Audit financiar, XVI, Nr. 1(149)/**2018**, *54-62*
ISSN: 1583-5812; ISSN on-line: 1844-8801

Riscurile induse de atacurile cibernetice asupra activității de audit financiar

Cristina Raluca POPESCU,
Universitatea din Bucureşti,
E-mail: popescu_cr@yahoo.com
Gheorghe POPESCU,
Academia de Studii Economice din Bucureşti,
E-mail: Gheorghe.Popescu@cig.ase.ro

Rezumat

Dezvoltarea şi generalizarea prelucrării automate a datelor a adus, odată cu creşterea vitezei şi preciziei de prelucrare, a conectivității multiple şi a transmiterii rapide a datelor şi rezultatelor la mari distanțe, vulnerabilități şi slăbiciuni noi care pot sta la baza unor noi categorii de riscuri. Riscurile induse de atacurile cibernetice asupra activității de audit financiar implică managementul riscurilor privind securitatea sistemelor informaționale. Identificarea, diminuarea efectelor sau eliminarea acestora reprezintă cerințe obligatorii fără de care un audit financiar de calitate nu poate fi realizat într-un mediu puternic informatizat. Pentru fundamentarea acțiunilor specifice managementului riscurilor privind securitatea sistemelor informaționale, în acest studiu, am analizat principalele tipuri şi tehnici utilizate în atacurile cibernetice realizând o radiografie a acestora, identificând punctele forte şi punctele slabe ale noilor tehnologii şi sisteme care sunt favorizante sau nu sistemelor de securitate. În acelaşi timp, am analizat sistemul de securitate al unui sistem informațional, organizarea acestuia în straturi şi au fost dezvăluite domeniile specifice privind evaluarea calității securității prin metoda Mehari. În final, au fost dezvăluite câteva din rezultatele unui studiu pe bază de chestionar realizat cu sprijinul studenților masteranzi ai cursului „Auditul şi controlul sistemelor informaționale", fiind prezentate trei dintre cele mai frecvente slăbiciuni identificate pentru fiecare domeniu de securitate.

Cuvinte-cheie: *Risc, audit financiar, securitatea sistemelor informatice, managementul riscului, atac cibernetic.*

Clasificare JEL: *D83, G32, K24, L86, M15, M41, M42*

Vă rugăm să citați acest articol astfel:
Popescu, C.R. and Popescu, G. (2018), Risks of cyber attacks on financial audit activity, *Audit Financiar*, vol. XVI, no. 1(149)/2018, pp. 140-147,
DOI: 10.20869/AUDITF/2018/149/006

Link permanent pentru acest document:
http://dx.doi.org/10.20869/AUDITF/2018/149/006
Data primirii articolului: 27.06.2017
Data revizuirii: 12.09.2017
Data acceptării: 13.09.2017

Introducere

Evoluția tehnologică a transmiterii, prelucrării şi stocării datelor financiar-contabile a dat naştere unor noi concepte precum: *cloud computing*, *real-time accounting* sau *mobile reporting* dar, în acelaşi timp, a adus cu sine şi noi ameninţări care stau la baza acestor noi concepte. Pentru ascunderea intenţiilor şi faptelor rău voitoare, infractorii continuă să-şi perfecţioneze tehnicile şi metodele atacurilor informatice. Utilizatorii sunt prinşi la mijloc, devenind acum, nu numai ţinte pentru atacatori ci şi posibili facilitatori sau, chiar complici. Utilizatorii au devenit la ora actuală veriga cea mai vulnerabilă a sistemului de securitate.

Literatura de specialitate relevă faptul că dezvoltarea tehnologică a adus cu sine şi progresul extrem de rapid al ameninţărilor la adresa securităţii informaţiei. Deşi anul 2014 a fost definit la nivel mondial ca „anul atacurilor cibernetice", literatura de specialitate subliniază o tendinţă de creştere a numărului şi impactului atacurilor cibernetice de la un an la altul, cu o dezvoltare acută a atacurilor asupra dispozitivelor mobile. Aceasta demonstrează o dată în plus faptul că, problema securităţii informaţiei, gestionată prin intermediul noilor tehnologii, este o prioritate de top.

Din păcate, din raţiuni uşor de înţeles, atacurile cibernetice nu sunt suficient popularizate. Dar când efectele acestora nu mai pot fi ascunse, ele şochează prin amploarea lor. Exemple în acest sens sunt chiar marile întreprinderi nevoite să îşi întrerupă activităţile fiindcă sistemul lor informaţional a devenit nefuncţional, sau când bancomatele unei reţele bancare devin neoperaţionale o perioadă suficientă de timp pentru a crea nemulţumiri sau a induce chiar panică. Se impune cu necesitate evaluarea impactului atacurilor cibernetice pe multiple planuri: legislativ, tehnologic, economic, social.

Specialiştii în securitatea datelor sugerează că a sosit momentul să se schimbe abordarea securităţii pentru a obţine o securitate reală. Trebuie implementate controale mult mai sofisticate pentru a fi de ajutor, asigurând preventiv protecţie reală, dar şi în timpul şi după realizarea unui atac.

1. Atacurile cibernetice, principalele tipuri şi tehnici utilizate

Sistemele informaţionale actuale sunt tot mai complexe şi includ echipamente foarte eterogene. Aceste echipamente sunt cel mai adesea structurate într-o reţea de calculatoare. Aceasta este o structură deschisă la care se pot conecta permanent noi utilizatori şi noi tipuri de echipamente (terminale, laptopuri, staţii de lucru, servere, telefoane inteligente, calculatoare personale, routere, diverse elemente de conectică şi reţelistică etc.), ceea ce lărgeşte practic necontenit cercul de utilizatori care au acces la resursele acesteia (aplicaţii personale, aplicaţii distribuite, diverse servicii, fişiere, baze de date, echipamente hardware partajate, diverse alte resurse partajate). Vulnerabilitatea reţelei se manifestă pe două planuri distincte: atacul la integritatea fizică a informaţiilor (distrugerea sau modificarea acestora) şi folosirea neautorizată a informaţiilor (scurgerea de informaţii către terţi neautorizaţi în a accesa informaţiile respective).

Pentru contracararea, eliminarea sau diminuarea efectelor atacurilor cibernetice, acestea trebuie să fie foarte bine cunoscute şi analizate. În literatura de specialitate atacurile cibernetice sunt analizate din mai multe puncte de vedere. Pentru problematica abordată de noi, în acord cu Tăbuşcă (2009), atacurile cibernetice pot fi considerate ca atacuri pasive şi atacuri active.

Atacurile **pasive** sunt toate acele atacuri în care intrusul observă informaţia care trece prin canalul de comunicare, fără să interfereze cu fluxul sau conţinutul mesajelor. Se face practic doar analiza traficului interceptat, descoperirea identităţii entităţilor care comunică; se descoperă lungimea şi frecvenţa mesajelor chiar dacă conţinutul acestora rămâne ascuns. Aceste atacuri nu cauzează pagube directe şi nu încălcă regulile de confidenţialitate în ceea ce priveşte „spiritul" acestora. Scopul acestor atacuri este de a asculta datele care sunt vehiculate prin reţea, de multe ori, aceste atacuri fiind utilizate de fapt pentru a identifica diverse posibile vulnerabilităţi.

Atacurile **active** sunt acelea în care intrusul se angajează în furtul mesajelor, modificarea lor, ştergerea, rularea de aplicaţii, schimbarea conţinutului sau a adreselor, redirecţionarea, substituirea, refuzul unui serviciu, repudierea etc. Acestea sunt cele mai serioase şi periculoase pentru că ele pot cauza prejudicii masive, cu consecinţe juridice dintre cele mai neplăcute. În această categorie trebuie încadrate şi programele create cu scop distructiv care afectează serios, uneori chiar

catastrofal, securitatea calculatoarelor şi a informațiilor în general. Această categorie include: viruşii, bombele logice, viermii, trapele, programele tip cal troian etc.

În conformitate cu CISCO (2015) o radiografie a atacurilor cibernetice actuale relevă:

a) Caracteristicile atacurilor actuale:

a1. Sunt mult mai ingenioase în a profita de lacunele existente în sistemul de securitate: în anul 2014, s-a profitat de 1% din cele mai comune vulnerabilități;

a2. Securitatea prelucrărilor Java a crescut cu 34% în anul 2014 şi se aşteaptă ca atacatorii să găsească noi vulnerabilități prin JavaScript;

a3. Volumul spamurilor a crescut cu peste 250% în 2014;

a4. S-a perfecționat o nouă tehnică de spam (*en.* snowshoe spam), care nu numai că îngreunează, dar uneori face chiar imposibilă detectarea sursei.

b) Utilizatorii alături de echipele IT au devenit părți componente ale sistemului de securitate:

b1. Atacatorii actuali se bazează pe utilizatori pentru a instala programe malware sau pentru a valorifica lacunele de securitate;

b2. 56% din versiunile OpenSSL sunt mai vechi de 50 de luni şi, prin urmare, sunt în continuare vulnerabile;

b3. Utilizarea imprudentă a internetului şi accesarea paginilor web neprotejate;

b4. Creatorii de programe malware folosesc extensiile browser-ului web ca mijloc pentru distribuirea de aplicații malware şi nedorite.

c) *Nu există concordanță privind percepția securității între diferite categorii de actori*:

c1. 59% dintre şefii care răspund de securitate (CIOSs) spun că aceasta este optimizată spre deosebire de doar 46% dintre operatorii de securitate (SecOps);

c2. Circa 75% din CISOs percep instrumentele de securitate ca fiind extrem de eficace, în timp ce 25% le consideră doar în mod parțial, eficace;

c3. 91% dintre respondenții companiilor care au implementat un sistem sofisticat de securitate susțin că directorii acordă securității o prioritate mare;

c4. Doar 50% din respondenți utilizează patch-urile pentru repararea unor greşeli sau omisiuni ale sistemelor pe care le utilizează;

c5. Organizațiile medii şi mari au sisteme de securitate mai sofisticate decât celelalte tipuri de organizații.

Cele mai frecvent întâlnite tipuri de atacuri (**Tabelul nr. 1**) includ: denial of service, viruşi, viermi şi troieni, furtul de dispozitive, phishing şi ingineria socială sau atacuri web.

Impactul atacurilor informatice asupra organizației victimă, deşi imposibil de cuantificat din cauza lipsei de informații, cel mai adesea conduce la pierderea de informații, întreruperea activității, compromiterea confidențialității informației (datele cel mai adesea compromise incluzând date de identificare precum adresă sau CNP, informații medicale, numere de telefon, date financiare, adrese de e-mail, nume de utilizator şi parole etc.), avarierea sau furtul de echipamente sau pierderea de venituri potențiale.

O privire atentă asupra principalelor cauze ce permit atacurilor cibernetice să reuşească arată faptul că în peste 50% din cazuri, succesul unui atac cibernetic este doar parțial datorat expertizei şi priceperii atacatorului, fiind, totodată, permis de vulnerabilitățile din cadrul sistemelor, eroarea umană şi/sau nivelului insuficient al controalelor de securitate implementate (Bendovschi, 2015). Pentru a susține această concluzie, compania Cenzic a detectat cel puțin o vulnerabilitate majoră în peste 95% din sistemele analizate în decursul anului 2013, cu o medie de 14 vulnerabilități pe aplicație (Cenzic, 2014). Un alt rezultat extrem de important în cercetarea curentă este faptul că, în cel puțin 20% din cazuri, atacatorii nu sunt în totalitate străini organizației, printre aceştia numărându-se parteneri de afaceri, foşti angajați etc.).

Tabelul nr. 1: Principalele categorii de atacuri cibernetice

Nr. crt.	Tip atac	
1.	DoS (Denial of Service)	Această categorie include atacurile menite să întrerupă funcționarea normală a echipamentelor hardware şi software prin metoda DoS.
2.	Atacuri asupra aplicațiilor web	Această categorie include atacurile desfăşurate prin intermediul aplicațiilor web.
3.	Spionajul cibernetic	Această categorie include atacurile desfaşurate cu obiectivul de a obține acces neautorizat la date clasificate, cu scopul spionajului.
4.	Abuzul în accesul privilegiat	Această categorie include atacurile sau incidentele cauzate de abuzarea sau utilizarea neadecvată a drepturilor de acces logic la rețeaua, sistemele, datele şi echipamentele organizației.
5.	Furtul sau pierderea fizică a echipamentelor	Această categorie include orice înstrăinare, intenționată sau accidentală, a echipamentelor şi activelor informaționale.
6.	Payment card skimming	Această categorie include atacurile sau incidentele bazate pe implantarea unui dispozitiv asupra echipamentelor de citire a datelor financiare (spre exemplu ATM-uri, terminale PoS etc.).
7.	Atacul sistemelor PoS (*en.* Point-of-sale)	Această categorie include atacurile desfăşurate prin accesarea de la distanță a datelor şi a tranzacțiilor financiare citite prin intermediul unui sistem de citire a cardurilor (precum terminale PoS), cu excepția cazurilor incluse în categoria anterioară.
8.	Crimă cibernetică	Această categorie include atacurile realizate cu orice alt obiectiv în afară de spionajul cibernetic, şi cuprinde orice tehnici ce nu pot fi încadrate într-o altă categorie.
9.	Paşi de zăpadă (*en.* Snowshoe spam)	Implică trimiterea de volume mici de spam de la un set mare de adrese IP pentru a evita detectarea.
10.	Soft malware	Software care are ca scop deteriorarea sau dezactivarea computerelor şi a sistemelor informatice.
11.	Erori	Această categorie include incidentele a căror cauză nu poate fi alocată unei alte categorii.

Sursa: Prelucrările autorilor, 2017

2. Securitatea informațiilor

Securitatea informatică este în acest moment o problemă vitală pentru toți utilizatorii de sisteme de calcul, mai ales în plină era a internetului, fie că sunt furnizori de servicii, fie că sunt simpli utilizatori. Nevoia tot mai mare de comunicare, pe de o parte, şi de protecție a informațiilor pe de altă parte sunt două cerințe diferite, dacă nu chiar opuse.

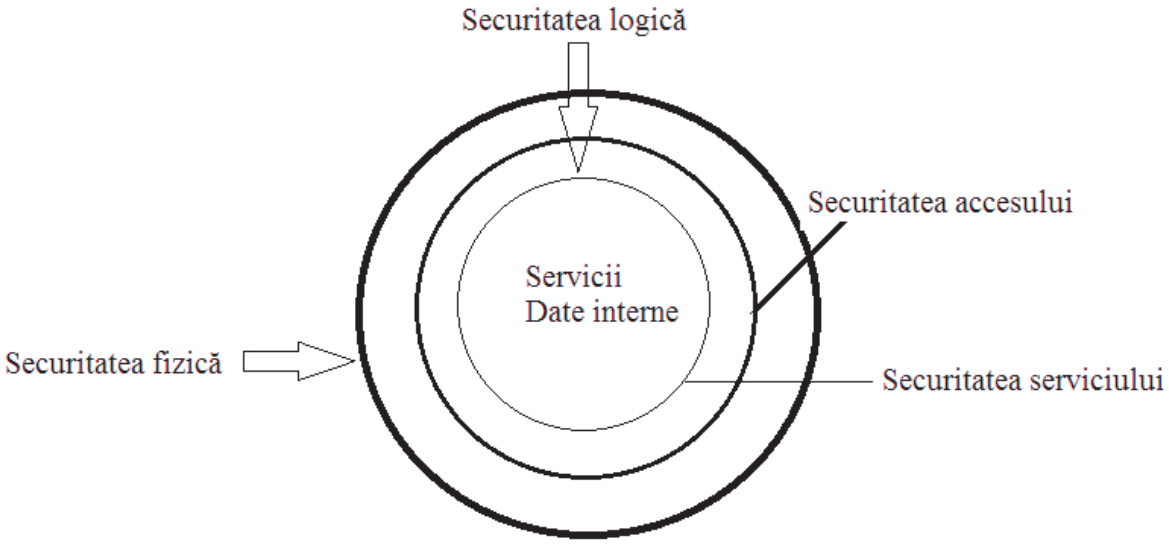
Implementarea unui sistem modern de securitate în acord cu Tăbuşcă (2009) prevede protecția pe mai multe nivele (**Figura nr. 1**).

Primul nivel este asigurat de *securitatea fizică*. Securitatea fizică, în general, constă în „încuierea" echipamentelor, plasarea lor în camere speciale ferite de foc, intemperii, distrugere fizică, fie în mod intenționat, fie nu. Este o măsură aplicabilă tuturor sistemelor de calcul, dar mai puțin posibilă în cazul rețelelor, mai ales cele de arie medie şi, cu atât mai puțin, a celor cu arie mare de răspândire.

Al doilea nivel de protecție este asigurat de *securitatea logică* şi cuprinde schema metodelor de control a accesului la resursele şi serviciile sistemului. Securitatea logică se ocupă atât de securitatea accesului, ca un prim subnivel, cât şi de securitate a serviciilor, subnivel care se află „sub" securitatea accesului din punct de vedere al structurii de securitate.

Securitatea **accesului** cuprinde: accesul la sistem, răspunzător în a determina dacă şi când este sistemul accesibil utilizatorilor şi, mai ales, în ce condiții. El este răspunzător de gestionarea evidenței accesului. Accesul la sistem poate efectua şi deconectarea forțată în anumite cazuri (expirarea contului, ora de vârf etc.); verificarea accesului unui cont, la nivelul validării numelui şi a parolei; drepturile de acces (la fişiere, la resurse, la servicii etc.) care determină ce tip de privilegii sunt fie la dispoziția unui utilizator, fie a unui grup de utilizatori.

Figura nr. 1: Niveluri de securitate



Sursa: Tăbuşcă, 2009

Securitatea **serviciilor** se ocupă de: controlul serviciilor responsabile cu funcțiile de avertizare şi de raportare a stării serviciilor, precum şi de activarea şi dezactivarea diverselor servicii oferite de către sistem; drepturile la servicii care determină cum foloseşte un anumit cont un serviciu dat (acces la fişiere, resurse, prioritate etc.).

Practic, odată stabilită conexiunea logică, subsistemul de securitate a accesului validează sau nu accesul. Subsistemul de securitate a serviciilor monitorizează activitatea utilizatorului şi ia măsuri în cazurile în care cererile acestuia depăşesc drepturile specificate în profilul utilizatorului respectiv. Accesul într-un sistem perfect sigur ar trebui să se facă prin intermediul acestor niveluri de securitate, fără să fie permisă ocolirea vreunuia din ele.

3. Mutații induse de prelucrarea automată a datelor asupra gestiunii financiar contabile şi a activității de audit

Potrivit Oprea (2008), principalele mutații induse de utilizarea sistemelor informatice puternic informatizate asupra gestiunii financiar-contabile se referă la:

- Îndepărtare de modul tradițional de păstrare a documentelor şi de gestionare a lor – *mai multe persoane pot accesa aceleaşi date*;
- Tendința de concentrare a prelucrării datelor – *riscul pierderii sau al consultării neautorizate creşte;*
- Principiul dominant al prelucrării automate a datelor (P.A.D.) GIGO (gunoi la intrare – gunoi la ieşire) – *o eroare într-un sistem integrat se propagă cu repeziciune;*
- Cerințe suplimentare pentru cei responsabili cu protecția datelor care – *nu pot intui* căile prin care datele pot fi accesate pe ascuns (pentru sustragere sau modificare) sau *nu reuşesc să descopere* de unde şi cine are acces neautorizat de la distanță;
- P.A.D. schimbă suportul informației şi mijloacele de lucru şi protecție: *creşte densitatea* informației – uşor de ascuns; *obscuritatea sau invizibilitatea* informației – nu poate fi sesizată vizual; *accesibilitatea* foarte facilă – noi categorii de infractori; *lipsa urmelor* – modificarea sau adăugarea de noi date uşor de făcut şi greu de depistat; *remanența* suporturilor –

datele şterse pot fi recuperate; *agregarea* datelor – poate dezvălui elemente vitale.

- Necunoaşterea calculatorului – i se conferă o *încredere exagerată;*
- Progresul tehnologic în accesarea datelor creşte, dar nu şi în securitatea lor;
- Integrarea puternică a sistemelor – a mărit apetitul pentru *fraudă* şi facilitează proliferarea *erorilor*;
- Procesoarele sunt foarte vulnerabile pentru specialiştii în hardware – *modifică* registrul şi folosesc instrucțiuni *privilegiate;*
- Facilitățile de comunicație – servesc ca mijloc de *fraudă* prin interceptarea semnalelor transmise;
- Terminalele la distanță pot fi *controlate şi deturnate* prin aparate speciale;
- Cu cât complexitatea creşte, cu atât riscurile cresc.

4. Riscurile în activitatea de audit financiar şi atitudinea față de risc în condițiile atacurilor cibernetice

Raționamentul profesional în audit este exercitat într-un context de risc (Gray şi Manson, 2008). Ideea de risc şi asigurare a fost prezentă în economie şi afaceri încă de la începutul perioadei în care omul a început schimburile de mărfuri. Procesul globalizării, criza economică declanşată în 2007 şi tot mai frecventele atacuri cibernetice, au făcut ca riscul să capete noi valențe, să fie mai diversificat în natura sa şi să fie mai atent abordat de orice entitate economică. Deşi nu este unanim acceptată noțiunea de risc, este acceptat faptul că riscul se referă la imprevizibilitate, la luarea deciziilor şi la potențiale pierderi. Riscul este legat de procesul luării deciziilor (March şi Shapira,1987) şi orice decizie care se ia în domeniul economic în general şi în afaceri în special, implică un anumit grad de risc. Imaginea fidelă şi denaturarea semnificativă, sunt evaluate în raționamentul profesional al auditorului tot pe baza riscului. Kendrick (2004) subliniază importanța înțelegerii atitudinilor personale cu privire la risc şi consideră că atitudinea şi comportamentul față de risc reprezintă dimensiuni cheie în înțelegerea riscului. Atitudinea factorilor de decizie față de risc în condițiile atacurilor cibernetice poate fi evaluată prin nivelul de implicare a top managementului în implementarea sistemelor de securitate complexe.

La nivelul unei entități economice auditate, riscul de audit în general, se manifestă prin componentele sale de bază: **risc inerent, risc de control şi risc de nedetectare** şi poate fi stabilit atât în termeni cantitativi (în procente) cât şi în termeni calitativi (*risc scăzut, moderat, ridicat sau foarte ridicat*).

În condițiile riscurilor induse de atacurile cibernetice asupra sistemelor informaționale auditate trebuie evaluat nivelul de calitate al sistemelor de securitate şi **nivelul de risc al securității**.

Pentru evaluarea calității sistemelor de securitate şi cuantificarea nivelului de risc al securității există numeroase preocupări în lumea specialiştilor. Una dintre acestea este furnizată de metoda Mehari, marcă înregistrată a Clubului francez de securitate a informațiilor - CLUSIF (*fr.* Club de la securite de l'information français), care pune la dispoziție: ghiduri pentru analiza mizelor, evaluarea serviciilor de securitate şi analiza riscului de securitate. Printre facilitățile practice oferite, Mehari pune la dispoziție o bază proprie de cunoştințe care permite cuantificarea nivelului calității în funcție de activitățile (controalele) implementate sau neimplementate. Nivelurile de calitate definite de metoda Mehari în ordine crescătoare de la 1 la 4, se caracterizează prin aceea că, de exemplu, *serviciul la nivelul 4 de calitate*: va rămâne activ în fața tuturor agresiunilor – ar putea fi spart în circumstanțe excepționale de cei mai buni spărgători de coduri din lume, cu cele mai bune unelte. În aceste condiții, riscul se determină prin metoda Mehari ca diferență între nivelul maxim de calitate 4 şi nivelul mediu de calitate al securității determinat pe baza unei investigații complexe a sistemului de securitate.

În urma unui studiu realizat în cursul anului universitar 2016-2017, cu ajutorul a 60 de studenți la programul de masterat CAIG (Contabilitate, audit şi informatică de gestiune) la firmele la care aceştia lucrau în perioada respectivă sau au lucrat anterior momentului desfăşurării studiului, s-a obținut un nivel mediu de calitate de 2,73 şi deci un nivel mediu de risc al calității de 1,27.

Principalele trei deficiențe constatate pe fiecare domeniu de securitate sunt sintetizate în **Tabelul nr. 2**.

Tabelul nr. 2: Principalele trei deficiențe constatate din fiecare domeniu de securitate

Domeniu	Activități implementate în mod incorect sau incomplet
1. Organizarea securității	**Nu** s-a efectuat o clasificare a informațiilor (documente, date, fişiere, baze de date etc.) în funcție de impactul unui dezastru care ar putea afecta aceste informații ale întreprinderii.
	Nu există în contractele de angajare sau în regulamentul interior, o clauză care precizează obligațiile de a respecta ansamblul de reguli de securitate în vigoare.
	Nu s-au analizat riscurile asociate accesului terților (furnizori, clienți, investitori etc.) în sistemul de informații sau în locurile care conțin informații şi nu s-au stabilit şi măsurile de securitate necesare.
2. Securitatea locației	**Nu** există o procedură care să permită detectarea ulterioară a neregulilor în gestionarea autorizațiilor de acces (ecusonul sau cardul nu a fost returnat, a fost pierdut, este fals etc.).
	Nu există un sistem în care să se garanteze că acelaşi ecuson nu poate fi folosit de către o a doua persoană (de exemplu prin memorarea tuturor intrărilor şi care să nu permită o intrare în plus, fără să fi existat o ieşire anterior).
	Nu sunt monitorizate toate căile de acces posibile, în plus față de controlul accesului pe căile normale, spre exemplu, accesul pe alte căi (cum ar fi ferestre accesibile din exterior, ieşirile de urgență, prin podele false sau plafoane).
3. Securitatea spațiilor	**Nu** există un sistem de reglare a energiei electrice, care să includă cel puțin o sursă de alimentare electrică care să nu poată fi întreruptă pentru echipamentele cele mai sensibile.
	Circuitele electrice şi cablurile **nu** sunt protejate de echipamente specializate împotriva supratensiunii şi împotriva fulgerelor.
	Nu a fost realizat un inventar sau o clasificare a tuturor tipurilor de locații sensibile.
4. Rețele extinse	**Nu** se verifică dacă utilizarea se face în conformitate cu configurarea şi necesitatea de utilizare a utilizatorului.
	Nu există clauze penalizatoare suficient de eficiente cu privire la calitatea serviciilor furnizate de prestatorul unor servicii.
	Soluțiile de recuperare în caz de dezastre sunt **insuficient** exersate.
5. Rețeaua locală	**Nu** a fost partiționată rețeaua locală în domenii de securitate, fiecare dintre acestea necesitând un set de reguli de securitate, sau în zone de încredere în care controalele să fie adaptate în mod specific.
	Nu există o procedură de gestionare a cererilor de conectare inter-domenii şi un grup care să se ocupe cu analiza acestor cereri, cu autorizarea acestora şi cu definirea unor norme de filtrare care urmează să fie puse în aplicare (firewall, cereri de servicii, protocoale etc.).
	Nu a fost realizată o analiză sistematică a potențialelor puncte unice de eşec cu scopul de a se asigura că echipamentele de serviciu (cum ar fi alimentatorul de energie, aerul condiționat etc.) nu afectează redundanța planificată a echipamentelor de rețea sau arhitectura rețelei.
6. Operațiuni în rețea	**Nu** există o politică referitoare la securitate îndreptată către personalul care operează în rețea, acoperind toate aspectele securității informaționale (confidențialitatea informațiilor, disponibilitatea serviciilor şi a informațiilor, integritatea informațiilor şi a configurărilor, abilitatea de a urmări operațiile etc.)
	Nu este obligatoriu ca toate operațiunile de mentenanță să se termine cu o verificare sistematică a tuturor parametrilor de securitate (cum au fost definite la începutul implementării).
	Integritatea configurării sistemelor **nu** este testată în mod regulat în conformitate cu cerințele configurării teoretice aşteptate (cel puțin săptămânal, dacă nu la fiecare activare a sistemului).
7. Sisteme de arhitectură şi securitatea logică	**Nu** există un audit efectuat în mod regulat, cel puțin o dată pe an, al ansamblului de drepturi atribuite la fiecare profil şi proceduri de management al profilurilor.
	Nu există un proces sistematic de actualizare a tabelului de autorizații la schimbarea funcției.
	Procesul de atribuire sau modificare a legitimațiilor utilizatorilor **nu** respectă o serie de reguli care asigură validitatea intrinsecă a acestora. În cazul parolelor: lungime adecvată (opt caractere sau mai mult), obligatoriu mixaj de tipuri diferite de caractere, schimbarea frecventă (cel puțin o dată pe lună), imposibilitatea reutilizării unei parole vechi, a cuvintelor banale, a poreclelor, a numelor, a anagramelor, a datelor cu caracter personal, uşor de aflat etc.

Domeniu	Activități implementate în mod incorect sau incomplet
8. Mediul de Producție IT	**Nu** sunt aceleaşi clauze obligatorii pentru antreprenorii care lucrează cu sistemele de operare ca pentru personalul intern.
	Nu există niciun control de rutină care să verifice dacă drepturile personalului care gestionează sistemele de operare a sistemelor s-a modificat, fapt care ar putea declanşa o alertă în cazul în care acest lucru se întâmplă.
	Documentele de referință **nu** sunt protejate prin metode sigure, împotriva modificării premature sau ilicite.
9. Securitatea prelucrărilor	**Nu** există o procedură care detaliază acțiunile care trebuie efectuate în caz de eroare sau alertă.
	Nu există una sau mai multe aplicații capabile să analizeze datele individuale diagnosticate cu anomalii şi să declanşeze o alertă către personalul operațional.
	Nu sunt stabilite mecanismele de oprire a sistemului de înregistrare şi de procesare a înregistrărilor când se declanşează o alarmă.
10. Proiecte IT şi dezvoltarea securității	**Nu** există studii şi recenzii ale noului proiect în care sunt prezentate riscurile, deciziile luate cu privire la acceptarea sau nu şi cu privire la orice măsuri de securitate suplimentare necesare.
	La achiziția unei noi aplicații **nu** există o garanție potrivit căreia competența şi disponibilitatea personalului de întreținere ale furnizorului permit să se răspundă în mod satisfăcător la solicitările de întreținere ale utilizatorilor. De asemenea, acest acord ar trebui să ia în considerare perioadele de week-end şi de vacanță.
	În cazul dezvoltării unei aplicații confidențiale, **nu** sunt instituite profile care să permită distribuirea de informații confidențiale, astfel încât accesul la acestea să fie limitat numai la persoanele care au o nevoie reală.
11. Gestionarea stațiilor de lucru ale utilizatorilor	Procedurile de control legate de configurația utilizatorului **nu** sunt subiectul unui audit periodic.
	Conformitatea configurărilor hardware ale stațiilor de lucru **nu** sunt controlate în mod regulat, în raport cu opțiunile autorizate.
	Departamentul IT **nu** manageriază o referință pentru fiecare produs software instalat pe stațiile de lucru ale utilizatorilor (cod sursă şi executabil).
12. Operațiuni de telecomunicații	**Nu** există un audit efectuat în mod regulat, cel puțin o dată pe an, al aplicării efective a procedurii de evaluare, semnare şi asumare de către personalul operațional (angajat direct de către societate sau indirect, printr-o companie prestatoare de servicii) a obligațiilor privind securitatea.
	Măsurile de securitate determinate pentru a contracara noile riscuri identificate, **nu** sunt revizuite în mod oficial înainte de punerea în aplicare.
	Contractele de service **nu** detaliază intervalele de timp necesare şi zilele de intervenție compatibile cu cerințele de disponibilitate.
13. Procese de management	Directivele **PPI** (Protecția informațiilor personale) **nu** acoperă toate obligațiile legale, incluzându-le pe acelea care sunt legate de colectarea, accesarea, comunicarea, utilizarea, păstrarea şi distrugerea acestor tipuri de informații.
	Nu există un comitet legat de organismele guvernamentale care să aibă drept responsabilitate dezvoltarea comunicării datelor financiare şi care să studieze periodic şi să rezolve diferite probleme.
	Nu se realizează evaluări periodice care vizează nivelul de cunoaştere a personalului cu privire la protecția sistemelor informatice şi a mecanismelor de securitate.

Sursa: Prelucrările autorilor, 2017

Concluzii

În condițiile în care atacurile cibernetice au crescut an de an şi utilizatorii sistemelor informatice au devenit din ținte facilitatori sau complici, popularizarea principalelor mecanisme de realizare a acestor atacuri este nu doar necesară ci chiar obligatorie. Auditorul financiar atunci când auditează activitatea unei entități puternic informatizate, la evaluarea riscului de audit, alături de componentele sale de bază: **risc inerent, risc de control şi risc de nedetectare** trebuie să introducă o nouă componentă specifică, respectiv **nivelul de risc al securității**, fără de care un audit de calitate nu poate fi realizat.

BIBLIOGRAFIE

1. Bendovschi, A. (2015), Cyber-attacks – trends, patterns and security countermeasures, *Procedia Economics and Finance,* vol. 28, pp. 24-31, DOI 10.1016/s2212-5671(15)01077-1.
2. Gray, I., Manson, S. (2008), *The audit process: principles, practice and cases*, Thomson Learning, UK, London.
3. Kendrick, T. (2004), Strategic risk: Am I doing OK?, *Corporate Governance*, vol. 4, nr. 4, pp. 69-77, DOI 10.1108/14720700410558899 .
4. March, J.G. şi Shapira, Z. (1987), Managerial perspectives on risk and risk taking, *Management Science*, vol. 33, pp. 1404-1418, DOI 10.1287/mnsc.33.11.1404.
5. Oprea, D. (2008), *Protecția şi securitatea informațiilor*, Iaşi, Editura Polirom.
6. Tăbuşcă, A. (2009), A quick look at the future of protection – nine guidelines to follow, *Journal of Information Systems & Operation Management*, vol. 1, nr. 3.
7. CISCO (2015), *Annual security report 2015*, disponibil la https://www.cisco.com/c/dam/assets/global/DE/unified_channels/partner_with_cisco/newsletter/2015/edition2/download/cisco-annual-security-report-2015-e.pdf, accesat la data de 1.11.2017.