Audit financiar, XIV, Nr. 3(135)/**2016**, *248-257*
ISSN: 1583-5812; ISSN on-line: 1844-8801

Auditul securității pentru sistemele informatice bazate pe Cloud

Dragoş Marian MANGIUC,
Academia de Studii Economice din Bucureşti,
e-mail: mangiuc@gmail.com

Rezumat

Urmărind comportamentul standard aferent oricărei schimbări majore de paradigmă din istoria tehnicii de calcul, migrația către sistemele informatice bazate pe cloud a suportat şi suportă atât laude masive, cât şi critici majore. Întrucât avantajele orientării spre cloud sunt evidente, în special pentru companiile de dimensiuni mici şi mijlocii, criticii noilor tehnologii se concentrează asupra dezavantajelor. Dintre acestea, securitatea este considerată a fi cel mai important dezavantaj.

Articolul de față urmăreşte conturarea unei imagini reale a nivelului de securitate al sistemelor informatice bazate pe cloud, dincolo de numeroasele mituri şi concepții greşite cu care se confruntă un auditor. Cercetarea se bazează pe o parcurgere a literaturii relevante pentru domeniul sistemelor informatice bazate pe cloud şi este construită pornind de la o serie de rezultate sintetice obținute în urma unei analize informale a opiniilor şi a experienței în domeniu dobândite în ultimii ani de auditori români şi străini care au acceptat un interviu. Scopul principal al articolului este să stabilească dacă, din perspectiva unui auditor, sistemele informatice bazate pe cloud sunt mai sigure sau mai puțin sigure, prin comparație cu sistemele informatice „tradiționale", sau cu cele dezvoltate în antrepriză proprie (in-house). Articolul se subscrie unui demers de cercetare mai larg în domeniul tehnologiilor bazate pe cloud şi al altor tehnologii înrudite.

Cuvinte-cheie: *Securitate în cloud, Software as a Service, Platform as a Service, Infrastructure as a Service, audit de securitate*

Clasificare JEL: *L86*

Vă rugăm să citați acest articol astfel:
Mangiuc, D.M. (2016), Auditing security for the Cloud, *Audit Financiar*, vol. XIV, nr. 3(135)/2016, pp. 302-311, DOI: 10.20869/AUDITF/2016/135/302.

Link permanent pentru acest document:
http://dx.doi.org/10.20869/2016/AUDITF/2016/135/302

Introducere

Domeniul securității în implementarea, administrarea, utilizarea şi auditul aplicațiilor bazate pe cloud reprezintă tema principală a criticilor acestui sistem de distribuire a produselor software. În timp ce furnizorii de servicii cloud pretind că noua tehnologie este cea mai sigură variantă existentă în istoria informaticii, ignorând adesea probleme de securitate evidente, scepticii au tendința să „demonizeze" noua paradigmă, prezentând-o ca pe un sfârşit al adevăratei securități şi începutul unei ere „întunecate", în care dreptul la intimitate nu mai este decât o iluzie bine întreținută. Ceea ce face ambele puncte de vedere demne de analizat este faptul că, deşi diametral opuse, ambele tipuri de discurs au tendința să prezinte probleme colaterale sau în unele cazuri, inexistente, ca pe „marele impediment al tehnologiilor cloud", neglijând adesea elemente evidente şi demne de studiat. Prins în mijlocul celor două curente antagoniste, auditorul are datoria de a creşte nivelul de detaliu al expertizei realizate şi de a-şi completa propriile cunoştințe în domeniu până la un nivel rezonabil, pentru a nu cădea într-o extremă sau alta şi a-şi compromite imparțialitatea.

Prin natura sa, paradigma cloud moşteneşte o mare parte din problemele de securitate ale sistemelor anterioare de gestiune şi utilizare a aplicațiilor software, nefiind suficient de diferită de acestea pentru a le elimina complet. Pe de altă parte, fundamentarea livrării şi utilizării aplicațiilor prin intermediul rețelei Internet le face extrem de dependente de natura şi modul de operare al acesteia, ceea ce conduce la „moştenirea" unor probleme de securitate, care sunt, de multe ori, omise (intenționat sau nu), atât de cei care laudă noua abordare, cât şi de cei care o critică. Unele dintre problemele prezentate ca „motive majore de eşec" ale noilor tehnologii bazate pe cloud, sunt, de fapt, la fel de vechi ca tehnica de calcul, iar timpul a dovedit fără echivoc în ce măsură (şi cu ce costuri) riscurile ataşate lor pot fi gestionate sau minimizate.

Lucrarea de față îşi propune să utilizeze atât literatura relevantă pentru acest domeniu (din ce în ce mai consistentă), cât şi datele obținute prin interviuri cu persoane direct implicate în aspectul analizat la nivel local şi internațional, pentru a realiza o imagine clară a percepției auditorului cu privire la problemele reale de securitate în cloud, neafectată de interesul comercial sau de politicile de marketing agresive, caracteristice oricărui produs nou pe piață. Deşi nu există în prezent suficiente date de tip cantitativ pentru a elabora o propunere de model coerent destinat estimării securității unui sistem informatic de tip cloud şi realizării de comparații cu sistemele informatice tradiționale (acesta fiind obiectivul final al unei cercetări mai ample în domeniu), este posibilă estimarea comparativă a nivelelor de securitate aferente celor două tipuri de sisteme.

1. Metodologia de cercetare

Prezentul articol reprezintă unul din rezultatele unui studiu mai larg, efectuat în domeniul tehnologiilor bazate pe cloud şi al celor din categoria Enterprise 2.0 şi dezvoltă o cercetare în domeniul tehnicilor şi instrumentelor de audit asistat informatic.

În măsura în care acest lucru a fost posibil, s-a realizat o identificare directă a aşteptărilor practicienilor din domeniul studiat, prin interviuri directe sau pe baza unui chestionar. În cazul utilizării chestionarului, întrebările au fost formulate astfel încât să permită obținerea de răspunsuri imparțiale şi obiective. Membrii grupului chestionat au fost încurajați să adauge propriile păreri legate de chestionarul utilizat. Validarea concluziilor cercetării s-a realizat şi prin intermediul unor interviuri directe cu practicieni, membri ai unor organizații care au realizat sau sunt în curs de a realiza o migrare a propriilor servicii către cloud. De câte ori a fost posibil, s-a cerut şi părerea unor profesionişti aparținând unei companii care acordă consultanță şi asistență în procesul de migrație către cloud. O serie de concluzii sunt bazate pe rezultatele unor studii de piață sau ale unor cercetări anterioare.

2. Cine este proprietarul real al informațiilor stocate în Cloud?

Pe 17 august 2009, Departamentul de Justiție al Statelor Unite a anunțat public faptul că 130 de milioane de numere de card de credit au fost furate în cadrul a ceea ce urma să fie numit cel mai mare furt de identitate din istoria informaticii (US Department of Justice, 2009). La câteva zile după acest anunț, a fost acuzat în mod oficial şi autorul furtului, un fost angajat al serviciilor secrete, specializat în urmărirea şi identificarea hackerilor, care a preluat datele despre cardurile de credit exploatând

lipsuri de securitate ale rețelelor de calculatoare aparținând marilor vânzători de bunuri de consum.

Pornind de la studiul evenimentelor de acest tip, se poate observa faptul că o mare parte a breşelor sistemelor de securitate nu apar ca urmare a neglijenței celor responsabili, ci ca urmare a unor atacuri extrem de ingenioase ale unor experți în domeniul securității, al căror nivel de cunoştințe despre securitatea informatică îl depăşeşte, în anumite cazuri, pe cel al angajaților companiei care se ocupă cu implementarea mecanismelor de securitate şi, câteodată, chiar şi pe cel al experților solicitați să auditeze nivelul de securitate al sistemului informatic. Ca urmare, deşi organizațiile evaluează şi reevaluează permanent nivelul riscului de securitate, implementează sisteme de control intern, instalează şi configurează echipamente de tip firewall şi alte tehnologii asimilate, stabilesc procese şi protocoale de backup şi solicită elemente de securitate auditate şi auditabile pentru echipamentele hardware şi software achiziționate, breşele de securitate continuă să apară. În plus, la intervale tot mai reduse de timp, vânzătorii de soluții de securitate oferă noi variante, care se consideră a fi 100% sigure, ceea ce, în mod evident, se dovedeşte a fi cel puțin exagerat.

Din punct de vedere istoric, una dintre cele mai cunoscute „soluții miraculoase" de securitate a fost *Kerberos*, oferit la începutul anilor '90 ca fiind soluția universală a problemelor de securitate informatică (Perez-Mendez ş.a., 2012). Totuşi, gloria sa a apus repede (Bajpai, Vardhan şi Kushwaha, 2012), iar problemele de securitate asociate au continuat să existe. Câțiva ani mai târziu se considera că sistemul informatic al NASA a atins nivelul absolut al securității informatice (Reed, 2012). Cu toate acestea, cele câteva atacuri informatice reuşite au condus la auditarea securității sistemului informatic al NASA de către Congresul Statelor Unite, prin organismul său numit *General Accountability Office – GAO* (Purpura, 2013). Concluziile auditului au relevat faptul că rezultatele raportate de agenția spațială erau mult exagerate, iar costurile cu implementarea sistemului de securitate nu se justificau prin comparație cu nivelul rezultatelor obținute (Berriman ş.a., 2012). NASA nu a fost singura organizație care şi-a exagerat rezultatele în domeniu, atacurile ulterioare asupra companiilor *Microsoft* sau *Citibank* relevând o adevărată tendință în acest sens (Nunes şi Merrihue, 2007).

În urma realizării unei sinteze a literaturii de specialitate pot fi formulate următoarele concluzii:

- Datele de pe serverele Web sunt, în majoritatea cazurilor, necriptate, securitatea concentrându-se asupra limitării accesului din exterior şi încercând să realizeze un „zid" în jurul fiecărui server, după penetrarea căruia nu mai există niciun sistem de securitate intern;
- Majoritatea tranzacțiilor realizate on-line nu beneficiază de un sistem de auditare *post-factum*, aceasta realizându-se numai la nivelul sistemului de securitate ca ansamblu, iar rezultatele fiind apoi extrapolate asupra tuturor tranzacțiilor realizate;
- Modul în care distribuitorii de produse software şi utilizatorii acestora îşi gestionează securitatea propriilor sisteme este departe de a fi transparent (ceea ce, în majoritatea cazurilor, este de înțeles).

Toate aceste fenomene au fost observate cu mult timp înaintea apariției modelului *cloud computing* şi a tehnologiilor care îl utilizează, şi, ca urmare, acesta nu poate fi considerat vinovat de existența fenomenelor respective. Diferența majoră este că deşi înaintea apariției tehnologiilor bazate pe cloud existau astfel de cazuri, acestea erau relativ izolate, şi, ca urmare, efectele negative erau relativ facil de gestionat sau eliminat, breşele de securitate fiind acoperite rapid. Apariția tehnologiilor bazate pe cloud a condus la apariția a milioane de servere, cu un număr de accesări din partea clienților care ar fi părut imposibil cu câțiva ani înainte (Han, Susilo şi Mu, 2013). Cea mai bună dovadă în acest sens este celebra „criză a adreselor de IP" care a arătat că însăşi rețeaua Internet, în acele momente, ajunsese să îşi atingă limitele fizice. În aceste circumstanțe, pentru un auditor, se impune identificarea răspunsurilor corecte la două întrebări esențiale:

- Cine este adevăratul proprietar al informației stocate în cloud?
- Care dintre părțile implicate este grevată de responsabilitatea principală pentru asigurarea securității informațiilor stocate în cloud?

Răspunsul la prima întrebare pare să fie „organizația care beneficiază de serviciile cloud şi are rolul de utilizator". Elementele de informație stocate de către un furnizor de servicii cloud aparțin clienților săi, angajaților săi, conturilor şi portofoliilor pe care le administrează. În aceste condiții, problema securității devine extrem de discutabilă, odată ce devine evident că valorile de natură

informațională nu se află sub supravegherea directă a proprietarului lor de drept, ci a unei entități externe (furnizorul de infrastructură sau de servicii bazate pe cloud).

Această „răsturnare" a responsabilităților conduce la o a doua întrebare importantă şi anume: „Îşi asumă furnizorul de servicii cloud responsabilitatea legală în cazul unor scurgeri de date sau a unui furt de identitate, cu acoperirea tuturor daunelor?" Deşi după cunoştințele autorului şi părerile altor autori (Li ş.a., 2013), domeniul cloud nu a fost încă testat la nivelul sistemului juridic, neexistând probleme şi spețe suficient de importante pentru a se crea un precedent solid, totuşi, comportamentul furnizorilor de servicii informaționale în cazuri similare (care nu implicau tehnologii bazate pe cloud) nu poate fi considerat ca liniştitor. De exemplu, într-un caz de furt de identitate, hackerii au „golit" întreaga linie de credit a clientului unei bănci franceze. În aceste condiții, banca nu numai că nu a recunoscut nicio parte din vină, dar, mai mult, a solicitat în continuare plata de rate cu dobândă clientului său, pentru întreaga sumă sustrasă de hackeri. Un tribunal a anulat intenția băncii de a percepe dobândă, dar nu a obligat-o pe aceasta să suporte şi valoarea sumei sustrase, întrucât gestiunea contului nu era realizată de către bancă, ci era realizată direct de către client, printr-un serviciu de tip *Internet banking* (Edwards, 2014).

Furtul de identitate urmează, de regulă, un model standard. Autorul faptei ajunge în posesia unui set de informații esențiale cu privire la victimă (identitate, parole, numere de cont etc.), pe care le utilizează pentru a accesa resursele financiare ale acesteia şi chiar pentru a accesa noi surse de finanțare (linii de credit, carduri de credit etc.). Este posibil chiar ca autorul faptei să efectueze depuneri şi să plătească rate pentru o perioadă de timp, în scopul de a creşte limita de credit sau de a nu trezi suspiciuni până la realizarea loviturii finale. În momentul în care datoriile respective întârzie la plată, creditorii se vor întoarce împotriva persoanei în numele căreia au fost făcute creditele (victima), care va trebui să inițieze acțiunile legale de identificare şi urmărire a autorului faptei, în caz contrar fiind singura persoană responsabilă pentru achitarea acestora. Întrucât un studiu recent arată că numai în Statele Unite au loc circa 750.000 de tentative reuşite de furt de identitate anual (Ren, Wang şi Wang, 2012), întrebarea evidentă este: „Va permite setul de tehnologii cloud repetarea acestui scenariu la scară mondială?" Din păcate, răspunsul nu poate fi dat cu uşurință, nefiind la fel de evident.

3. Responsabilitate şi răspundere

Concluzia care se desprinde din analiza situației actuale este că în lipsa unei gestiuni coerente a securității în cloud, aceasta va putea conduce la creşterea cu un ordin de magnitudine a fenomenelor negative datorate în prezent breşelor de securitate. Un studiu recent al modului în care se negociază contractele între beneficiarii serviciilor de tip cloud şi furnizorii acestora (Carlsson şi Fuller, 2013) sugerează faptul că în situația în care un beneficiar de servicii cloud va suferi pagube majore din infracțiuni informatice, în timp ce baza sa de date este găzduită în cloud de către un furnizor, acel furnizor nu va putea fi făcut răspunzător de nicio parte din consecințe. Din punctul de vedere al unui auditor, această perspectivă este cel puțin interesantă, ținând cont de faptul că nivelul de securitate şi controlul accesului la servere este realizat în totalitate de compania care deține acele servere (furnizorul de servicii de tip cloud), nicidecum de clienții acesteia. Ca urmare, furnizorul serviciilor de tip cloud ar trebui să aibă răspundere legală clară şi explicită pentru nivelul de securitate şi protecție asociat serviciului pe care îl oferă. În plus, organizațiile care beneficiază de aceste servicii trebuie să înțeleagă faptul că termenul „public cloud" implică următoarele:

- Nivelul de acces este astfel realizat încât să permită accesul liber al tuturor celor care doresc să beneficieze de respectivul serviciu;
- Printre beneficiarii serviciului pot fi şi persoane cu intenții malițioase, care se vor pretinde utilizatori legitimi.

Din punct de vedere conceptual, obiectivele de securitate se implementează prin intermediul unui set de principii de proiectare a aplicațiilor şi a serviciilor (care definesc cadrul conceptual al tehnologiilor de securitate), precum şi prin intermediul unor dispozitive hardware şi aplicații software care implementează cadrul conceptual definit. Prin natura sa, tehnologia are un caracter dual, întrucât principiile de proiectare care implementează securitatea şi cele care permit obținerea de sisteme funcționale mai ieftine şi mai flexibile se contrazic adesea, obligând organizațiile la realizarea de compromisuri nedorite, dar imposibil de evitat. Aceste conflicte nu apar numai la nivelul tehnologiilor IT, ci pot afecta chiar nivelul procesului de afaceri aflat la baza acestor tehnologii. Dacă se acceptă premisa că utilizarea tehnologiilor cloud permite reducerea costurilor

şi facilitarea accesului la servicii, atunci, cu fiecare creştere a accesului, problemele de securitate (tentativele de fraudă) vor creşte în mod direct proporțional.

Se poate considera că, mai devreme sau mai târziu, toată lumea va încerca să beneficieze de servicii de tip cloud, întrucât o mare parte dintre acestea sunt disponibile în mod gratuit, fiind suportate din publicitate. Dacă un serviciu de e-mail bazat pe cloud este oferit fără a se percepe vreo taxă, atunci costurile reale ale acestui serviciu pot fi complet invizibile pentru utilizatorii săi, ponderea în care acestea includ elemente de securitate şi asigurarea protecției datelor personale neputând fi aflată de către un beneficiar al serviciului. Aceste probleme devin elemente de interes nu numai pentru persoanele şi organizațiile care apelează la servicii de tip cloud, ci şi pentru persoanele şi organizațiile care iau în calcul posibilitatea unei migrații. Companiile de dimensiuni mici şi mijlocii (IMM) sunt atrase de o ofertă de servicii de poştă electronică bazate pe cloud, mai ales dacă aceasta va permite integrarea directă în *browser* cu alte aplicații de gestiune a relațiilor cu clienții sau de gestiune a resurselor întreprinderii. Totuşi, pe măsură ce numărul clienților astfel gestionați creşte, problemele de securitate încep să prindă contur. Studii empirice (Pervez ş.a., 2013) relevă faptul că anumiți consumatori ar accepta să renunțe „într-o oarecare măsură" la intimitate pentru a beneficia de un serviciu complet gratuit, dar, când acel prag de semnificație este depăşit, lucrurile se impun a fi reevaluate. Un sondaj realizat printre utilizatori ai acestui tip de servicii, care dețin şi o serie de cunoştințe avansate în domeniul informatic, a condus la următoarele rezultate:

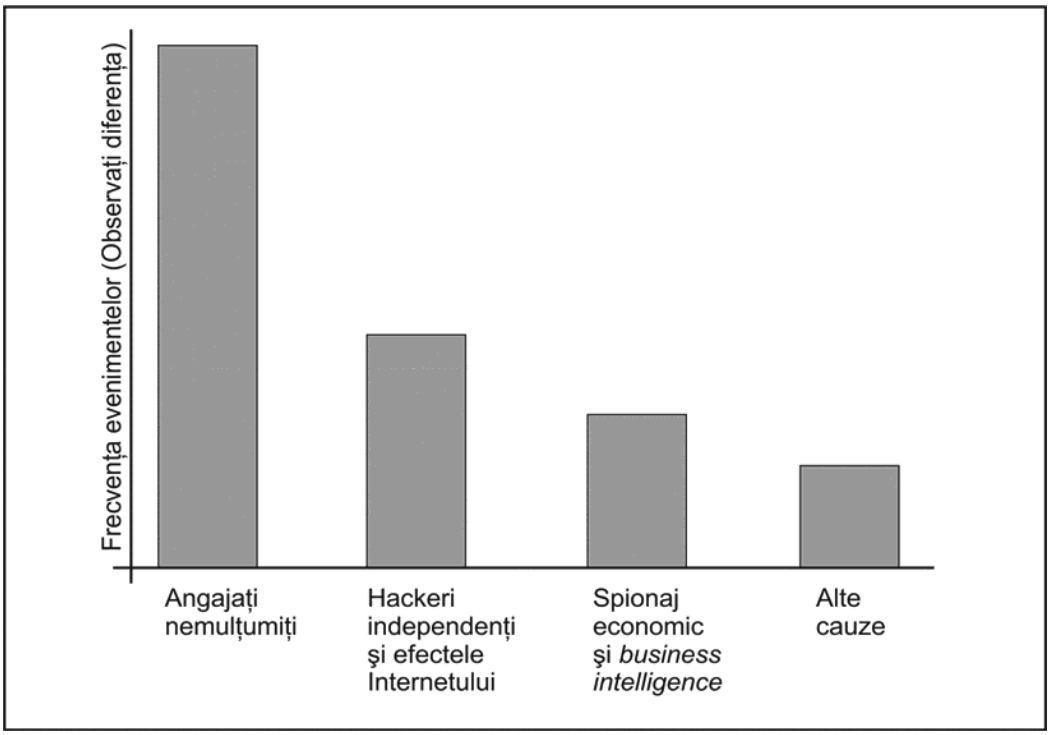
- La întrebarea „*Considerați că aveți un nivel de control suficient asupra datelor personale?*", peste 87% dintre cei intervievați au răspuns pozitiv, invocând în favoarea opiniei lor şi normele legale în vigoare privind prelucrarea datelor cu caracter personal.
- La întrebarea „*Sunteți conştient de faptul că furnizorul serviciului are dreptul de a utiliza datele dumneavoastră personale pentru a direcționa procesul de publicitate?*", numai 32% au răspuns pozitiv, considerând că posibilitatea de a-şi edita propriul profil reprezintă o soluție suficientă la această problemă.

Toate aceste elemente, fie ele de natură tehnică, personală sau de afaceri, afectează modul în care oamenii, companiile şi auditorii privesc securitatea informației. În plus, din discuții cu profesionişti în domeniul tehnologiilor bazate pe cloud rezultă că explozia acestor tehnologii va face sarcinile administrative din domeniul securității extrem de complexe, poate chiar imposibil de gestionat. Mai mult, posibilitatea unor atacuri provenind „din interior" nu poate fi eliminată. Un sondaj al FBI din 2012 (US House of Representatives, 2012) relevă faptul că numărul de atacuri malițioase realizate de către foşti angajați nemulțumiți este de două ori mai mare decât numărul atacurilor realizate de hackeri. Conform aceluiaşi sondaj, pe locul al treilea se află atacurile de tip *business intelligence*, traduse ca acțiuni de spionaj economic ale competitorilor, de asemenea facilitate de către tehnologiile bazate pe cloud. Rezultatele sondajului sunt prezentate în **Figura 1**, aşa cum au fost prezentate şi în sondajul original, fără informații cantitative, scopul acestuia fiind conştientizarea ponderii fiecărui tip de atacuri în totalul problemelor de securitate.

Prin comparație cu sistemele de tip public bazate pe cloud, cele de tip privat se poziționează mai bine din punct de vedere al securității, întrucât organizația care utilizează serviciul are şi proprietatea şi controlul asupra infrastructurii aferente serviciului. Totuşi, majoritatea structurilor de tip *private cloud* deține conexiuni de bandă largă cu structuri de tip *public cloud* (în vederea asigurării unei scalabilități cât mai elastice), ceea ce nu le face imune la problemele de securitate aferente serviciilor publice.

Soluția pentru păstrarea riscului aferent sistemelor informatice bazate pe cloud la un nivel rezonabil şi gestionabil este stabilirea şi respectarea unor standarde comune de securitate, atât la nivelul furnizorilor de servicii, cât şi la nivelul beneficiarilor acestora. De asemenea, la nivelul Uniunii Europene, sau poate chiar la nivel mondial, se impune înființarea unei autorități de securitate şi audit pentru cloud, cu putere de reglementare. Din păcate, deşi numeroase voci (atât din interiorul, cât şi din afara mediului academic) au enunțat această necesitate, propunerea nu a fost luată în considerare de către cei în măsură să reglementeze apariția şi funcționarea unei astfel de autorități.

Figura 1. Originile riscurilor de securitate informatică



Sursa: FBI, 2012

După cum relevă un sondaj anterior (Mangiuc, 2012), organizațiile care beneficiază de servicii bazate pe cloud ar trebui să adopte o atitudine mai realistă în privința problemelor de securitate, atunci când contractează respectivele servicii. Câteva dintre organizațiile chestionate păreau să neglijeze masiv problemele de securitate, motivând că reducerea de costuri permisă de abordarea cloud este prea importantă pentru a fi trecută cu vederea. În mod evident, migrarea de la o soluție *in-house* la o soluție cloud va presupune un compromis între securitate, performanță şi costuri. În aceste condiții, următoarele reguli sunt esențiale:

- Nivelul de securitate solicitat unui furnizor de servicii cloud nu trebuie stabilit în funcție de prețul ofertei acestuia, ci în funcție de nivelul riscului operațional pe care îl implică;
- Compromisurile masive în domeniul securității semnifică, în esență, lipsă de profesionalism din partea conducerii organizației, ceea ce poate face persoanele respective direct răspunzătoare în cazul unei scurgeri masive de informații, cu consecințe majore la nivelul proceselor de afaceri. Auditorul are obligația de a-şi exprima rezervele cu privire la nivelul de securitate în cazul în care observă asemenea compromisuri.

O asemenea lipsă de grijă se poate dovedi nefastă pentru organizație şi extrem de costisitoare la nivel legal, atât din punct de vedere al securității, cât şi din punct de vedere al conformității. În prezent, în Uniunea Europeană este în vigoare un pachet de reglementări detaliate, care include:

- Directiva 1999/93/CE privind un cadru comunitar pentru semnăturile electronice;
- Directiva 2000/31/CE privind comerțul electronic;
- Directiva 97/7/CE privind protecția consumatorilor în cazul contractelor la distanță;
- Directiva 2002/65/CE privind comercializarea la distanță a serviciilor financiare de consum;
- Directiva 2002/58/CE privind procesarea datelor personale şi protejarea confidențialității în sectorul

comunicațiilor publice (Directiva asupra confidențialității şi comunicațiilor electronice).

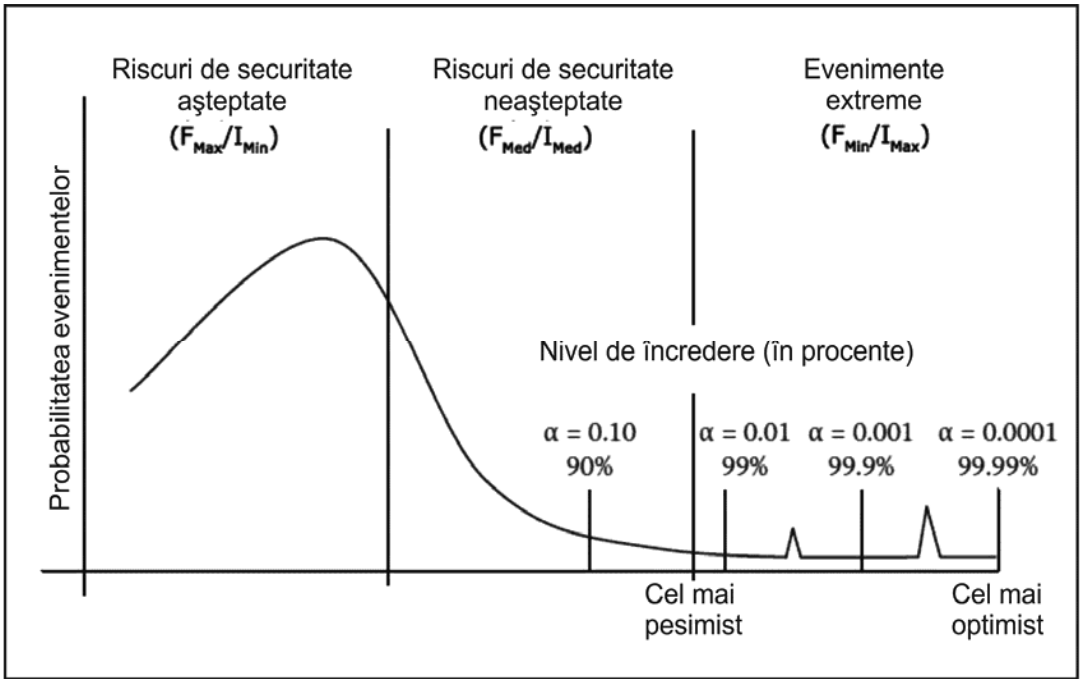
În plus, atât furnizorii, cât şi beneficiarii de servicii bazate pe cloud trebuie să aibă în vedere natura globală a acestei tehnologii, şi faptul că numeroase state solicită, prin legislația proprie, păstrarea datelor cu caracter personal şi a materialelor grevate de drepturi de autor între granițele proprii.

Fundamentul legal al relațiilor dintre furnizorii şi beneficiarii de servicii bazate pe cloud este reprezentat de contractele de tip *SLA* (*Service Level Agreement*), care, în numeroase cazuri, se limitează la a defini obligațiile de securitate în termeni destul de generali, fără a defini explicit standardele, protocoalele şi procedurile ce trebuie utilizate la nivelul calculatoarelor cu rol de client, serverelor, routerelor, echipamentelor de tip hub şi bridge, concentratoarelor de conexiuni şi al echipamentelor firewall care implementează propriu-zis sistemul de securitate. Acest lucru nu poate fi decât nociv în condițiile în care, la nivel declarativ, securitatea este un element-cheie pentru diferențierea în raport cu competiția şi un indicator-cheie de performanță, atât pentru furnizorii, cât şi pentru beneficiarii de servicii informatice bazate pe cloud. În momentul în care contractele de tip *SLA* vor include clauze inatacabile privind responsabilitățile de securitate, acestea vor conduce la obținerea de arhitecturi mai sigure, care includ elemente solide şi auditabile de securitate, încă din etapele de analiză şi proiectare.

4. Propunere de model pentru prioritizarea securității

Ca răspuns la toate problemele menționate anterior, autorul propune realizarea unui model care să permită unui furnizor sau unui beneficiar de servicii informatice bazate pe cloud stabilirea adevăratelor priorități în domeniul securității. Prima etapă a acestui model presupune identificarea, analiza şi evaluarea vulnerabilităților aferente soluției cloud alese. Există şanse foarte mari ca acest proces să genereze o listă extrem de lungă de vulnerabilități şi posibile amenințări, dar nu toate vor constitui priorități majore la nivelul organizației.

Figura 2. Modelul de determinare a impactului vulnerabilităților



Sursa: Mangiuc, 2016.

Criteriul determinant pentru prioritatea unei amenințări de securitate ar trebui să fie următorul: o vulnerabilitate prezintă risc ridicat de securitate, dacă exploatarea sa poate expune sau compromite un element de proprietate intelectuală al companiei. Mai mult, aceste amenințări considerate prioritare trebuie verificate încrucişat cu toate celelalte vulnerabilități, pentru a identifica combinațiile cu efecte distructive maxime. În timp ce frecvența unei anumite vulnerabilități se poate determina statistic, pe bază de date proprii sau de date externe relevante, procedeul de mai sus poate fi utilizat pentru a determina impactul unei vulnerabilități (**Figura 2**).

Preluând şi adaptând abordarea specifică studiului riscului operațional, se vor urmări:

- Evenimente cu frecvență mare şi impact redus (F_{Max}/I_{Min}) – pentru care se pot utiliza, cel puțin temporar, metodele de protecție deja existente, până în momentul finalizării procesului de proiectare a unei politici de securitate coerente.
- Evenimente cu frecvență medie şi impact mediu (F_{Med}/I_{Med}) – numite şi *known unknowns*, pentru care se vor crea şi analiza diferite scenarii capabile de a le proiecta posibilele efecte la nivelul infrastructurii bazate pe cloud.
- Evenimente cu frecvență redusă şi impact major (F_{Min}/I_{Max}) – numite şi *unknown unknowns*, pentru care este necesară proiectarea atentă a unor elemente dedicate în cadrul strategiei de securitate.

Pornind de la premisa existenței unui minim de instrumente de audit la nivelul sistemului informatic, un proces permanent de eşantionare poate indica deviațiile de la utilizarea curentă a sistemului (încărcare neobişnuită, număr mare de cereri din aceeaşi sursă etc.). Nivelul de încredere pentru evenimentele de tip F_{Min}/I_{Max} trebuie să fie de cel puțin 99,99%, ceea ce înseamnă că cel mult un caz din zece mii poate scăpa atenției celor care monitorizează sistemul. Un asemenea deziderat nu poate fi atins instantaneu, ci numai după un interval rezonabil de timp, prin analize repetate şi acumularea de experiență.

Modul de acțiune propus în prezenta lucrare se bazează şi pe o serie de practici din industria bancară, destinate identificării şi monitorizării riscului operațional, aşa cum este cerut de către *Basel Comitee on Banking Supervision* (Chorafas, 2004).

Tipul de analiză propus anterior asigură capacitatea auditorului de a descoperi vulnerabilități, precum şi pe cea de a stabili prioritățile. Nicio companie, indiferent de dimensiuni, nu îşi poate permite să urmărească toate vulnerabilitățile simultan, ci trebuie să se concentreze mai întâi pe cele cu risc ridicat de impact, indiferent cât de redusă pare posibilitatea lor de apariție. Această abordare, care poate fi numită *proiectarea unei politici de securitate*, ar trebui centrată pe alegerea celor mai eficiente economic contra-măsuri pentru reducerea expunerii la vulnerabilități:

- creşterea semnificativă a costului atacului pentru un eventual atacator;
- diminuarea pagubelor ce pot fi provocate printr-un atac, prin stabilirea de proceduri de control intern mai complexe şi cu grad mai mare de integritate;
- creşterea probabilității ca atacul să fie detectat şi oprit înainte de a-şi atinge scopul.

Propunerea de mai sus constituie doar o sugestie privind direcțiile de acțiune, întrucât pentru eficiență maximă este necesară îmbogățirea acesteia cu o serie de variabile de natură culturală şi comportamentală, care nu pot fi predefinite, ci trebuie evaluate în fiecare caz particular (de exemplu, nivelul de pregătire al angajaților, nivelul de înțelegere şi de acceptare a noilor măsuri de securitate, gravitatea pedepselor prevăzute în normele legale pentru respectivele infracțiuni).

De asemenea, se impune proiectarea unei arhitecturi de securitate distribuite, capabile de a căuta, captura şi analiza modelele de comportament de la nivelul rețelei. Această abordare este mult mai eficientă decât cea centralizată (Pinzon ş.a., 2011), deoarece este mai sensibilă la modelele locale de comportament din rețea şi, în plus, încarcă mai puțin echipamentele din cadrul rețelei. O asemenea arhitectură de securitate trebuie să fie capabilă de a culege datele şi probele necesare în cazul documentării unui eveniment de securitate, pentru a servi auditului intern, unui contract de asigurare, sau unei instanțe judecătoreşti. Studiile arată că unul din impedimentele principale întâmpinate de companiile din Uniunea Europeană atunci când doresc instrumentarea legală a acțiunii în cazul unui atac informatic este de a demonstra că acesta a avut loc (Munoz-Canavate şi Hipola, 2011). Detectarea şi identificarea anomaliilor

alertează administratorii cu privire la acele evenimente sau conexiuni care nu au apărut până atunci, sau, dacă au mai apărut, nu au intrat în atenția sistemelor de alertare. Utilizarea tehnologiilor specifice inteligenței artificiale (rețele neuronale, rețele bazate pe agenți, identificarea de evenimente) pot accelera semnificativ procesul de implementare a unui sistem de securitate corect proiectat. Asemenea tehnologii au şi capacitatea de a reduce numărul de alarme false, a căror apariție este inevitabilă, indiferent dacă este vorba de un sistem predominant automat sau de unul predominant manual.

Concluzii

Prezentul articol a identificat principalele tipuri de amenințări de securitate care grevează o soluție informatică bazată pe cloud, atât din categoria celor „moştenite" de la generațiile anterioare de soluții informatice, cât şi din categoria celor apărute ca urmare a fundamentării sistemului informatic pe conexiunea Internet.

Deşi constituirea unei autorități dedicate normalizării şi verificării modului de aplicare a normelor de securitate în cloud a fost cerută de numeroase voci din mediul economic şi din cel academic, ideea nu a fost luată în considerare de factorii de decizie, ceea ce conduce la concluzia că, din punctul de vedere al unui auditor, potențialul de fraudă al infrastructurii bazate pe cloud, perceput ca atare de către o mare parte a companiilor-utilizatori are două cauze majore:

- Absența unor practici standardizate de securitate a căror implementare să fie obligatorie pentru furnizorii şi beneficiarii de servicii cloud (şi verificabilă direct prin Internet).
- Ambiguitatea şi incertitudinea existentă din punct de vedere legal cu privire la modul de aplicare şi aria de acoperire a cadrului legislativ existent în domeniul afacerilor on-line.

Riscul de a răspunde legal pentru modul în care a fost gestionată informația în cloud va aparține aceluia care este proprietarul de drept al informației, iar consecințele pot deveni repede extrem de serioase în cazul unui management defectuos al securității. După cum şi-a propus să evidențieze şi lucrarea de față, capacitatea de a asigura un nivel rezonabil de protecție a datelor în cloud este cel puțin discutabilă în prezent şi probabil va rămâne aşa atât timp cât creşterea complexității infrastructurii cloud va lăsa în urmă creşterea eficienței mecanismelor de securitate.

Ca urmare, lucrarea propune o schiță de model pentru identificarea şi prioritizarea amenințărilor de securitate din cadrul unei infrastructuri bazate pe cloud, inspirat din modelul de estimare a riscului operațional, şi care poate fi utilizat pentru descrierea direcțiilor cele mai importante de dezvoltare a politicilor de securitate.

Se poate concluziona că proiectarea unei soluții de securitate absolută este o utopie. Totuşi, acest lucru nu trebuie să fie descurajant, întrucât recursul la cele mai bune tehnologii disponibile, precum şi utilizarea unor tehnici imaginative de protecție împotriva amenințărilor de securitate specifice rețelei Internet şi paradigmei bazate pe cloud poate creşte eficiența şi impactul soluțiilor de securitate propuse.

BIBLIOGRAFIE

1. Bajpai, D., Vardhan, M. şi Kushwaha, D.S. (2012), Authentication and Authorization Interface Using Security Service Level Agreements for Accessing Cloud Services, *Contemporary computing, Book Series: Communications in Computer and Information Science*, vol. 306, nr.1, pp. 370-382.
2. Berriman, B., Deelman, E., Juve, G., Rynge, M. şi Voeckler, J.S. (2012), High-Performance Compute Infrastructure in Astronomy: 2020 Is Only Months Away, *Astronomical Data Analysis Software and Systems XXI Book Series: Astronomical Society of the Pacific Conference Series*, vol. 461, nr. 1, pp. 91-94.
3. Carlsson, C. şi Fuller, R. (2013), Probabilistic Versus Possibilistic Risk Assessment Models for Optimal Service Level Agreements in Grid Computing, *Information Systems and E-Business Management*, vol. 11, nr. 1, pp. 13-28.
4. Chorafas, D.N. (2004), *Operational Risk Control with Basle II. Basic Principles and Capital Requirements*, Butterworth-Heinemann, London.
5. Directiva 1999/93/CE a Parlamentului European şi a Consiliului din 13 decembrie 1999 privind un cadru comunitar pentru semnăturile electronice.

6. Directiva 2002/58/CE a Parlamentului European şi a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale şi protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității şi comunicațiilor electronice).
7. Directiva 2002/65/CE a Parlamentului European şi a Consiliului din 23 septembrie 2002 privind comercializarea la distanță a serviciilor financiare de consum şi de modificare a Directivei 90/619/CEE a Consiliului şi a Directivelor 97/7/CE şi 98/27/CE.
8. Directiva 97/7/EC a Parlamentului European şi a Consiliului din 20 mai 1997 privind protecția consumatorilor cu privire la contractele la distanță.
9. Edwards, C. (2014), Ending identity theft and cyber-crime, *Biometric Technology Today*, vol. 2014, nr. 2, pp. 9-11.
10. Han, J., Susilo, W. şi Mu, Y. (2013), Identity-based data storage in cloud computing, *Future Generation Computer Systems – The International Journal of Grid Computing and E-Science*, vol. 29, nr. 3, pp. 673-681.
11. Li, M., Yu, S., Zheng, Y., Ren, K. şi Lou, W. (2013) "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, nr. 1, pp. 131-143.
12. Mangiuc, D. (2012), Cloud Identity and Access Management – A Model Proposal, *Journal of Accounting and Management Information Systems*, vol. 11, nr. 3, pp. 484-500.
13. Munoz-Canavate, A. şi Hipola, P. (2011), Electronic administration in Spain: From its beginnings to the present, *Government Information Quarterly*, vol. 28, nr. 1, pp. 74-90.
14. Nunes, P.F. şi Merrihue, J. (2007), The continuing power of mass advertising, *MIT Sloan Management Review*, vol. 48, nr. 2, pp. 63-77.
15. Perez-Mendez, A., Pereniguez-Garcia, F., Marin-Lopez, R. şi Lopez-Millan, G. (2012), A cross-layer SSO solution for federating access to kerberized services in the eduroam/DAMe network, *International Journal of Information Security*, vol. 11, nr. 6, pp. 365-388.
16. Pervez, Z., Awan, A.A., Khattak, A.M., Lee, S. şi Huh, E.N. (2013), Privacy-aware searching with oblivious term matching for cloud storage, *Journal of Supercomputing*, vol. 63, nr. 2, pp. 538-560.
17. Pinzon, C.I., Bajo, J., De Paz, J.F. şi Corchado, J.M. (2011), S-MAS: An adaptive hierarchical distributed multi-agent architecture for blocking malicious SOAP messages within Web Services environments, *Expert Systems with Applications*, vol. 38, nr. 5, pp. 5486-5499.
18. Purpura, P.P. (2013), *Security and Loss Prevention – An Introduction (Sixth Edition)*, Butterworth-Heinemann, London.
19. Reed, B. (2012), The 8-Year Effort to Address Systems-Level Space Solar Power Issues for Us Government Satellite Programs, *2012 38th IEEE Photovoltaic Specialists Conference*, vol. 38, nr. 1, pp. 2811-2814.
20. Ren, K., Wang, C. şi Wang, Q. (2012), Toward Secure and Effective Data Utilization in Public Cloud, *IEEE Network*, vol. 26, nr. 6, pp. 69-74.
21. US Department of Justice, Office of Public Affairs (2009), Alleged International Hacker Indicted for Massive Attack on U.S. Retail and Banking Networks. Data Related to More Than 130 Million Credit and Debit Cards Allegedly Stolen, Disponibil la http://www.justice.gov/opa/pr/2009/August/09-crm-810.html [Accesat pe 10 februarie 2016].
22. US House of Representatives, Committee on Homeland Security, Subcommittee on Oversight, Investigations, and Management (2012), America Is under Cyber Attack: Why Urgent Action Is Needed", Disponibil la *http://www.hsdl.org/? view&did=707644* [Accesat pe 10 februarie 2016].