Audit financiar, XVI, Nr. 1(149)/**2018**, *44-53*
ISSN: 1583-5812; ISSN on-line: 1844-8801

Provocări în domeniul securității informației – vulnerabilități aduse de aplicațiile ERP şi platformele cloud

Sînziana-Maria RÎNDAŞU,
Academia de Studii Economice din Bucureşti,
E-mail: sinziana_rindasu@yahoo.com

:

Rezumat

Profesia contabilă este într-un proces continuu de schimbare, datorită faptului că aplicațiile ERP şi tehnologiile emergente precum cloud computing continuă să aducă îmbunătățiri activităților financiar-contabile. Cu toate acestea, observăm că pe lângă varietatea de beneficii, aceste tehnologii prezintă riscuri specifice, care pot afecta caracteristicile fundamentale şi de securitate a datelor.

Prezenta lucrare are scopul de a evidenția cele mai întâlnite vulnerabilități ale aplicațiilor ERP şi ale platformelor cloud computing, în contextul contabilității digitale. Totodată, pe lângă aspectele tehnice şi bunele practici de prevenție şi corecție a acestor vulnerabilități, studiul se axează pe o componentă cheie a securității datelor: factorul uman. Cercetarea empirică realizată scoate în evidență faptul că tinerii profesionişti înțeleg necesitatea de protecție a datelor sensibile, însă nu întotdeauna manifestă cel mai corect comportament pentru a preveni incidentele de securitate.

Acest articol are rolul de a oferi o privire de ansamblu asupra aplicațiilor ERP şi a platformelor cloud computing, utilizate în prezent în domeniul financiar-contabil, axându-se pe principalele vulnerabilități şi pe factorul uman, care reprezintă unul dintre cele mai importante aspecte ale securității datelor.

Cuvinte-cheie: *Securitatea informației, ERP, cloud computing, factorul uman.*

Clasificare JEL: *M15, M41, M42.*

Vă rugăm să citați acest articol astfel:
Rîndaşu, S.M. (2018), Information security challenges – vulnerabilities brought by ERP applications and cloud platforms, *Audit Financiar*, vol. XVI, nr. 1(149)/2018, pp. 131-139, DOI: 10.20869/AUDITF/2018/149/005

Link permanent pentru acest document:
http://dx.doi.org/10.20869/AUDITF/2018/149/005
Data primirii articolului: 27.06.2017
Data revizuirii: 02.08.2017
Data acceptării: 08.11.2017

Introducere

Evoluția continuă a tehnologiilor informatice a contribuit la dezvoltarea majorității industriilor, dar şi a profesiilor, prin automatizarea şi robotizarea anumitor activități elementare, cu scopul de a permite profesioniştilor să se axeze pe activități mai complexe, dar care creează un plus de valoare companiilor. Digitalizarea şi robotizarea proceselor nu sunt destinate să înlocuiască resursa umană, ci mai degrabă să susțină progresul profesional al indivizilor.

Informația reprezintă esența oricărei organizații sau individ, este ceea ce creează un avantaj competitiv, iar aşa cum Ronald Reagan afirma, reprezintă: „oxigenul epocii moderne". În domeniul financiar-contabil aproape totul se rezumă la informație. În acest sens, ACCA (2013a) susține ideea că, în actuala era digitală informația a devenit una din resursele vitale în procesul de creare a valorii. Protejarea datelor sensibile, fie că ne referim la date stocate pe suport fizic sau electronic, prin implementarea unui sistem eficient de management al incidentelor de securitate informatică, trebuie să constituie o preocupare esențială pentru orice organizație, indiferent de mărime sau domeniu de activitate. Expunerea accidentală sau intenționată a informațiilor confidențiale poate afecta iremediabil activitatea companiilor, atât din punct de vedere financiar, cât şi reputațional.

În prezent, incidentele de securitate reprezintă una din cele mai importante preocupări în era internetului pentru orice IoE (en. Internet of Everything), datorită faptului că evoluția tehnologică a introdus în domeniul financiar-contabil noi concepte precum: sisteme ERP, cloud computing şi tehnologii mobile care prezintă, pe lângă varietatea de avantaje, vulnerabilități specifice care amenință securitatea informațiilor sensibile. În ultimii ani s-a observat o creştere a incidentelor de securitate, atât pe plan național, cât şi la nivel global. Conform ultimului raport emis de CERT (2016), în România, în anul 2016, s-au înregistrat peste 110 milioane de alerte de securitate cibernetică, creşterea față de anul anterior fiind de peste 60%. La nivel global, conform statisticii emise de Breach Level Index, s-au petrecut peste 1,3 miliarde de incidente de securitate informatică, creşterea fiind de peste 85%, comparativ cu anul 2015.

În domeniul financiar-contabil majoritatea activităților a fost digitalizată datorită nevoii de a avea access continuu la informațiile relevante, în timp real. Fie că vorbim de tehnologii mobile, sisteme ERP sau platforme cloud computing, aproape toate informațiile sensibile s-au mutat în mediul electronic. Obiectivul acestei lucrări este de a analiza principalele provocări privind securitatea informației în contextul contabilității digitale, care sunt vulnerabilitățile tehnologiilor utilizate în prezent, precum şi efectuarea unei investigații privind percepția şi nivelul de conştientizare a impactului incidentelor de securitate, din perspectiva viitorilor profesionişti contabili.

1. Analiza literaturii de specialitate – vulnerabilitățile aplicațiilor ERP şi ale platformelor cloud computing

Dezvoltarea sistemelor de planificare a resurselor întreprinderii ERP (*en.* Enterprise Resource Planning) a avut ca punct de plecare necesitatea de automatizare a activităților elementare de procesare şi introducere a datelor, care nu necesitau aplicarea unui raționament variabil. Deşi digitalizarea şi robotizarea anumitor procese precum: gestiunea stocurilor obținute şi a materialelor necesare în activitatea de producție a început în anii '50, de abia la începutului anilor '90 putem identifica primul sistem ERP (Møller, 2005), care încorpora diferite module: contabilitate, resurse umane, managementul proiectelor şi distribuției. Actualmente, sistemele disponibile încorporează aceleaşi funcții de bază, care sunt însă configurate în funcție de necesitățile fiecărei organizații. Majoritatea aplicațiilor actuale includ şi module de planificare financiară, gestionarea lanțului de aprovizionare (SCM - supply-chain management) şi a relațiilor cu clienții (CRM - customer relations management).

Conform literaturii de specialitate, impactul adus de apariția sistemelor ERP a fost pozitiv datorită faptului că aceste aplicații aveau la bază ideea de a cumula majoritatea proceselor cheie dintr-o companie, într-un singur sistem IT (Klaus, 2000), folosind o bază de date comună cu scopul de a elimina procesele redundante (Davenport, 1998). În domeniul financiar-contabil principalele avantaje s-au bazat pe: reducerea costurilor, eliminarea sau automatizarea proceselor elementare, creşterea calității raportărilor financiare şi îmbunătățirea flexibilității şi a competitivității (Kanellou şi Spathis, 2013; Stanciu şi Tinca, 2013; Ponorîcă ş.a., 2014, Voulgaris ş.a., 2014).

În ultima perioadă sistemele ERP au început să se adapteze nevoilor curente ale utilizatorilor. Prin urmare, putem aduce în discuție utilizarea aplicațiilor de tipul ERP într-o platformă cloud computing care să permită accesarea datelor de pe dispozitive mobile. Observăm aici tendința generală de migrare în cloud pentru a putea beneficia de acces continuu la date, fără a mai ține cont de barierele tehnologice sau geografice.

Aplicațiile ERP reprezintă o țintă a atacurilor cibernetice din cauza faptului că stochează informații confidențiale precum secrete organizaționale, informații financiare, date despre clienții şi furnizorii organizației, dar şi pentru a comite diverse acte de fraudă, prin modificarea malițioasă a datelor clienților sau furnizorilor (*en*. master data).

Pentru a analiza problematica vulnerabilităților aplicațiilor ERP, din punct de vedere al securității datelor stocate de sisteme, trebuie să înțelegem arhitectura şi modul de funcționare a acestora. Majoritatea aplicațiilor ERP au în comun cele trei niveluri. Începând cu baza oricărui ERP se află o bază de date în care toate informațiile sunt stocate, aspect ce îl putem regăsi în majoritatea aplicațiilor baze de date Microsoft sau Oracle care au ca limbaj de interogare SQL. Următoarea componentă este nivelul aplicației unde regăsim partea de implementare a modulelor aplicației, logica şi regulile sistemului, iar ultimul nivel al ERP-urilor îl reprezintă interfața aplicației pentru utilizator (Surjit ş.a., 2016; Bahssas, 2015). Totodată, în afară de arhitectura simplificată a unei aplicații ERP este important şi mediul în care această aplicație este implementată: local sau pe o platformă de tipul cloud computing.

Luând în considerare structura prezentată, prima vulnerabilitate a unui sistem ERP este dată de existența bazei de date utilizată. La nivelul bazei de date există posibilitatea să apară neconcordanțe care pot periclita caracteristicile fundamentale ale datelor: confidențialitatea, integritatea şi disponibilitatea, în cazul în care baza de date nu a fost implementată corespunzător (Bertino, 2005; Swart ş.a., 2007).

Printre potențialele vulnerabilități putem enumera: privilegii excesive sau neautorizate, vulnerabilități ale sistemului de operare pe care rulează baza de date, injecții SQL, malware, parole necorespunzătoare sau implementarea necorespunzătoare a bazei de date (Ali şi Afzal, 2017; Malik şi Patel, 2016; Lodha şi Dhande, 2014). Toate aceste vulnerabilități apar atât în cazul aplicațiilor ERP locale, dar şi în cazul în care aplicația ERP este pe o platformă cloud. Din punct de vedere al nivelului de securitate dintre un ERP local sau un ERP în cloud, nu putem spune că securitatea va fi sau nu îmbunătățită, deoarece totul depinde de modul de implementare şi de controalele create.

Analizând următorul nivel al aplicațiilor de tipul ERP, nivelul logic, la fel ca în cazul bazei de date din spatele aplicației ERP, în cazul în care implementarea nu s-a efectuat corespunzător apare problematica securității datelor, prin atacuri de tipul *brute force* sau *injecții SQL*. În cadrul acestui nivel, majoritatea problemelor apar din cauza implementării ineficiente a securității bazei de date.

Utilizatorii aplicațiilor ERP reprezintă, de asemenea, o vulnerabilitate pentru datele sensibile (Evans ş.a., 2016), deoarece organizațiile nu creează o cultură eficientă pentru a-i face conştienți de importanța unui posibil furt/afectare sau expunere de informații confidențiale. Factorul uman reprezintă unul din cele mai importante componente pentru un nivel eficient de securitate a datelor, indiferent dacă discutăm sau nu despre o aplicație ERP. Este esențial ca organizațiile să instruiască angajații asupra impactului unui incident de securitate.

În anul 2014 o parte din directorii Sony Pictures Entertainment au primit un e-mail, aparent de la Apple, pentru o verificare a adresei de e-mail. E-mailul primit de către aceştia a fost în realitate un phising, care a permis atacatorilor să obțină parola de la conturile de Apple, credențiale care au fost mai apoi folosite pentru a se autentifica în rețeaua Sony şi au furat informații financiare confidențiale şi parole ale servelor Sony, care au fost ulterior postate pe Internet. Conform declarațiilor directorului companiei, costurile de refacere a sistemelor IT s-au ridicat la 35 de milioane de dolari. Acest incident reprezintă un exemplu clasic care demonstrează că factorul uman reprezintă în continuare una din cele mai importante vulnerabilități. Totodată, faptul că directorii care au fost ținta atacului au avut aceleaşi parole pentru conturile corporației cu cele personale, indică faptul că nu există încă o cultură bine dezvoltată de prevenție a riscurilor asociate expunerii neautorizate a datelor sensibile.

După cum se poate observa şi din exemplul prezentat anterior, prevenția pierderii informațiilor sensibile este esențială, în special în cazul sistemelor ERP, care, conform statisticilor, sunt utilizate de peste 83% din companiile 500 Forbes. Pentru a preveni incidentele de securitate trebuie mai întâi identificate riscurile şi evaluat potențialul impact.

Având în vedere faptul că fiecare companie are propriile particularități, fiecare aplicație ERP va prezenta diferențe, în funcție de nevoile organizațiilor şi activitățile specifice. Prin urmare, nu putem vorbi despre un model universal de securitate a ERP-urilor, ci doar ne putem rezuma la prezentarea celor mai bune practici, care au rolul de a preveni incidentele de securitate.

Aşa cum a fost menționat anterior, una din principalele probleme de securitate este reprezentată de privilegiile excesive acordate utilizatorilor aplicațiilor (Horwath, 2012). Administratorii bazelor de date alocă drepturi diferențiate utilizatorilor, fie utilizând rolurile existente în aplicație, fie creând noi roluri care să se potrivească adecvat nevoilor de acces ale utilizatorilor în aplicație (Bruchez, 2012). Aceste roluri personalizate ar putea preveni accesul neautorizat la date, dar doar în cazul în care sunt implementate corespunzător.

Configurarea necorespunzătoare a bazei de date constituie, de asemenea, o vulnerabilitate extrem de importantă. În stocarea parolelor de acces în baza de date a aplicației ERP, fără ca datele să fie criptate, conferă potențialilor atacatori posibilitatea de a obține credențialele utilizatorilor. În cazul bazelor de date SQLServer există posibilitatea ca datele de autentificare ale utilizatorilor să fie stocate într-o altă bază de date şi să fie criptate, nefiind vizibile nici măcar administratorului bazei de date. De asemenea, o implementare care nu ține cont de vulnerabilitățile unei asemenea aplicații, poate să permită atacatorilor furtul de date utilizând injecții SQL (Bhatia, 2017), care reprezintă în continuare unul din cele mai semnificative puncte slabe ale bazelor de date.

În cazul infectării serverului cu programe malițioase, de tipul malware, există riscul pierderii sau furtului informațiilor sensibile ale organizației. În ultima perioadă putem observa apariția a tot mai multor tipuri de viruşi care pot rămâne nedetectați sau al căror impact să fie observat numai după o perioadă semnificativă de timp. Mai nou, putem observa aplicații precum ransomware al căror scop este să cripteze toate datele utilizatorilor, iar decriptarea se va face numai după ce atacatorii sunt plătiți să decripteze informațiile. În prezent se dezvoltă programe care pot preveni astfel de incidente (Kolodenke ş.a., 2017), dar evoluția programelor malware este mai acerbă decât cea de dezvoltare a programelor de prevenție.

Majoritatea bazelor de date încorporează module de auditare a bazei de date, care pot preveni expunerea informațiilor confidențiale, dacă se bazează pe controale eficiente, care au drept țintă zonele de risc ale aplicației. Auditarea bazei de date are rolul de prevenție prin determinarea vulnerabilităților, dar şi rol de detecție. În cazul bazelor de date, cele mai eficiente controale în cadrul unui audit sunt:

- analiza activităților de back-up sau de restaurare a bazelor de date – are rolul de a determina ce utilizatori au efectuat astfel de activități. Aşa cum am prezentat anterior, una din cele mai mari vulnerabilități într-o aplicație ERP o constituie privilegiile excesive acordate utilizatorilor, iar în cazul în care rezultatele acestui control arată că asemenea activități au fost efectuate de persoane care nu ar fi trebuit să aibă drepturi să efectueze acest tip de operațiuni, acest aspect trebuie să reprezinte un semnal de alarmă pentru organizație.
- analiza acțiunilor efectuate asupra bazei de date sau obiectelor acesteia – la fel ca în cazul controlului anterior, acest control are rol de monitorizare şi de detecție a activităților ilegale. Totuşi, având în vedere faptul că într-o aplicație ERP sunt mai mulți utilizatori care aduc schimbări constant bazei de date, iar în acest caz volumul de informații este suficient de mare pentru a fi analizat manual, se recomandă utilizarea tehnicilor de data mining pentru a identifica posibilele neconcordanțe.
- analiza logărilor în sistem – acest control este important deoarece monitorizează atât accesul utilizatorilor în aplicație, dar trebuie să ia în considerare şi activitățile de logare eşuate. Acest control poate preveni un atac de tipul brute-force, dar şi să evidențieze logări în sistem efectuate de foştii angajați ai organizației, ale căror credențiale nu au fost încă blocate, fiind omisă blocarea conturilor de utilizator.

Sistemele ERP reprezintă componente vitale ale oricărei organizații, deoarece înglobează cele mai importante procese ale companiei, iar, prin urmare, implementarea corectă, respectând bunele practici, este necesară pentru a preveni potențialele incidente de securitate. Din cauza complexității sistemelor ERP nu putem vorbi despre un referențial comun de securitate, care să răspundă necesităților tuturor companiilor, prin urmare, cea mai eficientă metodă de protecție a datelor sensibile în cazul aplicațiilor ERP este identificarea corectă a riscurilor, utilizând cele mai bune practici.

Contextul economic actual a creat necesitatea de a avea acces continuu la informații. Această nouă necesitate, în domeniul financiar o întâlnim sub denumirea de raportare în timp real, proces care creează un avantaj competitiv organizațiilor (ACCA, 2013b), prin îmbunătățirea agilității şi transparenței activităților. Pentru a putea satisface această necesitate a utilizatorilor şi a companiilor, majoritatea proceselor contabile şi financiare au migrat către platformele de cloud computing (Trigo ş.a., 2014). În acest fel, utilizatorii unei anumite aplicații pot vizualiza sau manipula datele indiferent de locație sau de dispozitivele utilizate, atâta timp cât au o conexiune la internet.

La fel ca în cazul aplicațiilor ERP, pentru a înțelege principalele vulnerabilități referitoare la securitatea datelor stocate pe platforme de tipul cloud computing, trebuie să avem o imagine clară asupra funcționalității şi arhitecturii platformelor.

Conceptul de cloud computing a avut la bază ideea accesului nelimitat, de tehnologie (elemente hardware), la informații, conform Giordanelli şi Mastroianni (2010). În prezent, conceptul de cloud computing este reprezentat de o rețea de servere şi un depozit de date (Kim, 2013), al căror scop este de a furniza o gamă variată de servicii web (stocarea şi manipularea datelor, efectuarea de interogări asupra bazei de date etc.).

Din punct de vedere al modului de livrare al serviciilor furnizate, distingem trei tipuri de platforme: IaaS – infrastructură ca serviciu, PaaS - platformă ca serviciu şi SaaS - software ca serviciu, conform standardului NIST 800-145.

O a doua clasificare se poate realiza în funcție de modelul de implementare folosit: public, privat, comunitate sau hibrid. Din punct de vedere al securității acestor modele, cel mai scăzut nivel de securitate se regăseşte în modelul public, fiind apoi urmat de comunitate, modelul hibrid şi privat.

IaaS încorporează toate funcționalitățile unui cloud, deoarece utilizatorii au dreptul de a modifica funcționalitățile şi aspectele privind securitatea aplicațiilor. Totodată, acest tip de platformă permite organizațiilor să aibă cel mai mare nivel de control asupra infrastructurii IT, comparativ cu celelalte două tipuri de platforme. Datorită acestor considerente, în cazul IaaS securitatea sistemelor de operare şi a aplicațiilor revine organizației, în timp ce furnizorul de cloud este responsabil doar cu securitatea rețelei şi a serverelor.

Conform studiului efectuat de Symantec în 2015, cele mai frecvente vulnerabilități în IaaS sunt: pierderea sau expunerea informațiilor confidențiale, accesul neautorizat – în principiu datorită furtului credențialelor utilizatorilor şi configurarea necorespunzătoare din punct de vedere al securității. Totodată, în cazul IaaS pot apărea probleme de securitate şi datorită celorlalți utilizatori de cloud (chiriaşi), atunci când serverul nu este dedicat.

Pentru a putea preveni incidentele de securitate, în cazul acestui tip de platformă, este foarte important să alegem cel mai adecvat model (public, privat, comunitate, hibrid), care să se plieze pe obiectivele organizației şi să ne asigurăm că implementarea s-a făcut corespunzător, respectând cele mai bune practici de securitate a datelor. Totodată, monitorizarea şi auditul sistemelor reprezintă procese vitale în prevenirea atacurilor cibernetice sau expunerii neintenționate a informațiilor confidențiale. De asemenea, pentru a îmbunătăți securitatea credențialelor este recomandată utilizarea a doi sau mai mulți factori de autentificare (Jaiswal şi Rohankar, 2014).

Modelul PaaS nu oferă organizațiilor aceeaşi libertate ca şi modelul IaaS, fiind creat pentru a permite dezvoltarea de aplicații de către organizație. În cadrul acestui model, compania care a închiriat platforma nu poate aduce modificări rețelei, serverelor sau sistemelor de operare. În PaaS furnizorul de cloud este responsabil de securitatea bazelor de date şi a rețelei, pe când chiriaşul răspunde pentru securitatea aplicațiilor dezvoltate pe această platformă.

Din punct de vedere al securității sistemului, majoritatea platformelor PaaS oferă instrumente precum: verificarea integrității, criptarea datelor, managementul acceselor şi firewall-uri (CSCC, 2015). Cu toate acestea, şi în acest nivel, regăsim vulnerabilități care pot afecta caracteristicile fundamentele ale datelor, în cazul în care dezvoltarea aplicațiilor nu se realizează în conformitate cu cele mai bune practici de menținere a securității datelor. De asemenea, trebuie implementate şi pentru acest tip de platformă controale eficiente, care să prevină potențialele incidente de securitate.

Cel de-al treilea model de platformă este reprezentat de SaaS, care este cel mai răspândit tip de cloud, întrucât are cele mai scăzute costuri, comparativ cu ultimele două modele. Majoritatea aplicațiilor contabile, în principal aplicații de tipul ERP, sunt încorporate în acest model. În SaaS utilizatorii pot accesa aplicațiile

disponibile, dar nu pot implementa alte aplicații. De asemenea, în cadrul acestui model, majoritatea aspectelor de securitate a datelor sunt atribuite furnizorului de cloud.

Potențialele vulnerabilități în modelul SaaS, identificate prin analiza literaturii de specialitate, sunt: privilegii excesive, accesul neautorizat, configurări necorespunzătoare ale aplicațiilor care pot afecta caracteristicile fundamentale ale datelor şi aspecte legate de securitatea maşinii virtuale (Hussein şi Khalid, 2016; Ahmed ş.a., 2017; Sharma ş.a., 2017).

Deoarece acest model este mai restrictiv din punct de vedere al implementării de aplicații de către client şi, totodată, din cauza faptului că nevoile fiecărei organizații prezintă particularități specifice, majoritatea controalelor privind securitatea datelor este responsabilitatea furnizorului de cloud, care trebuie să furnizeze un nivel acceptabil de asigurare a securității informațiilor sensibile. Totodată, având în vedere faptul că în cloud se stochează informații variate, care presupun, în funcție de nevoia de confidențialitate, tratamente speciale reglementate de organismele naționale şi internaționale, este primordial să asigurăm pentru fiecare tip de informație nivelul adecvat de securitate.

În concluzie, platformele cloud prezintă vulnerabilități specifice, în funcție de fiecare model în parte. La fel ca şi în cazul aplicațiilor ERP, nu putem vorbi despre un model absolut de securitate, care ar avea capacitatea de a preveni orice fel de incident, însă este necesar să înțelegem modul în care datele stocate în platformele cloud computing pot genera riscuri care au potențialul de a genera un incident de securitate.

Datorită multiplelor avantaje aduse de către cloud computing, tot mai multe companii iau în calcul migrarea către o platformă cloud, pentru a-şi îmbunătăți performanțele şi pentru a deveni mai competitivi. Având în vedere faptul că această tehnologie este emergentă, este de aşteptat să apară noi tipuri de vulnerabilități, în special din cauza creşterii utilizărilor altor tehnologii, împreună cu platformele cloud, spre exemplu tehnologiile mobile, care au început să fie tot mai des utilizate, în special în domeniul financiar contabil. Aceste aspecte pot contribui la dezvoltarea de noi riscuri, însă este important să înțelegem faptul că migrarea în cloud nu reprezintă în mod automat o scădere a nivelului de securitate, ci în multe cazuri poate îmbunătăți securitatea comparativ cu aplicațiile locale.

2. Metodologia cercetării

În prima parte a lucrării am prezentat faptul că factorul uman este o componentă extrem de importantă în asigurarea corectă a securității datelor. Domeniul financiar-contabil este vulnerabil în fața incidentelor de securitate, deoarece stochează şi produce informații cu un nivel înalt de confidențialitate.

În ultimii ani organismele profesionale au început o diseminare internațională a impactului securității informației în domeniul contabil, cu scopul de a atrage atenția practicienilor asupra eventualelor riscuri asociate cu manipularea datelor confidențiale, în special cele utilizate în cadrul aplicațiilor informatice. Totodată, rapoartele realizate de către ACCA în 2014 şi 2016 atrag atenția asupra necesității ca profesioniştii din acest domeniu să îşi îmbunătățească şi să îşi dezvolte capacități de a proteja informațiile sensibile, în special cele asociate cu tehnologiile emergente, precum: cloud computing, Big Data şi tehnologii mobile. Studiile efectuate de ACCA au demonstrat faptul că de-a lungul timpului, la nivel internațional, s-a putut observa o creştere a nivelului de conştientizare în rândul membrilor.

Având rapoartele realizate de ACCA ca punct de referință, am realizat o cercetare empirică, având la bază un chestionar adresat studenților programului de master Contabilitate, Audit şi Informatică de Gestiune din cadrul Academiei de Studii Economice din Bucureşti, în ultimul an de studiu, pentru a analiza percepția acestora referitoare la securitatea în domeniul financiar-contabil. Scopul acestei cercetări a fost de a afla dacă viitorii profesionişti contabili şi-au însuşit suficiente cunoştințe pentru a înțelege impactul incidentelor de securitate şi dacă au o cultură suficient de bine dezvoltată în domeniul protecției datelor sensibile.

Chestionarul a fost trimis către 80 de potențiali respondenți, dintre care 49 de persoane au decis să participe, rata de răspuns fiind de 61,25%.

Chestionarul a cuprins 16 întrebări de diferite tipuri: întrebări cu unul sau mai multe răspunsuri posibile, pentru situațiile în care nu era necesar un nivel aprofundat de analiză, întrebări de tipul matrice de răspuns, scale de evaluare, dar şi întrebări deschise destinate subiectelor care necesitau o analiză mai aprofundată.

Toți studenții implicați în cercetare lucrează în domeniul financiar-contabil şi au în medie doi ani de experiență, vârsta medie a respondenților fiind de 24 de ani.

3. Rezultatele cercetării

Pentru a putea analiza nivelul de familiaritate a participanților cu conceptele referitoare la securitatea informației, aceştia au fost întrebați, dacă în timpul programelor de studiu au primit suficiente informații referitoare la securitatea datelor. La această întrebare, numai 17 participanți au considerat că nivelul de informații primit a fost suficient, pe când 27 de persoane, reprezentând 55,10% din eşantionul total au afirmat că au primit informații despre importanța securității datelor, însă consideră că nivelul de informații primit nu a fost suficient. Restul de cinci participanți au afirmat că nu au primit astfel de informații.

Variația răspunsurilor se poate justifica prin faptul că studenții au participat la programe diferite de licență. Totuşi, luând în considerare necesitatea curentă de a crea în rândul profesioniştilor din domeniul financiar-contabil o cultură bine definită de protecție a datelor sensibile şi de prevenție a incidentelor de securitate, este necesar, în opinia noastră, ca universitățile să introducă în programă cursuri care să se axeze pe acest domeniu, pentru a face mai uşoară integrarea absolvenților în profesie.

Următoarea întrebare a chestionarului a fost de tipul matrice de răspuns, iar participanții au evaluat, pe o scară de la 1 la 5 (1 – dezacord total, 5 – complet de acord), necesitatea ca profesioniştii contabili să fie conştienți de impactul pe care incidentele de securitate le pot avea asupra informațiilor financiare şi activităților operaționale. 43 de studenți au afirmat că sunt complet de acord cu această afirmație, iar restul participanților au afirmat că sunt parțial de acord cu această afirmație. Răspunsurile obținute sunt conforme cu rezultatele prezentate de către ACCA, fapt ce denotă că tinerii profesioniști manifestă un nivel semnificativ de conştientizare privind potențialul impact al incidentelor de securitate. Cu toate acestea, creşterea accentuată a alertelor de securitate la nivel național, conform raportului publicat de CERT, reprezintă un semnal de alarmă, ce scoate în evidență lipsa unor cunoştințe suficient de bine dezvoltate, care stau la baza viitoarelor incidente cibernetice.

Pentru a analiza dacă există o cultură a protecției informațiilor în companiile în care studenții lucrează, aceştia au fost întrebați dacă au participat la cursuri pentru menținerea şi protecția datelor sensibile. 79,59% dintre participanți au răspuns afirmativ la această întrebare, iar restul respondenților au afirmat că nu au participat la niciun curs de acest fel. Acest rezultat reprezintă un factor pozitiv, însă luând în considerare faptul că în prezent mediul universitar din România nu acoperă în totalitate curricula necesară în domeniul securității informației, aşa cum au demonstrat cercetările anterioare (Stanciu şi Rîndaşu, 2017), restul de 20% dintre companiile la care participanții studiului sunt angajați trebuie să acorde o importanță sporită asupra aspectelor de securitate a informațiilor.

Având în vedere faptul că acțiunile angajaților afectează în mod direct securitatea datelor, participanții au fost întrebați dacă parolele pe care le utilizează în cadrul organizațiilor sunt sigure, în funcție de complexitatea minimă cerută de sistem şi de intervalul de valabilitate. Deşi 95,91% dintre studenți au răspuns afirmativ la această întrebare, 31 dintre aceştia au confirmat că îşi păstrează parolele notate la locul de muncă. Chiar dacă sistemele utilizate de companiile în care lucrează respondenții, implică utilizarea unor parole puternice, păstrarea parolelor scrise la locul de muncă este o practică ce poate duce la apariția expunerii malițioase a datelor sensibile. Aşa cum demonstrează literatura de specialitate (Evans ş.a., 2016; Symatec, 2015).

Pentru a analiza dacă organizațiile în care lucrează participanții la studiu au implementat controale de asigurare a securității, precum programe anti-virus, numai 75,51% dintre respondenți au răspuns afirmativ. Acest aspect ridică un semn de întrebare asupra prioritizării protecției informațiilor la nivelul organizațiilor, cu atât mai mult din cauza faptului că programele malware reprezintă una din cele mai importante vulnerabilități ale aplicațiilor ERP (Ali şi Afzal, 2017).

O altă întrebare a chestionarului s-a axat pe scanarea ataşamentelor primite pe e-mailul de la locul de muncă. Analizând răspunsurile oferite, s-a observat că numai două persoane scanează întotdeauna ataşamentele, 20 de respondenți au afirmat că scanează ataşamentele doar atunci când expeditorul nu le este cunoscut, iar restul de 29 au afirmat că nu scanează niciodată ataşamentele, cu toate că majoritatea participanților au afirmat că dispun de un anti-virus. Această practică a respondenților atrage atenția asupra faptului că angajații reprezintă o componentă importantă a riscului de expunere a datelor, cu toate că dispun de majoritatea instrumentelor necesare de securizare a activității.

Răspunsurile oferite de către participanți demonstrează că aceştia sunt conştienți de impactul pe care îl pot avea

incidentele de securitate, dar totodată, rezultatele indică faptul că respondenții nu manifestă întotdeauna un comportament corespunzător, ar trebui să reprezinte un semnal de alarmă pentru organizații. Practici precum păstrarea parolelor de acces notate la locul de muncă şi deschiderea ataşamentelor din email-uri, fără a fi scanate în prealabil, reprezintă modalități de expunere a datelor sensibile ale companiilor pentru care respondenții lucrează.

Cu toate că 80% dintre participanți au fost instruiți cu privire la securitatea informațiilor, majoritatea încă practică acțiuni care sunt în neconcordanță cu o politică eficientă de prevenire a datelor confidențiale. Considerăm că acest rezultat se poate explica prin două moduri: este posibil ca sesiunile de instruire la care au participat angajații să nu fi fost suficient de clare sau participanții nu înțeleg cu adevărat rolul semnificativ pe care îl dețin în protejarea informațiilor.

Concluzii

În prezent, incidentele de securitate reprezintă una din cele mai importante preocupări în era IoE datorită faptului că evoluția tehnologică a introdus în domeniul financiar-contabil noi concepte precum: sisteme ERP, cloud computing şi tehnologii mobile care prezintă, pe lângă varietatea de avantaje, vulnerabilități specifice care amenință securitatea informațiilor sensibile. În ultimii ani s-a observat o creştere a incidentelor de securitate, atât pe plan național, cât şi la nivel global. Conform ultimului raport emis de CERT, în România, în anul 2016 s-au înregistrat peste 110 milioane de alerte de securitate cibernetică, creşterea față de anul anterior fiind de peste 60%. La nivel global, conform statisticii emise de Breach Level Index, s-au petrecut peste 1,3 miliarde de incidente de securitate informatică, creşterea fiind de peste 85%, comparativ cu anul 2015.

În domeniul financiar-contabil majoritatea activităților a fost digitalizată datorită nevoii de a avea acces continuu la informațiile relevante, în timp real. Fie că vorbim de tehnologii mobile, sisteme ERP sau platforme cloud computing, aproape toate informațiile sensibile s-au mutat în mediul electronic. Obiectivul acestei lucrări a fost de a analiza principalele provocări privind securitatea informației în contextul contabilității digitale, care sunt vulnerabilitățile tehnologiilor utilizate în prezent, precum şi efectuarea unei investigații privind percepția şi nivelul de conştientizare a impactului incidentelor de securitate, din perspectiva viitorilor profesionişti contabili.

Analizând datele prezentate putem afirma că există o varietate de vulnerabilități, care au un potențial crescut de a afecta securitatea informațiilor financiare, dar şi a activităților operaționale, precum şi a reputației organizațiilor.

Din cauza faptului că în prezent atât aplicațiile ERP, cât şi platformele cloud computing sunt încă în curs de dezvoltare, este de aşteptat ca noi tipuri de vulnerabilități să apară o dată cu progresul tehnologic. Cea mai bună soluție de prevenție a incidentelor de securitate este de a utiliza în implementarea sistemelor şi a aplicațiilor, cele mai bune practici de securitate, dar şi de a implementa controale eficiente, care să monitorizeze constant potențialele expuneri de informații sensibile.

O altă concluzie importantă a acestui studiu o reprezintă necesitatea creării unei culturi stabile de management şi prevenție a riscului, în special în cazul informațiilor sensibile. Cercetarea empirică efectuată a demonstrat că tinerii profesionişti înțeleg importanța protecției datelor, însă nu întotdeauna manifestă cel mai corect comportament pentru a preveni incidentele de securitate. Având în vedere aceste rezultate, considerăm importantă implicarea mediului universitar, prin oferirea în cadrul programelor de studii a unui suport suficient privind securitatea informațiilor.

BIBLIOGRAFIE

1. Ahmed, H.A.S., Ali, M.H., Kadhum, L.M., Zolkipli, M.F. şi Alsariera, Y.A. (2017), A review of challenges and security risks of cloud computing, *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 9, nr. 1-2, pp. 87-89.
2. Ali, A. şi Afzal, M.M. (2017), Database security: Threats and solutions, *Database*, vol. 6, nr. 2, pp. 25-27.
3. Bahssas, D.M., AlBar, A.M. şi Hoque, M.R. (2015), Enterprise Resource Planning (ERP) Systems: Design, trends and deployment, *The International Technology Management Review*, vol. 5, nr. 2 pp. 72-81, DOI 10.2991/itmr.2015.5.2.2.
4. Bertino, E. şi Sandhu, R. (2005), Database security-concepts, approaches, and challenges, *IEEE*

Transactions on Dependable and secure computing, vol. 2, nr. 1, pp. 2-19, DOI 10.1109/tdsc.2005.9.

5. Bhatia, T. şi Verma, A.K. (2017), Data security in mobile cloud computing paradigm: a survey, taxonomy and open research issues, *The Journal of Supercomputing*, vol. 73, pp. 2558–2631, DOI 10.1007/s11227-016-1945-y .
6. Bruchez, R. (2012), *Microsoft SQL Server 2012 Security Cookbook*, Packt Publishing Ltd.
7. CERT (2016), *Raport cu privire la alertele de securitate cibernetică procesate de CERT-RO în anul 2016*, disponibil on-line la https://cert.ro/vezi/document/raport-alerte-cert-ro-2016 (accesat 15 Aprilie 2017).
8. Cloud Standards Customer Council (2015), *Practical Guide to Platform-as-a-Service*, disponibil on-line la http://www.cloud-council.org/CSCC-Practical-Guide-to-PaaS.pdf (accesat 15 Aprilie 2017).
9. Davenport, T.H. (1998), Putting the enterprise into the enterprise system, *Harvard Business Review*, vol. 4, pp. 121-131.
10. Evans, M., Maglaras, L.A., He, Y. şi Janicke, H. (2016), Human behaviour as an aspect of cybersecurity assurance, *Security and Communication Networks*, vol. 9, nr. 17, pp. 4667-4679, DOI 10.1002/sec.1657.
11. Giordanelli, R. şi Mastroianni C. (2010), The cloud computing paradigm: Characteristics, opportunities and research issues, *Istituto di Calcolo e Reti ad Alte Prestazioni* (ICAR) .
12. Horwath, J. (2012), *Setting Up a Database Security Logging and Monitoring Program*, disponibil on-line la http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.394.3370&rep=rep1&type=pdf (accesat 30 Aprilie 2017).
13. Hussein, N.H. şi Khalid, A. (2016), A survey of Cloud Computing Security challenges and solutions, *International Journal of Computer Science and Information Security*, vol. 14, nr. 1, pp. 52-56.
14. Jaiswal, P.R. şi Rohankar, A.W. (2014), Infrastructure as a service: security issues in cloud computing, *International Journal of Computer Science and Mobile Computing*, vol. 3, nr. 3, pp. 707-711.
15. Kanellou, A. şi Spathis, C. (2013), Accounting benefits and satisfaction in an ERP environment, *International Journal of Accounting Information Systems*, vol. 14, nr. 3, pp. 209-234, DOI 10.1016/j.accinf.2012.12.002 .
16. Kim, W. (2013), Cloud computing architecture*, International Journal of Web and Grid Services*, vol. 9, nr. 3, pp. 287-303.
17. Klaus, H., Rosemann, M. şi Gable, G.G. (2000), What is ERP?, *Information Systems Frontiers*, vol. 2 nr. 2, pp. 141-162.
18. Kolodenker, E., Koch, W., Stringhini, G. şi Egele, M. (2017), PayBreak: Defense against cryptographic ransomware, *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, pp. 599-611.
19. Lodha, S. R. şi Dhande, S. (2014), Web Database Security Techniques, *International Journal*, vol. 2, nr. 3, pp. 293-299.
20. Malik, M. şi Patel, T. (2016), Database security-attacks and control methods, *International Journal of Information*, vol. 6, nr. 1/2, pp. 175-183, DOI 10.5121/ijist.2016.6218.
21. Møller, C. (2005), ERP II: a conceptual framework for next-generation enterprise systems?, *Journal of Enterprise Information Management*, vol. 18, nr. 4, pp. 483-497, DOI 10.1108/17410390510609626.
22. Ponorîcă, A., Al-Saedi A. şi Sadik H. (2014), The impact of enterprise resource planning systems on management accounting, *Challenges of the Knowledge Society*, vol. 4, nr. 1, pp. 682-690.
23. Sharma, M.M., Husain, S. şi Ali, M.S. (2017), Cloud computing risks and recommendations for security, *International Journal of Latest Research in Science and Technology*, vol. 6, nr. 1, pp. 52-56.
24. Stanciu, V. şi Rîndaşu, S. (2017) Emerging information technologies in accounting – are the aspiring professional accountants prepared to face the challenges? A case study of Romanian universities, *Proceedings of the 29th International Business Information Management Association Conference*, pp. 2455-2467.
25. Stanciu, V. şi Tinca, A. (2013), ERP solutions between success and failure, *Accounting and Management Information Systems*, vol. 12, nr. 4, pp. 698-612.

26. Surjit, R., Rathinamoorthy R. şi Vishnu Vardhini, K. J. (2016), *ERP for Textiles and Apparel Industry*, WPI Publishing.
27. Swart, R., Marshall, B., Olsen, D. şi Erbacher, R. (2007), ERPII System Vulnerabilities and Threats: An Exploratory Study, *Managing Worldwide Operations & Communications with Information Technolgy*, pp. 925-928.
28. Symantech, (2015) *Mistakes in the IaaS cloud could put your data at risk*, disponibil on-line la http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/mistakes-in-the-iaas-cloud-could-put-your-data-at-risk.pdf (accesat 18 Aprilie 2017).
29. The Association of Chartered Certified Accountants (2013a), *Big data: its power and perils*, disponibil on- line at http://www.accaglobal.com/bigdata (accesat 24 Aprilie 2017).
30. The Association of Chartered Certified Accountants (2013b), *Understanding investors: the road to real-time reporting,* disponibil on-line la http://www.accaglobal.com/content/dam/acca/global/PDF-technical/financial-reporting/pol-afb-ui03.pdf (accesat 20 Aprilie 2017).
31. The Association of Chartered Certified Accountants (2014), *Digital Darwinism: thriving in the face of technology change*, disponibil on-line la http://www.accaglobal.com/content/dam/acca/global/PDF-technical/futures/pol-afa-tt2.pdf (accesat 20 Aprilie 2017).
32. The Association of Chartered Certified Accountants (2016), *Cybersecurity - Fighting Crime's Enfant Terrible*, disponibil on-line la http://www.futuretoday.com/technology/digital/cybersecurity.html (accesat 20 Aprilie 2017).
33. Trigo, A., Belfo, F. şi Estébanez, R. P. (2014), Accounting information systems: The challenge of the real-time reporting, *Procedia Technology*, vol. 16, pp. 118-127, DOI 10.1016/j.protcy.2014.10.075.
34. Voulgaris, F., Lemonakis, C. şi Papoutsakis, M. (2014), The impact of ERP systems on firm performance: the case of Greek enterprises, *Global Business and Economics Review*, vol. 17, nr. 1, 112-129, DOI 10.1504/gber.2015.066536.