Trebuie înțeles modul în care serviciile de bază, cum ar fi monitorizarea, jurnalizarea și auditul ar fi transferate la un nou furnizor.
- ✓ Trebuie înțelese funcțiile de control utilizate de către furnizorul inițial de cloud, și modul în care acestea s-ar traduce la noul furnizor.
- ✓ Atunci când se migrează către o nouă platformă, trebuie înțeles impactul asupra performanței și disponibilității aplicației, și modul în care vor fi măsurate aceste efecte.
- ✓ Trebuie înțeles modul în care testele vor fi finalizate înainte și după migrare, pentru a verifica dacă serviciile sau aplicațiile funcționează corect. Trebuie să ne asigurăm că, responsabilitățile pentru testare atât ale furnizorului cât și ale utilizatorului, sunt bine cunoscute și documentate.

Recomandări pentru soluțiile SaaS de cloud (Software as a Service):

- ✓ Trebuie efectuate extrageri periodice de date și backup într-un format care este ușor de utilizat, fără implicarea furnizorului SaaS.
- ✓ Trebuie înțeles dacă metadatele pot fi păstrate în siguranță și migrate.
- ✓ Trebuie înțeles că orice instrumente personalizate implementate vor trebui să fie refăcute sau, noul furnizor trebuie să furnizeze aceste instrumente.
- ✓ Trebuie asigurată temeinicie eficienței controlului asupra furnizorilor vechi și noi.
- ✓ Trebuie asigurată posibilitatea de migrare a copiilor de siguranță și a altor copii ale jurnalelor, ale înregistrărilor de acces, precum și a oricăror alte informații pertinente care pot fi cerute, din motive de verificare a respectării legalității și conformității.
- ✓ Trebuie înțelese interfețele de management, monitorizare, raportare și integrarea lor între mediile de lucru.
- ✓ Trebuie verificat dacă există o prevedere pentru noul furnizor, pentru a testa și evalua aplicațiile, înainte de migrare?

4.4.3 Securitate, continuitatea afacerii, și recuperarea după dezastru

Volumul de cunoștințe acumulate în domeniul securității fizice tradiționale, în planificarea tradițională a continuității afacerii și în recuperarea după dezastru, rămân destul de relevante pentru Cloud Computing. Ritmul rapid al schimbărilor și lipsa de transparență în Cloud Computing, cer ca profesioniștii formați în *securitate tradițională*, în *planificarea continuității activității* –BCP și în *recuperarea după dezastru* –DR să fie în mod continuu angajați în verificarea și monitorizarea furnizorilor de servicii de cloud pe care îi alegem. Provocarea este de a colabora la identificarea riscurilor, la recunoașterea interdependențelor, la a integra și valorifica resursele într-un mod dinamic și puternic. Cloud Computing și infrastructura sa aferentă ajută la diminuarea anumitor probleme de securitate, dar pot să ducă la creșterea altora, așa încât, în nici un caz nu pot elimina nevoia de securitate. În timp ce în afaceri și tehnologie continuă să se producă schimbări majore, principiile tradiționale de securitate rămân.

Recomandări

- ✓ De reținut faptul că centralizarea datelor face ca riscul de abuz intern din cadrul furnizorului de cloud, să fie un aspect semnificativ.

✓ Furnizorii de cloud ar trebui să vadă în adoptare, o chestiune importantă de securitate, cu cele mai severe cerințe din partea oricărui client. În măsura în care aceste practici de securitate nu au un impact negativ asupra experienței clientului, practicile severe de securitate ar trebui să se dovedească a fi eficiente pe termen lung prin reducerea riscurilor, precum și prin control orientat intereselor clientului, în mai multe domenii de interes.

✓ Furnizorii ar trebui să aibă o compartimentare robustă a atribuțiilor de serviciu, să efectueze controale de fond, să ceară/impună acorduri de confidențialitate pentru angajați, și să limiteze accesul angajaților la informațiile clienților, și anume, numai la ceea ce este absolut necesar pentru îndeplinirea sarcinilor de serviciu.

✓ Clienții ar trebui să efectueze inspecții la locațiile furnizorului de cloud ori de câte ori este posibil.

✓ Clienții ar trebui să examineze planurile furnizorului de cloud pentru recuperarea în caz de dezastru și pentru continuitate a afacerii.

✓ Clienții ar trebui să identifice interdependențele fizice din infrastructura furnizorului de cloud.

✓ Este recomandabil să ne asigurăm că există stipulat în contract, o decizie a conducerii organizației furnizorului, care în mod clar să definească în capitole distincte, obligațiile contractuale referitoare la securitate, la recuperare, și la accesul la date.

✓ Clienții ar trebui să ceară documentația controalelor de securitate interne și externe ale furnizorului, precum și documentația din care să rezulte aderarea (și respectiv certificarea) la standarde industriale.

✓ Asigurarea pentru clienți a *Obiectivelor de Timp de Recuperare* (RTO), trebuie să fie pe deplin înțeleasă și definită în relații contractuale și coerent integrată în procesul de planificare tehnologică. Trebuie să ne asigurăm că planificarile tehnologice, politicile, precum și capacitățile operaționale pot satisface aceste cerințe.

✓ Clienții trebuie să confirme că furnizorul are o politică existentă privind Programul de Continuitate a Activității -BCP, care să fie aprobată prin consiliul director al furnizorului.

✓ Clienții ar trebui să se intereseze de dovezi de susținere a managementului activ și de revizuirea periodică a Programului de Continuitate a Activității -BCP pentru a se asigura că programul BCP este activ.

✓ Clienții trebuie să verifice dacă programul BCP este certificat și/sau mapat la standarde recunoscute la nivel internațional, cum ar fi ISO 27001.

✓ Clienții ar trebui să constate dacă furnizorul are o resursă online dedicată securității și programului BCP, în care sunt disponibile ca referință, prezentarea generală a programului și documentele în care sunt rezumate problemele cheie.

✓ Este necesară asigurarea că furnizorii cloud sunt verificați prin intermediul unei organizații specializate, de exemplu Vendor Security Process (VSP), astfel încât, să existe o înțelegere clară privind care date sunt destinate pentru a fi accesate de terți utilizatori, și care sunt controalele care urmează să fie efectuate. Concluziile unei organizații de tip VSP ar trebui să servească în procesul de luare a deciziilor și în evaluarea pentru a decide nivelul de risc acceptabil.

✓ Caracterul dinamic al Cloud Computing și maturitatea relativă justifică reluarea ciclică frecventă a tuturor activităților de mai sus.

4.4.4 Arhitectura și Proceduri operaționale în Data Center

Este imperios necesar ca o organizație ce are în vedere achiziționarea de servicii de cloud, de orice fel, să fie în deplină cunoștință de cauză despre exact acele servicii care sunt contractate și despre ce nu este inclus. Mai jos este un rezumat al informațiilor care trebuie să fie revizuite în cadrul procesului de selecție a vânzătorului de servicii, și întrebări suplimentare pentru a ajuta la calificarea furnizorilor și pentru o mai bună adaptare a serviciilor oferite de aceștia.

✓ Indiferent de certificările deținute de furnizorii cloud, este important de a primi sarcina de a executa audituri la furnizor sau, măcar permisiunea pentru client sau pentru o terță parte externă de a supraveghea audituri la furnizor.

✓ Clienții Cloud ar trebui să înțeleagă modul în care furnizorii cloud implementează arhitecturile tehnologice și impactul infrastructurii asupra capacității lor de a satisface acordurile la nivel de serviciu.

✓ În timp ce arhitecturile tehnologice ale furnizorilor cloud diferă, ei trebuie să fie în măsură să demonstreze completa compartimentare a sistemelor, rețelelor, managementului, a alocării de resurse cloud către fiecare client (provisioning) și a personalului.

✓ Trebuie înțeles modul în care se realizează alocarea de resurse la furnizorul la care suntem abonați, pentru a putea avea cea mai bună predicție asupra disponibilității și performanței sistemului, constatate în timpul fluctuațiilor activității noastre în cloud. Dacă e posibil, putem să analizăm alți clienți ai furnizorului pentru a

evalua impactul pe care fluctuațiile activității lor poate să-l aibă asupra noastră, ținând cont de experiența noastră de client în relație cu furnizorul. În orice caz, astfel de rezultate, nu pot înlocui cerința că înțelegerile la nivel de service trebuie să fie clar definite, măsurabile, aplicabile, și adecvate cerințelor noastre.

✓ Clienții Cloud ar trebui să înțeleagă politicile și procedurile de management al patch-urilor elaborate de furnizorii lor de cloud, și modul în care acestea pot afecta mediul lor de lucru. Cunoștințele acestea ar trebui să fie reflectate în prevederile contractului.

✓ Îmbunătățirea continuă este deosebit de importantă într-un mediu cloud pentru că orice îmbunătățire a politicilor, proceselor, procedurilor, sau instrumentelor pentru un singur client, ar putea duce la îmbunătățirea serviciilor pentru toți clienții. E recomandabil să-i căutăm pe acei furnizori de cloud care sunt în permanent proces de îmbunătățire a aderării la standarde.

✓ Asistența tehnică sau serviciul Help Desk reprezintă de multe ori o fereastră a clientului în operațiunile furnizorului. Pentru a obține o experiență bună și constantă de asistență pentru clienți ca utilizatori finali, este esențial să ne asigurăm că procesele furnizorului de asistență pentru clienți, procedurile, instrumentele, și orele de asistență sunt compatibile cu ale clientilor.

✓ Trebuie analizat Procesul de Continuitate a Activității și Planurile de Recuperare după Dezastru, și din perspectivă IT, și în legătură cu modul în care acestea se referă la utilizatori și la procese. Arhitectura tehnologiei unui furnizor de cloud poate utiliza metode noi dar care, uneori, se pot dovedi nesatisfăcătoare în unele privințe, de exemplu pentru *modul de operare failover*. (Reamintim că *modul de operare failover* constă în existența unor elemente redundante hard și/sau soft de rezervă, care preiau automat executarea unei funcții, atunci când, componenta inițial asignată pentru acea funcție, nu mai funcționează).

Așadar propriile planuri de continuitate a activității clienților ar trebui de asemenea, să aibă în vedere impactul și limitările tehnologiei cloud computing.

4.5 Auditare și atestare

Din cele mai multe reglementări care se referă la tehnologia informației cu care organizațiile trebuie să se conformeze, puține dintre ele au ținut cont și de tehnologia Cloud Computing. Pot fi auditori și evaluatori care să nu fie familiarizați cu Cloud Computing, în general, sau cu un anumit serviciu de cloud în special. Așa stând lucrurile, se cuvine ca cei care apelează la servicii de cloud să aibă cunoștință despre:

- Dacă reglementările privind utilizarea unui serviciu de cloud dat, sunt aplicabile
- Responsabilitățile privind conformitatea, să fie împărțite între furnizorul și clientul cloud
- Capacitatea furnizorului de cloud de a oferi dovezile necesare pentru dovedirea conformității
- Rolul pe care poate să-l aibă clientul cloud în medierea unor posibile neînțelegeri dintre furnizorul de cloud și auditor / evaluator

Recomandări

✓ Trebuie implicați specialiști în domeniile juridic și contractual. Regulile standard după care funcționează furnizorul de cloud pot să nu se adreseze cerințelor de conformitate ale clientului; de aceea este în beneficiul clientului de a implica încă de la început personal juridic și contractual, cu scopul de a se asigura că prevederile contractuale ale serviciilor de cloud sunt adecvate pentru îndeplinirea obligațiilor de conformitate și de audit.

✓ În privința dreptului la clauza de audit. Clienții vor avea nevoie adesea de posibilitatea de a audita furnizorul de cloud, dată fiind natura dinamică atât a cloud-ului cât și a cadrului de reglementare. Dreptul legat de clauza contractuală de audit trebuie obținut oricând e posibil, de exemplu în cazul particular când, vorbim de un serviciu al furnizorului, pentru care, clientul are responsabilități privind conformitatea de reglementare. Ulterior, nevoia pentru acest drept ar trebui să fie redusă și, în multe cazuri, înlocuită cu certificări corespunzătoare ale furnizorului, în raport cu standardul ISO / IEC 27001.

✓ Trebuie analizată problematica conformității și determinarea dacă reglementările de conformitate adresate organizației vor fi afectate de utilizarea serviciilor de cloud, pentru un anumit set de aplicații și date.

✓ Trebuie analizat impactul reglementărilor asupra securității datelor. Utilizatorii finali potențiali de servicii Cloud Computing ar trebui să ia în considerare aplicațiile și datele pe care le au în vedere la trecerea serviciilor în cloud, precum și măsura în care acestea sunt supuse reglementărilor de conformitate.

✓ Trebuie revizuiti partenerii relevanți și furnizorii de servicii. Aceasta este o orientare generală privind asigurarea că relațiile furnizorului de servicii nu determină impact negativ asupra conformității. Evaluarea furnizorilor de servicii care prelucrează date supuse reglementărilor de conformitate, și apoi evaluarea controalelor de securitate efectuate de către acești furnizori, este fundamentală. Multe reglementari de

conformitate au prevederi specifice cu privire la evaluarea și gestionarea riscurilor furnizor terți. Ca și în cazul serviciilor de IT non-cloud, organizațiile trebuie să înțeleagă care dintre partenerii lor de afaceri cloud prelucrează date care fac obiectul unor reglementari de conformitate.

✓ Trebuie înțelese responsabilitățile contractuale privind protecția datelor și contractele aferente. Modelul de serviciu cloud impune care dintre client sau furnizor de servicii cloud este responsabil pentru implementarea controalelor de securitate. Într-un scenariu de implementare IaaS, clientul are un grad mai mare de control și responsabilitate decât într-un scenariu SaaS. Dintr-un punct de vedere al controalelor de securitate, acest lucru înseamnă că clienții IaaS vor trebui să implementeze multe dintre controalele de securitate pentru conformitatea cu reglementările în vigoare. Într-un scenariu SaaS, furnizorul de servicii cloud trebuie să asigure controalele necesare. Din perspectivă contractuală, este foarte important de înțeles cerințele specifice precum și contractul de servicii cloud și acordurile aferente.

✓ Trebuie analizat impactul reglementărilor asupra infrastructurii furnizorului. În domeniul infrastructurii, trecerea la servicii de cloud, cere analizare minuțioasă. Unele cerințe de reglementare pot duce la controale care sunt greu sau imposibil de realizat în unele tipuri de servicii cloud.

✓ Trebuie analizat impactul reglementărilor asupra politicilor și procedurilor. Migrarea de date și aplicații în serviciile de cloud, probabil că generează impact asupra politicilor și procedurilor. Clienții ar trebui să evalueze care politici și proceduri legate de reglementări vor trebui modificate / actualizate. Exemple de politici și proceduri afectate sunt rapoartele de activitate, jurnalizările, păstrarea datelor, reacția la incidente, controlul testării, precum și politicile de confidențialitate.

✓ Trebuie pregătit probe privind modul de îndeplinire al cerințelor. Colectarea dovezilor de conformitate pe multitudinea de reglementari de conformitate și a cerințelor reprezintă o provocare. Clienții serviciilor de cloud ar trebui să utilizeze procese de colectare și stocare de dovezi de conformitate, cum ar fi jurnalele de audit și rapoarte de activitate, copii ale configurațiilor de sistem, rapoartele privind modificările aplicate, precum și alte rezultate ale procedurilor de testare. În funcție de modelul de serviciu cloud, furnizorul de cloud ar putea avea nevoie de o mare parte din aceste informații.

✓ Chestiunea calificării și selecționării auditorului. În multe cazuri, organizația nu are nicio atitudine în selectarea auditorilor sau a evaluatorilor de securitate. În cazul în care o organizație are un proces de selecție, este recomandabil de a alege un auditor "conștient cloud", deoarece mulți s-ar putea să nu fie familiarizați cu tehnologiile cloud și provocările virtualizării. Testarea familiarizării lor cu terminologia IaaS, PaaS, și SaaS este un bun punct de plecare.

✓ Despre declarațiile de audit SAS 70 -Statement on auditing Standards.

SAS 70 reprezintă un set de declarații referitoare la îndeplinirea standardelor de audit emise de American Institute of Certified Public Accountants. Acestea sunt de 2 tipuri. SAS 70 Type I și Type II sunt utile auditorilor de organizații prestatoare de servicii. Furnizorii de cloud ar trebui să aibă aceste declarații de audit cel puțin la un nivel minim, deoarece acestea vor oferi un punct recunoscut de referință pentru auditori și evaluatori. Din moment ce SAS 70 Type II asigură doar faptul că controalele sunt puse în aplicare așa cum au fost documentate, este important să înțelegem că auditul SAS 70 acoperă o arie largă în privința modului cum controalele satisfac cerințele.

✓ Despre îndeplinirea de către furnizorul de cloud a standardelor ISO/IEC 27001/27002.

Furnizorii de cloud care doresc să ofere servicii critice ar trebui să adopte standardul ISO / IEC 27001 pentru sistemele de management al securității informației - SMSI. În cazul în care furnizorul nu a obținut certificarea ISO / IEC 27001, acestea trebuie să demonstreze alinierea cu practicile ISO 27002 de management al securității informațiilor. Alianța Cloud Security emite un apel la acțiune pentru a alinia furnizorii de cloud la certificarea ISO / IEC 27001.

Anexa nr. 1 - Caracteristici

1. ASPECTE NON-FUNCȚIONALE

Cele mai importante aspecte non-funcționale sunt:

Elasticitatea este un aspect esențial central al sistemelor de cloud computing și se circumscrie capacității de a susține infrastructura să se adapteze la cerințele non-funcționale în continuă schimbare, de exemplu cantitatea și dimensiune datelor suportate de o aplicație, numărul de utilizatori concomitenți etc. Se poate distinge între scalabilitatea orizontală și verticală, unde scalabilitatea orizontală se referă la suma instanțelor de satisfăcut, de exemplu numărul de cereri care se schimbă, iar scalabilitatea verticală se referă la dimensiunea instanțelor și astfel, implicit la suma resurselor necesare care mențin dimensiunea.

Fiabilitatea este esențială pentru toate sistemele de cloud computing – pentru a susține aplicațiile prezente de tip centru de date într-un cloud, fiabilitatea este considerată unul dintre aspectele principale pentru exploatarea capacităților cloud computing-ului. Fiabilitatea denotă capacitatea de a asigura operarea constantă a sistemului fără întrerupere, adică nicio pierdere de date, nicio resetare a codului pe durata executării etc. Fiabilitatea se atinge de obicei prin utilizarea redundantă a resurselor. În mod interesant, multe dintre aspectele de fiabilitate de la o soluție pe bază hardware la una pe bază software. (Redundanța din sistemele de fișiere vs. controlerile RAID, servere statice front end vs. UPS etc.). În mod remarcabil, este o relație puternică între disponibilitate (mai jos prezentată) și fiabilitate, fiabilitatea se centrează mai ales pe împiedicarea pierderii (datelor sau progresul executării).

Calitatea suportului de servicii este o capacitate relevantă, esențială în multe cazuri de utilizare în care anumite cerințe trebuie să fie satisfăcute prin servicii externalizate și/sau resurse. În cazurile de afaceri, măsurătorile de bază QoS precum timpul de răspuns, randamentul etc. trebuie să fie cel puțin garantate, pentru a se asigura că garanțiile de calitate ale utilizatorului de cloud sunt respectate. Fiabilitatea este un aspect QoS particular care formează o cerință specifică de calitate.

Agilitatea și adaptabilitatea sunt aspecte esențiale ale sistemelor de cloud computing care sunt asociate în mod puternic cu capacitățile elastice. Include reacția on-time la modificările de cantitate a cererilor și dimensiunea resurselor, dar și adaptarea la modificările condițiilor de mediu care, de exemplu, necesită tipuri diferite de resurse (sau cel puțin administrarea lor) care să fie autonome și să le activeze pentru a furniza auto-capacități.

Disponibilitatea serviciilor și a datelor este o capacitate esențială a sistemelor de cloud computing și a fost, de fapt, unul dintre aspectele centrale care au dus la apariția cloud computing-ului în primă instanță. Disponibilitatea reiese din capacitatea de a introduce redundanța pentru servicii și date, astfel încât eșecurile pot fi transparent mascate. Toleranța la defecte impune și capacitatea de introduce o nouă redundanță (de exemplu noduri defecte sau noi) în manieră online fără intruziune (fără o penalizare semnificativă pentru performanță). Disponibilitatea se atinge mai ales prin replicarea datelor / a serviciilor și distribuirea lor cu diverse resurse pentru a atinge echilibrul sarcinii. Acest lucru poate fi privit ca esența originală a scalabilității din sistemele cloud.

2. ASPECTE ECONOMICE

Pentru considerații economice, sistemele de cloud computing ajută la realizarea următoarelor aspecte:

Reducerea costurilor este una dintre principalele preocupări pentru construirea unui sistem cloud care se poate adapta la comportamentul consumatorului și reduce costul pentru achiziția și întreținerea infrastructurii. Scalabilitatea și plata în funcție de utilizare sunt aspecte esențiale ale acestei probleme. Astfel, stabilirea unui sistem de cloud computing presupune de obicei costuri adiționale – fie prin adaptarea logicii de afaceri la interfețele specifice cloud host sau îmbunătățind infrastructura locală să fie „cloud-ready”. Vedeți și randamentul investițiilor mai jos.

Plata în funcție de utilizare. Capacitatea de a construi costul în conformitate cu consumul real de resurse este un aspect relevant al sistemelor de cloud computing. Plata în funcție de utilizare privește calitatea suportului de servicii, unde cerințele specifice ce trebuie atinse de către sistem și astfel plătite pot fi specificate. Unul dintre motoarele economice cheie pentru nivelul curent al interesului în cloud computing este modificarea structurală din acest domeniu. Trecând de la un model de investiție de capital normal la o cheltuială operațională, cloud computing promite să permită mai ales IMM-urilor și antreprenorilor să accelereze dezvoltarea și adoptarea soluțiilor inovatoare.

Timpul îmbunătățit de introducere pe piață, mai ales pentru întreprinderile mici și mijlocii care vor să își vândă serviciile repede și ușor cu mici întârzieri provocate de achiziția și stabilirea infrastructurii, mai ales în scop compatibil și competitiv cu industriile mari. Întreprinderile mai mari trebuie să poată publica noile capacități cu mici cheltuieli generale pentru a rămâne competitive. Cloud computing-ul poate susține acest lucru asigurând infrastructurile dedicate anumitor cazuri de utilizare specifice care preiau capacitățile esențiale pentru a susține previzionarea ușoară și astfel pentru a reduce timpul de introducere pe piață.

Returnarea investițiilor (ROI) este esențială pentru toți investitorii și nu poate fi garantată întotdeauna – de fapt, unele sisteme de cloud computing dau greș în acest aspect. Pentru a fi viabil din punct de vedere comercial, cei care doresc migrarea în cloud trebuie să se asigure că efortul și costul sunt depășite de beneficii – acest lucru poate presupune ROI direct (de exemplu mai mulți clienți) și indirect (de exemplu beneficiile din publicitate). Externalizarea resurselor versus creșterea infrastructurii locale și folosirea tehnologiilor (private) cloud necesită astfel să fie depășită și punctele limită să fie identificate.

Transformarea CAPEX în OPEX este o caracteristică implicită și controversată a sistemelor de cloud computing, deoarece beneficiul real de cost (cf. ROI) nu este întotdeauna clar. Cheltuielile de capital (CAPEX) sunt necesare pentru a construi infrastructura locală, dar prin externalizarea resurselor computaționale către sisteme cloud la cerere și scalabile, o companie va face de fapt cheltuieli operaționale (OPEX) pentru furnizarea capacităților, deoarece va achiziționa și utiliza resursele în conformitate cu nevoile operaționale.

„Ecologizarea” este relevantă nu numai pentru a reduce costurile suplimentare de consum de energie, dar și pentru a reduce amprenta de carbon. În timp ce emisia de carbon a mașinilor individuale poate fi estimată destul de bine, aceste informații sunt foarte puțin luate în considerare când se scalează sistemele pe Cloud, ceea ce permit reducerea consumului de resurse neutilizate (reducere). În plus, escaladarea trebuie să fie foarte bine echilibrată cu costurile, dar și cu problemele asociate cu emisiile de carbon.

3. ASPECTELE TEHNOLOGICE

Principalele provocări tehnologice care pot fi identificate și care sunt asociate cu sistemele de cloud computing sunt:

Virtualizarea este o caracteristică tehnologică esențială care ascunde complexitatea tehnologică de utilizator și permite flexibilitate sporită (prin agregare, rutare și translație). Mai concret, virtualizarea susține următoarele aspecte:

Facilitatea: ascunzând complexitatea infrastructurii (inclusiv management, configurare etc.), virtualizarea poate face mai simplu pentru utilizator să dezvolte noi aplicații, cât și reduce timpul suplimentar pentru controlarea sistemului.

Independența infrastructurii: în principiu, virtualizarea permite interoperabilitate mai ridicată făcând platforma de cod independentă.

Flexibilitatea și adaptabilitatea: expunând un mediu virtual de executare, infrastructura de susținere se poate face mai flexibilă în conformitate cu diversele condiții și cerințe (desemnarea mai multor resurse etc.).

Independența amplasării: serviciile pot fi accesate independent de amplasarea fizică a utilizatorului și a resursei.

Partajarea serviciilor este o problemă esențială în sistemele de cloud computing, unde situarea codului și/sau datelor este în principal necunoscută și aceeași resursă se poate alocă mai multor utilizatori (chiar și în același timp). Acest lucru afectează resursele infrastructurii, dar și datele / aplicațiile / serviciile care sunt găzduite pe resurse partajate, dar trebuie făcute disponibile în multiple instanțe izolate. În mod clasic, toate informațiile sunt menținute în baze de date separate sau tabele, cu toate acestea, în cazuri mai complicate, informațiile pot fi modificate concurrent, chiar dacă sunt menținute pentru diverși utilizatori izolați. Partajarea serviciilor implică multe probleme potențiale, de la protecția datelor la problemele legislatorului.

Securitatea, confidențialitatea și complianța sunt evident esențiale pentru toate sistemele care manipulează date sau cod potențial sensibil.

Managementul datelor este un aspect esențial mai ales pentru stocarea datelor, acolo unde datele sunt distribuite flexibil pe mai multe resurse. Implicit, consistența datelor trebuie să fie menținută peste o distribuție largă a surselor de date replicate. Deoarece dimensiunea datelor se poate modifica din când în când, managementul datelor se adresează atât aspectelor verticale cât și orizontale ale scalabilității. Un alt aspect crucial al managementul de date este furnizarea garanțiilor de consistență (consistența eventuală vs. puternică, izolarea translației vs. nicio izolare, operațiunile atomice pe itemi individuali de date vs. multipli timpi de date etc.).

API (application programe interface) și/sau îmbunătățirea programării sunt esențiale pentru a exploata aspectele cloud computing-ului: modelele comune de programare necesită ca dezvoltatorul să fie atent la

scalabilitate și capacitățile autonome, în timp ce mediul cloud asigură capacitățile într-un mod care permite utilizatorului să lase acest management sistemului.

Măsurarea oricărui tip de resurse și consumul de servicii sunt esențiale pentru a oferi prețuri elastice, facturare și tarify. De aceea este o condiție preliminară pentru elasticitatea cloud-ului.

Anexa nr. 2 - Analiza SWOT

Punctele tari	Punctele slabe	Oportunitățile	Amenințările
• costuri fixe • Nicio infrastructură • Acces din întreaga lume • Actualizări software • Reduce orele suplimentare • Controale de securitate consistente echilibrate pe infrastructura cloud (DDOS, Firewall-ing, verificări de vulnerabilitate, antimalware etc.) • Cunoștințe și experiență în domeniile tehnologice asociate • Experiență semnificativă în construirea de aplicații specifice industriei • Proiecte continue de cercetare și tehnologii open source • SOA puternic (Service Oriented Architecture) și sisteme distribuite în comunitatea de cercetare • Sinergii puternice între cercetare și industrie; Platforme tehnologice • Eforturi guvernamentale concertate (legislație etc.) • Vânzare de produse și telecomunicații (față de vânzare de noi tehnologii) • Furnizarea de procese complexe precum servicii, în loc de	• Securitatea platformei necontrolată de consumatorul de servicii • Confidențialitatea, regulile de complianță IP și reglementare diversă trebuie avute în vedere dinainte • Lățime de bandă disponibilă • Bariere tehnice • Lipsa controlului modificării • Calendare de cercetare vs. piețe în continuă mișcare • Niciun ecosistem al pieței în jurul furnizorilor din România • Sucursale și fragmentarea industriilor cheie • Nicio platformă pentru căutarea / selectarea furnizorilor	• Flexibil • Integrare viitoare • Canale suplimentare client • Costuri mai reduse de deținere • Scalabilitate • Fuziuni / achiziții: Adaptare mai rapidă • Experiență puternică în implicarea în eforturile de standardizare • Companiile românești utilizează (și au nevoie de) proprii clouds (clouds privați) • Interes sporit din partea industriei și a mediului academic în tehnologiile cloud • Infrastructurile existente cu resurse puternice și mai ales cu rețelele puternice de comunicații puternice (de exemplu telecoms) • Clouds asigură o susținere excelentă pentru aplicațiile de telefonie mobilă (care de obicei au resurse locale cu putere redusă). • Creșterea competitivității și a productivității, a furnizorilor de servicii prin adoptarea platformelor computaționale locale / hibride / specifice • Furnizarea aplicațiilor în loc de orientarea pe	• Indisponibilitate • Imposibilitatea de a personaliza • Protecția datelor • Este posibil ca clienților să nu le placă datele în cloud • Procedura de restaurare mai lentă, mai puțin flexibilă, pierderea granularității • Investiții ridicate și fonduri necesare pentru construirea infrastructurii • Lipsa furnizorilor IaaS • Impact tehnologic / dezvoltare subestimată

infrastructuri de nivel redus • Industrie de telecomunicații puternică (cercetare, orientare asupra consumatorului, capacități de investiție) • Povești comerciale de succes		tehnologie • Noi modele business pentru produse îmbunătățite și adoptare de cloud • Conștientizare a agendei ecologice și noi metode de a reduce amprenta de carbon	
--	--	---	--

Anexa nr. 3 Studii suport pentru utilizarea Cloud-ului în România

Numeroase studii legate de adoptarea cloud-ului ([BSA](#) – pentru utilizatori de PC-uri; [TechSoup](#) – pentru ONG-uri; [CIO Council](#) – pentru organizații mari) confirmă un interes ridicat pentru cloud computing în România și, în general, o deschidere mai ridicată față de celelalte țări.

- [Studiu CIO Council](#) (pe întreprinderi mari, iulie 2013): 60% dintre întreprinderile mari din România folosesc Cloud și până în 2017 acest procent va crește la 100%.
- [Studiu IPSOS Mori](#) (pe companii cu mai puțin de 25 de angajați, iunie 2013): puțin peste jumătate dintre firmele mici din România folosesc soluții de Cloud și 38% dintre companiile intervievate vor direcționa bugetele IT în soluții Cloud.
- [Studiu BSA](#) (pe utilizatori de PC-uri, august 2012): în Europa, România ocupă locul al patrulea în topul țărilor cu cel mai ridicat nivel de familiarizare cu soluțiile de cloud computing: unul din cinci utilizatori români (20%) se consideră cunoscător al soluțiilor bazate pe cloud.
- [Studiu TechSoup](#) (pe organizații non-guvernamentale, septembrie 2012): unul dintre cele mai accelerate ritmuri de adoptare a soluțiilor bazate pe Cloud din lume în rândul ONG-urilor din România (13% dintre ONG-uri în următoarele 6 luni, 19% în 6-12 luni, 31% în 1-2 ani, 16% în următorii 2-3 ani).