SEPA • Sisteme de plăți SWIFTNET • Outsourcing • Învățământ bancar

intelligent management

# BANK Watch

Nr. 9 / 15 decembrie 2009 - 15 ianuarie 2010
www.marketwatch.ro

FIN WATCH

# PROVOCĂRI ÎN CREAREA UNUI PERIMETRU DEFENSIV STRUCTURAT

paginile 6-7

Infrastructuri de plăți • Canale electronice de distribuție • Sisteme informatice

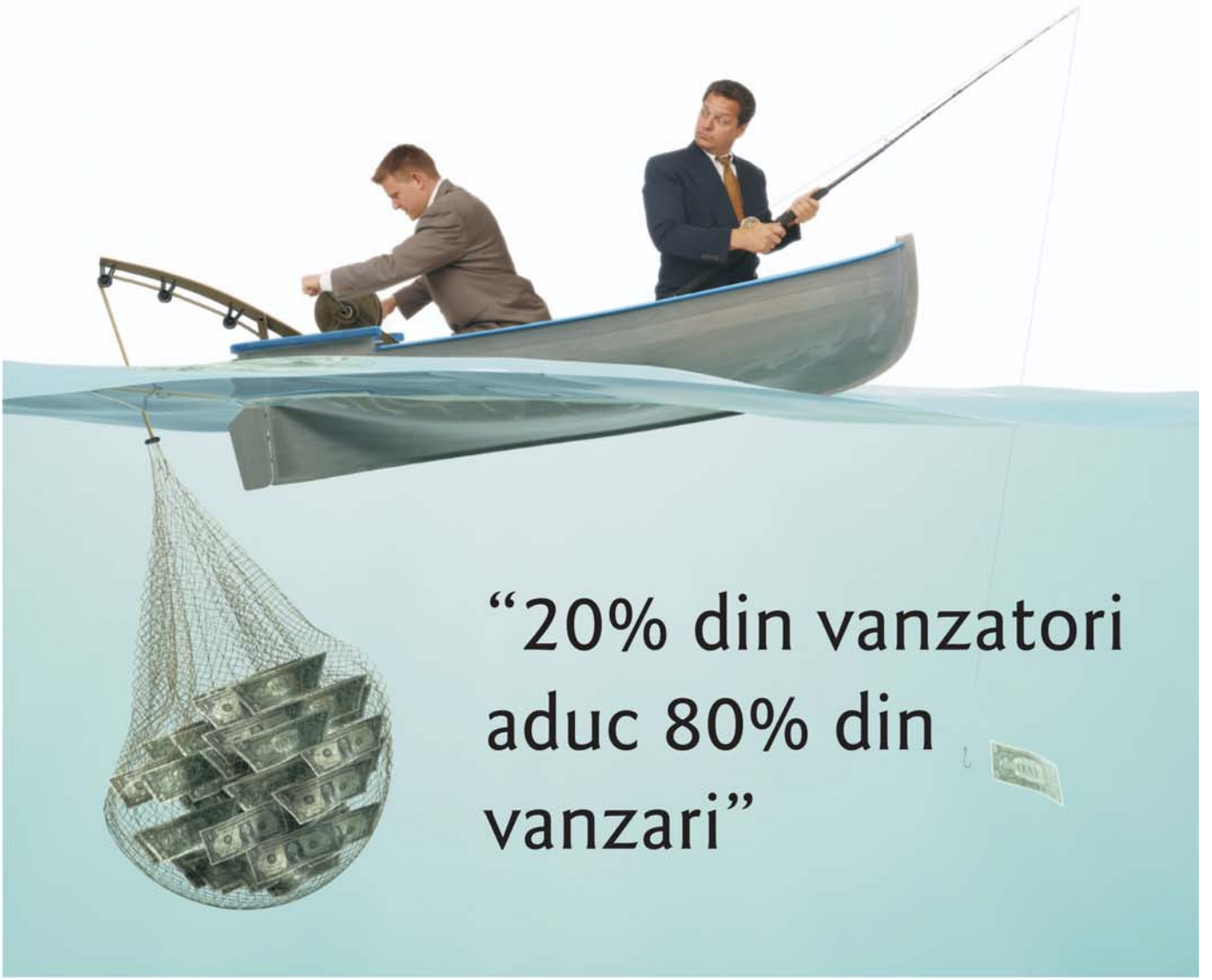
✓ IT&C Consultancy
✓ Project Management
✓ Technology Expertise

glit®
innovate IT

E-mail: office@glit.ro; Tel: 031 620 1772; Fax: 031 620 1773; www.glit.ro

**AnytimeSales**

prospect | convert | sale | retain




Adevarat, dar cum sa-i ajuti pe ceilalti 80% sa vanda la fel de mult?

---

Pentru atingerea targetului de vanzari in 2009, alege **AnytimeSales**

www.anytimecrm.ro

# Stimaţi cititori,

Editura Fin Watch, cu sprijinul Asociaţiei Române a Băncilor, editează revista lunară BankWatch, ajunsă acum la a 9-a ediţie (s-a lansat în martie 2009).
În anul său de debut, revista a fost distribuită gratuit, în mod promoţional, către instituţiile bancare din România.
În ceea ce priveşte distribuţia revistei în 2010, vă transmitem oferta de abonamente care vă dă posibilitatea ca revista să fie distribuită şi să furnizeze informaţii valoroase, prin conţinutul articolelor, următoarelor direcţii şi departamente din bancă:

- Strategie şi management
- Operaţiuni, Plăţi, Decontări
- IT şi telecom
- Conformitate
- Securitate
- SWIFT

De asemenea, considerăm necesar ca revista să ajungă în reţeaua băncii (cel puţin la sucursale), pentru ca să-şi atingă scopul şi crezul său, şi anume, acela de a oferi informaţii şi analize privind cele mai noi tehnologii şi concepte bancare, personalului bancar din zona de management şi strategie, dar şi din cea operaţională, pentru cunoaşterea şi aderarea la practici moderne de business şi tehnologie.
Preţul unui abonament anual (10 ediţii) la BankWatch este de 100 Ron (TVA şi costuri expediere incluse)
Mulţumindu-vă pentru interesul arătat în 2009, vă dorim mult succes în noul an şi o colaborare cât mai bună!

REDACŢIA




**Pentru abonare la revista BankWatch, trimiteti la redactie@finwatch.ro urmatoarele informaţii:**

Denumire companie .....
Adresă .....
Tel./Fax. ..... Email.....
Persoana contact..... Nr. abonamente dorite.....
*Date de facturare:*
CUI ..... Nr. Înreg. Reg. Com. .....
IBAN ..... Banca / sucursala .....




# SUMAR





**Editor:** FIN WATCH
Aleea Negru Vodă nr. 6, bl. C3, sc. 3 parter, 030775, sector 3, Bucureşti
Tel.: 021.321.61.23; Fax: 021.321.61.30;
redactie@finwatch.ro
www.marketwatch.ro
P.O. Box 4-124, 030775

- **Director General FIN WATCH:** Călin.Mărcuşanu@finwatch.ro
- **PUBLISHER FIN WATCH:** Gabriel.Vasile@finwatch.ro
- **Colegiu redacţional:** Rodica.Tuchilă@arb.ro, Adrian.Apolzan@ing.ro, Călin.Rangu@irucservice.ro, Constantin.Rotaru@arb.ro, lDumitru@transfond.ro, Marcelina.Joavină@microsoft.com, Răzvan.Grigorescu@CEC.Ro, CChicu@alphabank.ro, CretuC@visa.com

Luiza.Sandu@marketwatch.ro
Radu.Ghitulescu@marketwatch.ro

- **Marketing:** Valentina.Tudor@marketwatch.ro
- **Publicitate:** Director: Alexandru.Batali@finwatch.ro, Alexandru.Pădure@marketwatch.ro
- **Desktop Publishing:** Omni Press & Design, (art@opd.ro)
- **Foto:** Septimiu Şlicaru (tslicaru@yahoo.com)
- **Abonamente:** redactie@finwatch.ro
- **Distribuţie:** Ionel.Tudor@marketwatch.ro, Elena Corneanu, Sorin Pârvu
- **Tipar:** VISUAL 2003





- **Data închiderii ediţiei:** 22 decembrie 2009

RĂZVAN GRIGORESCU
PHD, CISSP, CISA, CGEIT,
ISO 27K01 LA,
ITIL&COBIT SM

# Provocări în crearea unui perimetru defensiv structurat

Poate cel mai important lucru pe care lumea securității informației l-a învățat de-a lungul multor ani de luptă împotriva atacurilor informatice, a evenimentelor neprevăzute, a erorilor de cod și a greșelilor, neglijenței sau sabotajelor în exploatarea sistemelor informatice, a constat în faptul că nu există în fapt un perimetru, metodă sau produs de securitate impenetrabil.

Orice sistem are lacune și limitări sau poate fi configurat în mod eronat, însă poate cel mai important aspect constă în faptul că orice sistem poate fi compromis în urma unor acțiuni menite să-l destabilizeze. Lupta fără de sfârșit între cei care încearcă să protejeze și cei care încearcă să compromită sistemele IT&C, este de la început inegală.

Pentru cei care încearcă să penetreze mecanismele de securitate, este suficient să reușească o dată. O singură vulnerabilitate identificată într-un mecanism de control va permite atacatorului să compromită sistemul respectiv și să aibă acces la informațiile protejate. Atacatorii își pot permite să aloce perioade apreciabile de timp în scopul identificării unei slăbiciuni la nivelul unui echipament de securitate. Aceștia pot decompila cod program, inspecta pachete sau utiliza diverse alte tehnici în speranța identificării sau creării unei căi de acces în sistem.

Pe de altă parte, cei care implementează mecanismele de securitate nu pot în mod real aloca aceeași perioadă de timp pentru fiecare verigă din infrastructura aflată în exploatare.

Un alt exemplu edificator cu privire la această asimetrie implică ceea ce este cunoscut sub numele "atacul din prima zi"[1]. Acest tip de atac precede apariția remediilor pentru anumite vulnerabilități sau a existenței semnăturilor care să poată face posibilă identificarea și oprirea atacului. Veștile despre noile vulnerabilități circulă repede în lumea atacatorilor și vor fi utilizate în scop malefic, mai rapid decât pot cei responsabili cu asigurarea securității să-și protejeze sistemele.

În momentul în care o problemă sau vulnerabilitate este identificată și publicată, un atacator "se apucă imediat de treabă", în sensul de a găsi modalități prin care să o poată exploata. Deși acest gen de notificări nu conțin de regulă prea multe informații tehnice care să explice în ce constă vulnerabilitatea respectivă sau cum poate fi ea exploatată, un atacator experimentat sau "norocos" poate pune cap la cap elementele lipsă și intră în posesia informațiilor cheie. Acest lucru se traduce prin faptul că o vulnerabilitate poate fi exploatată foarte repede, uneori chiar din "prima zi". Un astfel de atac poate surveni cu mult înaintea găsirii unui remediu – mai ales în cadrul unor infrastructuri de date complexe. Există anumite etape obligatorii care trebuie parcurse, parte a ciclului de viață al remediilor puse la dispoziție de producatori:

- identificarea și testarea la producator;
- inițierea unor campanii de informare la beneficiari;
- verificarea de către beneficiari pe medii de testare/dezvoltare;
- implementarea în mediul de producție, uneori pe sisteme numeroase aflate în așteptarea unor "ferestre de mentenanță".

Datorită acestei inerente debalansări a forțelor, lumea securității informației a înțeles cu mult timp în urmă, că singura modalitate de a combate atacurile și de a furniza un nivel acceptabil al securității, constă într-o strategie denumită "apărare în adâncime"[2]. La baza acestui tip de strategie stau implementarea mai multor nivele de securitate, versus construirea unui singur nivel perfect – impenetrabil. Prin utilizarea mai multor nivele, strategii și tehnologii de securitate, în situația în care unul dintre nivele este compromis, acest lucru nu va conduce la o expunere imediată a bunurilor protejate. Această nouă abordare schimbă regulile jocului în favoarea "băieților buni"; de această dată, un atacator trebuie să reușească multe lucruri, din prima încercare și într-un interval scurt de timp, ceea ce statistic este mult mai dificil.

## AAA

Autentificarea, Autorizarea și Administrarea, în titulatura de specialitate

a securității informatice cunoscută ca "triada A", tratează aspectele legate de "Cine" încearcă să acceseze resursele și "Dacă" respectiva entitate este autorizată să o facă. Etapa de autentificare implică obligativitatea utilizatorului de a furniza informații legate de "ceea ce știe" – o parolă, "ceea ce deține" – un dispozitiv de generare parole, sau "ceva ce reprezintă" – caracteristici biometrice (amprentă, voce, iris etc.); în practică, se utilizează și combinații între ele.

- Metode și tehnologii de *autentificare* includ politici de parolă, PKI[3] - certificate digitale, card-uri inteligente, generatoare de parole unice (OTP[4]), dispozitive de citire și comparare biometrică;
- *Autorizarea* este responsabilă cu stabilirea resurselor pe care utilizatorul are dreptul să le acceseze;
- *Administrarea* se concentrează pe centralizarea managementului și organizării drepturilor și privilegiilor. În această categorie, cele mai "vizibile" produse sunt cele legate de "autentificare unică – SSO[5]" și "managementul identității" – cea din urmă permițând în mod centralizat definirea utilizatorilor și acordarea privilegiilor pentru mai multe resurse și aplicații.

## Firewalls

Sunt echipamente destinate consolidării perimetrului rețelei de date proprii instituției și protejării punctelor critice de joncțiune, așa cum sunt conexiunile către Internet, furnizori externi și chiar segmentarea rețelei interne pentru separarea mediilor de testare/dezvoltare față de cel de producție. Principiul de utilizare al acestor dispozitive este acela de a menține utilizatorii ne-autorizați în afara rețelei de date a instituției. Echipamentele de tip "firewall" fac parte integrantă, de ani buni, din infrastructura oricărei întreprinderi, în prezent absența unui astfel de echipament fiind considerată neglijență gravă sau tentativă de sinucidere IT.

## Rețele private virtuale[6]

Această tehnologie și-a făcut apariția atunci când Internet-ul a devenit rețeaua de date atotcuprinzatoare care este astăzi, permițând companiilor să-și conecteze punctele de lucru aflate la mari distanțe sau să permită angajaților acestora să acceseze resursele de date interne companiei, de oriunde din lume. Această tehnologie permite crearea unor tunele de comunicație virtuale peste rețele de date nesigure (Ex. Internet-ul), algoritmii de criptare utilizați asigurând confidențialitatea informațiilor.

## Detecția și Prevenția Intruziunilor[7]

Echipamentele "firewall" despre care am vorbit constituie un prim nivel al protecției dar sunt limitate din punct de vedere al analizelor interne pe care le realizează asupra traficului de date. Dispozitivele și aplicațiile ce intră în categoria detecției și prevenției intruziunilor sunt destinate analizelor și inspecțiilor mai elaborate asupra conținutului pachetelor de date, fiind programate să genereze alarme sau să filtreze traficul cu potențial periculos. Există în prezent două tipuri de abordări în utilizarea acestor sisteme bazate pe:

- biblioteci de semnături, utilizate în scopul identificării și contracarării acțiunilor și scenariilor de atac cunoscute;
- învățarea unui tipar al traficului de date considerat normal, orice abatere peste anumite limite fiind investigată ca fiind susceptibilă de un atac informatic.

## Identificarea vulnerabilităţilor

Aplicațiile utilizate în evaluarea și identificarea vulnerabilităților se bazează pe sesiuni de investigare a versiunilor sistemelor de operare, bazelor de date, aplicațiilor etc și compararea cu vulnerabilități cunoscute. Acest proces permite în mod proactiv, îmbunătățirea prestației sistemelor din punct de vedere al securității informației, prin aplicarea actualizărilor recomandate de producători, în vederea eliminării vulnerabilităților semnalate.

## Managementul Securității

Datorită faptului că securitatea informației a devenit un domeniu atât de complex iar protejarea infrastructurii reprezintă o activitate critică, există numeroase aplicații/dispozitive menite să ușureze acest proces, prin centralizarea și interpretarea informațiilor relevante, provenite de la diverse echipamente IT&C. Aceste aplicații intră la categoria Managementului Securității Informației (SIM)[8], care este capabil să agrege informații, să le coreleze și să emită rapoarte pe această temă.

## Platforme Antivirus

Acestea reprezintă probabil cele mai vizibile produse pe parte de securitate și le cunoaștem în marea lor majoritate prin prisma experienței personale. Acest nivel de securitate se focalizează pe protejarea utilizatorilor codului program, cu efecte nocive asupra sistemelor de calcul, existând mai multe familii de astfel de specimene (viruși, viermi, Troieni, bombe logice etc), diferind prin modalitățile de replicare, efectele și factorii declanșatori.

Strategiile anti-virus se concentrează pe mai multe direcții:

- local, pe fiecare stație de lucru;
- pe echipamentele de comunicație plasate la puncte de convergență între rețele externe organizației;
- centralizat, prin intermediul unor console de management și agenți distanți;
- la nivelul Proxy serverelor de Internet și a serverelor de E-mail;

Pentru îmbunătățirea performanțelor de detecție, în practică se utilizează în mod simultan platforme antivirus furnizate de mai mulți producători și bazate pe mai multe tipuri de tehnologii. ■

1 - Zero day-attack (Engl. orig.)
2 – Defense în Depth (Engl. orig.)
3 – Public Key Infrastructure (Engl. orig.)
4 – One Time Password (Engl. orig.)
5 – Single Sign-On (Engl. orig.)
6 – VPN (Virtual Private Network – Engl. orig.)
7 – IDS/IPS (Intruder Detection/Protection System – Engl. orig.)
8 – SIM (Security Information Management – Engl. orig.)

# ATM-ul intelligent, încotro?

Integrarea înseamnă a avea acces la aceleași resurse, prin aceeași logică de business și cu aceleași rezultate. Diferența stă doar în modul de prezentare. Conținutul trebuie să fie același, indiferent dacă îl accesezi prin Internet Banking, de la ATM sau de la unitatea bancară. Prin conținut se înțeleg aceleași produse, cu aceiași parametri, eventual doar cu alte tarife, deoarece canalele alternative de distribuție sunt în general oferite mai ieftin de către bancă față de operațiunile prin unitățile bancare.


Dar, cât de departe suntem de un astfel de sistem? Destul de departe. Dacă inițial sistemele de carduri dețineau un avans tehnologic apreciabil, fiind sisteme centralizate, informatizate puternic, în timp ce multe aplicații de core-banking erau descentralizate și dezvoltate în limbaje învechite, în prezent gradul de dezvoltare al serviciilor prin ATM lasă de dorit. Chiar și kiosk-urile bancare par mai evoluate. Dar, să o luăm treptat.

Aplicațiile de front-office bancar devin din ce în ce mai web-based, interfețe de tip browser îi permit lucrătorului bancar să deruleze toate operațiunile bancare necesare, atât cash cât și non-cash. Interfața de lucru este adaptată în funcție de specializarea sa, de rolul său pe fluxul de lucru, de drepturile pe care utilizatorul le are. Dacă ne uităm la aplicația de Internet Banking pe care o utilizează clientul bancar acasă, aceasta are în principiu aceleași funcționalități, restrânse însă la drepturile sale. Dacă funcționarul bancar putea accesa informațiile tuturor clienților, clientul utilizator al Internet Bankingului va vedea doar datele proprii. Operațiile care se pot efectua vor fi însă similare. Bineînțeles, va lipsi partea de cash, deși o dată cu extinderea banilor virtuali, a cash-ului electronic, s-ar putea ca acel client să-și încarce singur din cont o suma de bani pe chip-ul cardului de plată. Deci, cele două aplicații pot fi similare, putând fi aceeași aplicație, dar cu drepturi diferite, inclusiv limitări la anumite operațiuni, dar limitări intenționate, nu impuse de diferența tehnologică.

Dacă clientul este obișnuit cu ecranul de calculator și cu informațiile furnizate de aplicația de Internet Banking, de ce nu ar întâlni aceeași interfață, același ecran și la ATM? Deoarece procesatorul de carduri, dacă deține și managementul bancomatului, nu are de fapt nimic în comun cu aplicațiile băncii. Are multe în comun referitor la conturi și la operațiunile de plată. Dar, acestea sunt accesate prin interfațări, de multe ori dedicate și dificil de a fi integrate într-o arhitectura deschisă, de tip SOA (Service Oriented Architecture). Deși multe ATM-uri permit plățile de utilități, altele permit depunerea de numerar în conturile curente, toate aceste operațiuni sunt dedicate. Ele au fluxuri operaționale diferite de cele derulate prin unitatea bancară sau prin alte canale alternative.

Practic, ATM-ul ar trebui să fie doar un ecran de prezentare, operațiunile afișate și derularea lor să fie sub forma unor servicii care să apeleze aceleași funcționalități de business, aceeași logică de business și să apeleze aceleași structuri de date și produse ca și celelalte aplicații bancare. Un kiosk bancar ar putea mult mai ușor să preia acest rol. Un kiosk este de fapt un calculator sub o formă aparte, cu un display care să afișeze o aplicație bancară similară cu cea din front-office sau cea de Internet Banking. Acest kiosk poate avea și funcționalități de plată, în schimb nu mai trebuie să treaca printr-un procesator dedicat, ci să apeleze aceiași adaptori către un middleware de tip SOA ca și celelalte aplicații. Dacă sunt plăți sau retrageri cu carduri gen VISA sau Mastercard, se vor apela gateware-urile acestora, bineînțeles, dar atât ar trebui să rămână dedicat, în rest totul putând fi integrat în structura comună a infrastructurii băncii. Bineînteles, vorbim de acele bănci care își dezvoltă infrastructurile software conform best-practice-urilor internaționale, plecând de la conceptual SOA și al arhitecturilor pe trei nivele (back- middleware-front). Deci, ATM-ul inteligent și multifuncțional bate la ușă, iar unii au și făcut pasul.

■ Dr. Călin Rangu
CEO IIRUC Service

# Securitatea în rețelele moderne tip Enterprise

Numărul de incidente raportate pe tema securității în rețelele informatice urmează un trend crescător, un nivel îngrijorător atingând atacurile **externe**, provenite din domeniul public (**Internet**) și, mai recent, atacurile **interne**, provenite din interiorul rețelelor. Având în vedere evoluția naturală a rețelelor tip Enterprise și SMB ca suport pentru servicii de tip Quad Play (Date, Voce, Video și Mobilitate), protejarea acestora capătă o importanță din ce în ce mai mare.

Printre cele mai utilizate mijloace **externe** de a produce daune atunci când este vizată o rețea sunt atacurile de tip DoS/DdoS, atacuri prin e-mail, web sau accesul neautorizat pe anumite servere ce conțin date confidențiale sau aplicații critice pentru activitatea unei companii.

Primul pas făcut în direcția implementării unei defensive eficiente este de a „ridica" un **Firewall** ca o barieră în fața punctului de intrare în rețea, unde tot traficul este monitorizat pe măsură ce intră sau iese din rețea. Al doilea nivel de securitate, furnizat din spatele firewall-ului este făcut prin **Sisteme de detecție și prevenire a atacurilor (IDS/IPS).**

În rețelele informatice se utilizează pentru transportul datelor prin spațiul public **tunele securizate** numite **VPN** (Virtual Private Network). Pentru VPN-uri bazate pe protocolul IP, traficul din rețelele interne este încapsulat în pachetele IP care sunt transferate între sediile companiilor prin rețelele diferitor provideri. Această încapsulare oferă atât **autentificarea** interlocutorilor prin metode moderne bazate pe certificate cu chei publice sau PSK (Pre-SharedKey), **integritatea** mesajelor prin sume de verificare (SHA, MD5 și HMAC), cât și **confidențialitatea** traficului prin criptare acestuia (DES, 3DES și AES). Prin aceste metode se blochează schimbul de date cu interlocutori neautorizați, se detectează alterarea informațiilor de către terțe persoane și se păstrează confidențialitatea informațiilor schimbate.

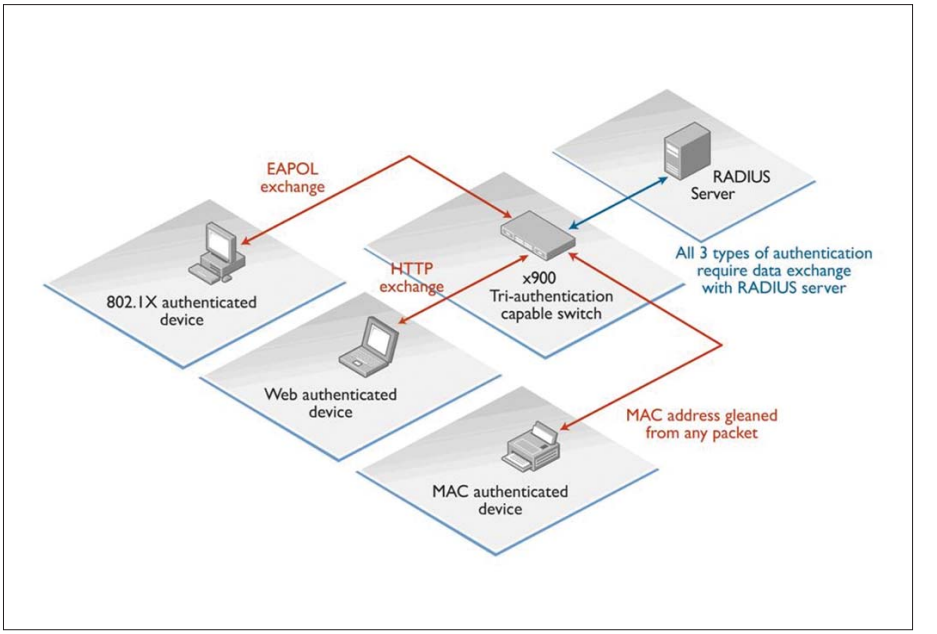
**Răspunsul Allied Telesis** la toate aceste deziderate ce privesc atacurile provenite din **exterior** vine prin gama de **Security Appliances** alcătuită din seriile de routere AR400 și AR700.

În ceea ce privește atacurile **interne**, acestea se bazează pe calculatoarele neprotejate corespunzător (firewall, antivirus) și pe accesul acestora în rețea fără o verificare prealabilă a conformității cu politica de securitate a companiei. Tehnicile de atac din interior sunt bazate în special pe programe de tip malware, care își găsesc calea în rețea fie prin angajați, contractori, fie prin vizitatori. Atacurile care se pot lansa din interior pot viza atât resursele interne (servicii – Web, FTP, E-Mail, echipamente de rețea – routere, switch-uri) cât și resursele externe.

**NAC** (Network Access Control) permite administratorilor de rețea să **impună centralizat** politica de securitate, mai degrabă decât să o „solicite/verifice" pentru fiecare echipament în parte.

Implementarea **NAC** pe echipamentele **Allied Telesis** are la bază standardul **TCG/TNC** (Trusted Computing Group – Trusted Network Connect)

*(continuare în pag 11)*



# OUTSOURSING-ul și CRIZA

DR. CĂLIN RANGU
CEO IIRUC Service

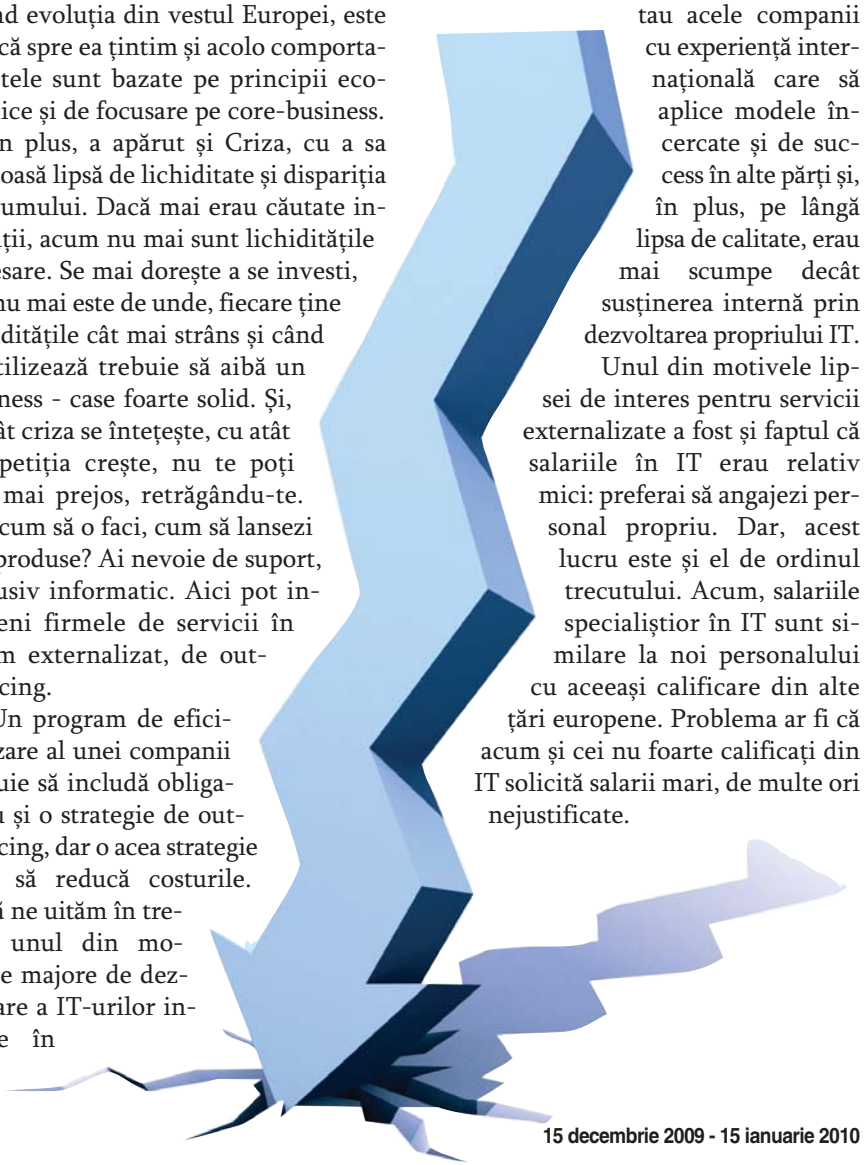
Timpurile actuale sunt pline de întrebări. Fiecare se așteaptă la tot ce e mai rău. Ești întrebat cât de afectat ești de Criză. Dar este atât de rău? De fapt, este o schimbare de paradigmă. Trebuie să ne repoziționăm și să evaluăm corect situația, pentru a beneficia de oportunitățile care apar.

Dacă luăm exemplul României, domeniul IT în sistemul bancar s-a dezvoltat accelelerat. Pe o piață emergentă, în care marginile sunt de câteva ori mai mari decât în țările stabile din vest, nu fondurile de investiții au fost problema. Băncile aveau destul de mulți bani, puteau păstra și pentru investiții, pentru o dezvoltare accelerată.

Înainte de apariția crizei, competiția crescuse foarte mult, marginile începeau să scadă, se căutau soluții de a fi mai eficienți, de a cheltui mai puțin, având în vedere că marginile descreșteau continuu. Pentru a păstra pentru acționari un profit cât mai bun, pe lângă acțiunile de eficientizare, investițiile erau căutate, mai bine le depreciai pe o perioadă de 3-5 ani, scăzând cheltuielile operaționale din anul în curs. Astfel, investițiile erau în continuare preferate. În plus, aveam de a face cu dorința românului de a avea. De ce aș lua IT-ul ca servicii dacă pot să am IT-ul meu, să construiesc un Data Recovery Centre propriu, cu propriul personal, cu care să mă mândresc. Dar, acest lucru începuse deja să se estompeze pe măsură ce au apărut modelele internaționale. Analizând evoluția din vestul Europei, este clar că spre ea țintim și acolo comportamentele sunt bazate pe principii economice și de focusare pe core-business.

În plus, a apărut și Criza, cu a sa faimoasă lipsă de lichiditate și dispariția consumului. Dacă mai erau căutate investiții, acum nu mai sunt lichiditățile necesare. Se mai dorește a se investi, dar nu mai este de unde, fiecare ține lichiditățile cât mai strâns și când le utilizează trebuie să aibă un business - case foarte solid. Și, cu cât criza se întețește, cu atât competiția crește, nu te poți lăsa mai prejos, retrăgându-te. Dar cum să o faci, cum să lansezi noi produse? Ai nevoie de suport, inclusiv informatic. Aici pot interveni firmele de servicii în regim externalizat, de outsourcing.

Un program de eficientizare al unei companii trebuie să includă obligatoriu și o strategie de outsourcing, dar o acea strategie care să reducă costurile. Dacă ne uităm în trecut, unul din motivele majore de dezvoltare a IT-urilor interne în companii non-IT a fost că nici nu a existat o piață reală de outsourcing, bazată pe principii competitive. Serviciile externalizate nu erau profesionalizate, nu existau acele companii cu experiență internațională care să aplice modele încercate și de succes în alte părți și, în plus, pe lângă lipsa de calitate, erau mai scumpe decât susținerea internă prin dezvoltarea propriului IT. Unul din motivele lipsei de interes pentru servicii externalizate a fost și faptul că salariile în IT erau relativ mici: preferai să angajezi personal propriu. Dar, acest lucru este și el de ordinul trecutului. Acum, salariile specialiștior în IT sunt similare la noi personalului cu aceeași calificare din alte țări europene. Problema ar fi că acum și cei nu foarte calificați din IT solicită salarii mari, de multe ori nejustificate.



Deci, patru factori concurează în acest moment asupra paradigmei schimbării abordărilor în domeniul dezvoltărilor și serviciilor IT:

1. Creșterea competiei pe piața de bancară, cu scăderea marginilor
2. Lipsa de lichidități datorită crizei financiare
3. Creșterea salariilor din IT uneori peste nivelul mediu european
4. Apariția companiilor de servicii IT profesionale, cu extindere și experiență europeană

Însă, nu sunt numai semne pozitive. Și firmele de servicii au nevoie de investiții. Înainte de a oferi soluții informatice către clienți, acestea trebuie să investească în dezvoltarea capacității de realizare a acelor servicii, deci dau de aceeași problema – finanțarea. Din această cauză, companiile solide, internaționale, pot accesa și dezvolta mai ușor infrastructuri de servicii, obținând mai ușor fondurile necesare decât inițiativele mici sau medii.

Globalizarea era prezentă înainte de Criză, dar aceasta o accentuează. Cei mici sunt înghițiți de cei mari. Cei mari se specializează, cedând zonele care până mai ieri erau utile dar acum mai mult îi încurcă către alții, tot mari. Piața serviciilor se globalizează. De exemplu, o firmă de servicii din România nu are nevoie să-și dezvolte propriul sistem de management al incidentelor, când poate lua servicii SaaS (Software as a Service) de la firma mamă și doar să le adapteze specificului național.

Piața serviciilor se specializează, deoarece devin tot mai scumpe și este nevoie de aplicarea principiilor economiei de scară. Nu te-a găsit Criza cu o rețea națională? Este mult mai greu să o creezi acum. Nu ai în firma de servicii o structură profesionalizată de dezvoltare software? Mai bine iei tu însuți servicii de la o astfel de firmă, tu păstrându-te acolo unde poți avea un avantaj competitiv. A cam trecut vremea celor care fac de toate. Criza a adus necesitatea de a ști să faci ceva bine, chiar foarte bine, pentru a putea rezista. Dacă o bancă face banking, serviciile IT ar trebui făcute de cei care știu să le facă. Dar, acest știut nu înseamnă semidoctism, ci specializare reală, costuri reduse, un mod de lucru eficient. Dacă o firmă oferă servicii IT, acestea trebuie să reducă cheltuielile pentru client, asigurând și un nivel de calitate mai bun. Este posibil ca serviciile să fie și ieftine și de calitate mai buna? Da, dacă firma este organizată pe procese, pe standarde care au avut success în lume, dacă se focalizează pe servicii specifice și nu dorește să facă de toate pentru toți. Având mai mulți clienți, prin utilizarea aceluiași personal și a același infrastructură, costul unitar către client scade. Organizarea pe standarde, de tip ITIL/ISO 2000, ISO 270001 etc asigură un nivel de calitate sustenabil și omogen. Implementarea într-o bancă a ITIL costă sume foarte mari și nu duce în mod direct la dezvoltarea produselor de business în sine. Pentru o firmă de servicii IT este obligatoriu de a implementa un mod de lucru pe procese. Deci, și costul și calitatea trebuie să fie elementele favorizante în a decide o externalizare. Iar Criza favorizează această abordare. ■

*(urmare din pag 9)*

pentru asigurarea interoperabilității cu soluțiile **NAC** oferite de vendori consacrați în domeniu precum **Microsoft** sau **Symantec**.

Orice implementare **NAC** de securizare a rețelei are la bază următoarele principii:

- blocarea (sau limitarea strictă) accesului în rețea în lipsa autentificării
- izolarea și remedierea echipamentelor autentificate, dar neconforme cu politica de securitate
- setarea nivelului de acces la resursele rețelei în funcție de identitatea echipamentului

Pentru punerea în aplicarea a principiilor de mai sus și aplicarea lor pentru toată varietatea echipamentelor care se conectează la rețea, **Allied Telesis** implementează în switch-urile cu management tip L2+ trei metode de autentificare și integrarea cu soluții **NAC** third-party. Cele trei metode de autentificare (ilustrate și în figura alăturată) sunt:

**• 802.1x**

Este o autentificare robustă, care permite accesul pe bază de parolă criptată sau pe bază de certificat, folosită pentru echipamentele ce implementează protocolul 802.1x (calculatoare personale, laptop-uri)

**• Web-based**

O autentificare des întâlnită, pe bază de user și parolă criptată (protocol HTTPs) adresată echipamentelor ce nu implementează protocolul 802.1x (ex. PDA), dar oferă browser WEB.

**• MAC-based**

Autentificare pe baza adresei MAC a dispozitivelor din mediul IT (ex. imprimantă, cameră video), care nu pot fi accesate grație metodelor de mai sus.

Allied Telesis a implementat interoperabilitatea NAC pe toate switch-urile L2+: Switchblade x908, familia x900, familia x600, seria 9900, seria 9400, seria 8000GS, seria 8600, seria 8500 și seria 8000s.

# Internet Security – ne îndreptăm către o zonă de phishing și șantaj corporativ mult mai targetat?

În pofida închiderii celor mai importante ISP-uri de spam din lume, cantitatea totală de mesaje spam a crescut considerabil, conform unui raport întocmit de nimeni altcineva decât Google. Compania binecunoscutului motor de căutare pe Internet a raportat recent că volumul de mesaje spam a fost cu 53% mai mare în al doilea trimestru al anului 2009 decât în primul trimestru. Se așteaptă ca lupta împotriva spammer-ilor să fie în continuare una de acțiune și reacțiune, atât timp cât furnizorii de securitate dezvoltă contramăsuri tot mai bune, îndepărtează gazdele malițioase și înregistrează câte o victorie pe ici, pe colo, ca cea a închiderii McColo; la rândul lor, băieții răi continuă să profite, pozând în inocenți și răspândind malware.

## Spam la superlativ

De curând, un membru al echipei de securitate al companiei Google, Amanda Kleha, a făcut câteva declarații interesante cu privire la această situație. Ea a declarat că McColo ISP, închisă în luna noiembrie a anului 2008, ar fi generat o scădere a circulației globale a spam-ului cu 70%. Totuși, în ultimele patru luni, volumul a crescut din nou la nivelele inițiale. 3FN, cunoscut și ca Pricewert, era un alt server de spam închis de către Federal Trade Commision (FTC) pe 4 iunie 2009, lucru ce a generat o scădere a volumului spam-ului cu aproximativ 30%, conform Amandei Kleha. Referitor la eveniment, aceasta a comentat: *„El a reprezentat, totodată, o invitație pentru spammer-ii oportuniști de a pune stăpânire pe piață."* Volumul spam-ului a crescut cu 14% față de nivelul observat la închiderea 3FN. Kleha a mai declarat că, recent, s-a observat faptul că spammer-ii utilizează tehnici retro de spamming, considerate de către organizațiile de securitate moarte și îngropate de mult. Aceste tehnici se bazează pe newsletter-uri ce conțin link-uri malițioase și care sunt trimise oamenilor cu conturi active de e-mail. De asemenea, sunt reutilizate și vechile tehnici de spam bazate pe imagini. Acest tip de spamming, la modă prin 2007, a cunoscut apoi un declin serios când vendorii de securitate și-au adaptat software-urile cu scopul de a combate aceste amenințări. Kleha a mai adăugat că reapariția vechilor tehnici de spamming poate însemna intrarea în domeniu a unor noi grupuri de spammer-i. Cu toate acestea, ea nu omite posibilitatea ca această practică să fie doar o testare a vechilor spammer-i pentru a afla care sunt limitele noilor tehnici de protecție antispam.

## Free Webmail - o nouă zonă de atac

Deoarece email-urile corporative și cele prin rețele plătite vin sub o mai bună protecție, utilizatorii devenind tot mai pricepuți, mesajele de phishing sunt direcționate către utilizatorii serviciilor de webmail gratuit. Anul acesta, Symantec a raportat o creștere a atacurilor îndreptate către acest sector. Noile mesaje vin sub deghizarea furnizorului de servicii și încearcă să obțină parolele, cât și listele de contact ale utilizatorilor. Datorită faptului că spammer-ii încearcă să ignore creșterile de volum pentru a exploata maximum de vectori posibil, McAfee a făcut câteva predicții despre tendințele viitoare ale acestui fenomen:

## Serviciile gratuite de web-hosting/ blogging vor fi tot mai des folosite în mod abuziv de către spammer-i

Faptul că oamenii au posibilitatea de a crea website-uri publice fără necesitatea autentificării în cazul achiziționării unor

nume de domenii ca Geocities, Blogspot și Live înlesnește munca spammer-ilor, dându-le ocazia să-și răspândească mesajul cu cheltuieli minime pentru resurse.

## Phishing și șantaj corporativ mult mai targetat

Software-ul malițios ce se răspândește în rețelele corporative și datacenter-ele financiare va fi tot mai des utilizat pentru a aduna informații sensibile, informații ce pot fi folosite pentru șantaj sau vândute pe piața neagră. Atacurile browser-based vor fi folosite tot mai mult din cauza securității slabe pentru a transfera datele sustrase. Breșele de securitate ale datelor confidențiale managerizate de parteneri sau companii subsidiare vor putea duce la o revizuire generală a practicilor de securitate.

## Un experiment ce ridică multe semne de întrebare

Un experiment „spear-phishing" întreprins de curând de un cercetător a condus la următoarele rezultate: majoritatea produselor și serviciilor importante de email corporativ au fost incapabile să detecteze o invitație LinkedIn falsă din partea lui „Bill Gates", care a „aterizat" cu succes în căsuțele de email ale utilizatorilor. Joshua Perrymon, CEO al PacketFocus, a trimis un email LinkedIn fals utilizatorilor din diferite organizații, ce fuseseră de acord să participe la acest test. El și-a putut strecura mesajul prin varietatea de produse și servicii de email, inclusiv prin instrumente smartphone de email. Cercetătorul a testat 10 combinații diferite de dispozitive, servicii, produse comerciale și open-source de securitatea email-ului, patru produse importante de email și trei brand-uri importante de smartphone.

Concluzia: problema este că majoritatea tehnologiei anti-phishing este construită pentru a împiedica atacuri la scară largă și nu pe cele mici, targetate și înșelătoare. Deși experimentul lui Perrymon a fost simplu și direct, rezultatul său a avut efectul unui duș rece asupra furnizorilor de securitate. El a ajutat la conștientizarea a cât de ușor este să furi informații de la o parte targetată, demonstrând cât de serioasă este problema și cât de ușor de realizat abuzul. Perrymon a declarat că experimentul a fost întreprins pentru a determina cât de eficiente sunt controalele de securitate ale email-ului în cazul diferitelor produse. Și, deoarece aceste atacuri sunt de tipul „social engineering", a mai adăugat el, „nu există o soluție reală. Lăsând la o parte realizarea de tehnologie PGP sau alte tehnologii de autentificare a email-ului – care nu sunt adoptate la scară largă – singura modalitate prin care un furnizor de securitate poate opri aceste mesaje să ajungă în căsuțele de email ale utilizatorilor este să găsească o cale de identificare a mesajelor înșelătoare, lucru foarte dificil de realizat. Este vorba despre un atac pe mai multe nivele, ce țintește lucruri diferite, prin urmare și foarte greu de oprit."

## De ce e necesar un software de filtrare pentru Internet?

Software-urile de filtrare pentru Internet vă dau posibilitatea de a controla conținutul afișat, de a bloca website-uri și a pune parole. Servicii puternice, precum filtrarea email-ului, blocarea popup-urilor și monitorizarea chat room-ului, sunt instrumente disponibile ce însoțesc software-urile actuale de filtrare pentru Internet, fiecare create pentru a proteja împotriva tacticilor agresive ale companiilor de pornografie online.

■ Teodor Nițu

## CE TREBUIE SĂ AVEŢI ÎN VEDERE LA ALEGEREA UNUI SOFTWARE DE FILTRARE PENTRU INTERNET

Deşi pe piaţa actuală nu există filtrul perfect pentru Internet, există totuşi câteva soluţii foarte bune ce pot răspunde necesităţilor dumneavoastră. Iată, prin urmare, care sunt criteriile de evaluare a acestor software-uri:

**Uşor de utilizat**
Cel mai important atribut al unui program de filtrare pentru Internet este design-ul uşor de folosit, lucru ce dă posibilitatea oricărei persoane, indiferent de nivelul de experienţă în computere, să instaleze şi să utilizeze cu uşurinţă filtrul la capacitatea sa maximă.

**Filtrare eficace**
Software-urile de filtrare de top oferă un bun echilibru între filtrarea materialului nedorit şi nefiltrarea unei cantităţi prea mari de conţinut. Un alt aspect important este posibilitatea de a customiza sensibilitatea filtrului în cazul fiecărui membru al familiei.

**Algoritmul de filtrare**
Cele mai bune programe de filtrare folosesc o combinaţie de tehnici de filtrare, inclusiv filtrare URL, filtrare „keyword" şi filtrare dinamică.

**Raportarea activităţii**
Cele mai utile software-uri de filtrare pentru Internet oferă rapoarte despre activitatea pe computer a fiecărui membru al familiei, şi anume website-urile vizitate, activitatea pe chat room, conversaţiile IM şi altele.

**Software Client-Server based**
Programele bune de filtrare oferă o platformă flexibilă, ce permite utilizatorilor să decidă dacă soluţia lor optimă de filtrare este de tipul client (home computer) based, server (Proxy or ISP) based sau o combinaţie a acestora.

**Filtrarea limbii străine**
Software-urile eficace de filtrare pentru Internet oferă posibilitatea de a filtra cuvinte problemă în diverse limbi. Unul din trucurile utilizate de adolescenţi pentru a păcăli filtrele pentru Internet este de a tasta într-o limbă străină echivalentul unui anume cuvânt.

**Filtrarea şi blocarea porturilor**
Programele de filtrare ar trebui să poată bloca sau filtra toate protocoalele de Internet importante, inclusiv accesul web, chat room-urile, email-ul, reţelele peer-to-peer, ferestrele de bulletin boards şi pop-up.

CĂTĂLINA CHICU,
ŞEF DEPARTAMENT
DEZVOLTARE PRODUSE NOI
ALPHA BANK ROMANIA

# Directiva Serviciilor de Plăți – Stadiul transpunerii și probleme de aplicare

Directiva Serviciilor de Plăți 2007/64/CE, transpusă în România prin Ordonanța de Urgență nr. 113/2009, ar fi trebuit să se aplice în cele 30 de State Membre ale Spațiului Economic European începând cu data de 1 noiembrie 2009. Câte țări au respectat acest termen? Care a fost modul de abordare a transpunerii? Cum a decurs dialogul între bănci și autorități? Ce obstacole au rămas nerezolvate? Unde se situează România? Articolul va explora aceste întrebări, în căutarea de răspunsuri.

## Stadiu transpunere

Conform informațiilor publicate de Comisia Europeană în luna noiembrie, doar 17 țări au respectat termenul de transpunere a Directivei; 7 țări au anunțat că vor finaliza transpunerea până la sfârșitul anului 2009, în timp ce 3 țări intenționează aplicarea Directivei în primul semestru din 2010. Situația completă a stadiului transpunerii este prezentată în următorul tabel:

Transpunerea Directivei în legislația națională – situația la 01.11.2009 *(sursa: Comisia Europeană)*

| State Membre care au finalizat transpunerea Directivei până pe 01.11.2009 | State Membre care intenționează finalizarea transpunerii Directivei până la sfârșitul anului 2009 | State Membre care vor aplica Directiva în prima jumătate a anului 2010 |
|---|---|---|
| AT, BG, CZ, DK, DE, ES, FR, HU, IE, IT, LU, MT, NL, PT, RO, SI, UK | EE, EL, LV, LT, PL, CY, SK | BE, FI, SE |

În Belgia, de exemplu, proiectul de lege a fost finalizat la timp, dar autoritățile au prevăzut o perioadă de grație de 3 luni pentru a permite implementarea în instituții. În Grecia, adoptarea legii a fost tergiversată de alegeri anticipate. În Finlanda, proiectul de lege a fost adoptat în decembrie 2009, urmând ca Titlul II să se aplice din ianuarie 2010 și Titlurile III și IV din luna mai 2010. În Suedia încă se lucrează la proiectul de lege, urmând ca acesta să fie adoptat în februarie 2010 și aplicat din aprilie 2010.

Asociația Suedeză a Băncilor a publicat un ghid cu recomandări de interpretare și aplicare a prevederilor Directivei. Ghidul va fi utilizat de bănci până la finalizarea transpunerii naționale a Directivei. Grupul de experți al European Banking Industry Comitee (EBIC) a inițiat discuții cu toate autoritățile naționale ale țărilor cu transpunere întârziată, în scopul evaluării posibilității elaborării și adoptării unui ghid similar modelului suedez.

## Incertitudini

Experții europeni au prezentat o serie de incertitudini privind aplicarea corectă a


prevederilor Directivei în cazul plăților transfrontaliere. În primul rând, nu se știe cum vor fi procesate plățile inițiate din și către țările "întârziate", existând riscuri reale de executare eronată.

O altă incertitudine este legată de SEPA Direct Debit (SDD). O dată cu intrarea în vigoare a Directivei, a fost lansată și schema SDD. Schema include două sub-scheme: SDD Core și SDD B2B. Varianta Core este utilizată de consumatori, varianta B2B – de persoane juridice. Având în vedere că Directiva reprezintă cadrul legal pentru schemele SEPA, nu se știe cum va putea fi utilizată schema SDD de băncile din țările care nu au transpus Directiva. Ca mod de abordare al proiectului însă nu ar fi o noutate, deoarece și schema SEPA Credit Transfer (SCT) a funcționat timp de aproape 2 ani fără cadru legal. Tot aici trebuie subliniat faptul că țările care au decis să aplice Directiva în egală măsură microîntreprinderilor și consumatorilor, nu vor putea utiliza schema SDD B2B pentru microîntreprinderi.

*(continuare în pag. 18)*

# INSTITUTUL BANCAR ROMÂN

## CURSURI SCURTE

### 1. ABC BANCAR

19-20.02.2010, orele 9 -15

**Obiectiv** - de a prezenta personalului care lucrează în sistemul financiar-bancar o imagine de ansamblu a sistemului bancar şi a activităţii unei bănci comerciale.

**Audienţa** - persoanele nou angajate în instituţiile de credit

### 2. ACTIVITATEA DE CASIERIE -

20 februarie 2010, orele 9 - 16.

**Obiective** - Formarea de competenţe şi abilităţi în domeniul operaţiunilor de casierie pentru personalul bancar. Programul cuprinde acţiunile şi activităţile desfăşurate în cadrul Serviciului Casierie, obligaţiile şi responsabilităţile casierilor, elemente de legislatie şi risc, precum şi activităţi conexe.

**Tematică**

- Organizarea Serviciului Casierie (păstrarea numerarului, reguli de securitate, responsabilităţile deţinătorilor de chei şi sigilii, accesul în Tezaur);
- Descrierea pe scurt a principalelor operaţiuni care pot fi efectuate de Serviciului Casierie; (deschiderea casei operative, relaţia cu Tezaurul, operaţiuni cu numerar, schimburi valutare, operaţiuni cu carduri (ATM / POS), certificate de depozit, cecuri de călătorie, operaţiuni Western Union);
- Depunerile şi retragerile de numerar în lei şi valută, cu respectarea legislaţiei privind operaţiunile în valută, cunoaşterea clientelei şi spălarea banilor;
- Operaţiunile de schimb valutar (casa de schimb valutar), cu respectarea legislaţiei privind cunoaşterea clientelei şi spălarea banilor;
- Depistarea falsurilor. Elemente de siguranţă ale bancnotelor. Modul de lucru în cazul depistării unui fals ;
- Operaţiunile efectuate la închiderea zilei de lucru (reconcilieri, verificări, numărarea şi împachetarea bancnotelor şi monedelor, inchiderea casei operative, remiteri către Tezaur);
- Remiterile şi alimentările către/de la alte sucursale ale bancii, alte banci sau BNR;
- Rapoarte, registre, formulare, raportări .
- Operaţiunile cu carduri*
- Certificatele de depozit*
- Cecurile de călătorie*
- Operaţiunile Western Union*
- Clienţii băncii, relaţia casierilor cu clienţii şi atragerea de noi clienţi

** Aceste subiecte pot fi dezvoltate sau restrânse în funcţie de cerinţe.*

### 3. TRECEREA DE LA BUSINESS CONTINUITY PLANNING LA BUSINESS CONTINUITY MANAGEMENT-

29.01.2010, orele 9 - 17:30

**Audienţa**

- planificatori pentru recuperarea în caz de dezastru
- manageri de proiect
- manageri de unităţi bancare
- senior manageri
- specialişti IT
- toate persoanele care au ca obiectiv sau ca responsabilitate creşterea eficienţei şi capabilităţilor de business continuity în organizaţia din care fac parte

**Conţinut**

- Revizuirea conceptelor
- Înţelegerea impactului schimbărilor din organizaţie asupra Business Continuity Management
- Integrarea Business Continuity Management în ciclul de viaţă al proceselor de business
- Stabilirea cerinţelor şi standardelor de Business Continuity
- Mentenanţa documentaţiei
- Training şi testare
- Indicatori de performanţă

## CURSURI LA DISTANŢĂ

**cursuri NOI, lansare 15 martie 2010**

Relaţii id@ibr-rbi.ro,

Înscrieri până la 01.03.2010

### 1. COMUNICARE ŞI NEGOCIERE

**Tematica pachetului de curs**

- Introducere în tehnicile de comunicare
- Comunicarea internă
- Rapoarte, rezumate şi note
- Referate şi mesaje
- Corespondenţa de afaceri
- Impactul tehnologiei informaţiei asupra comunicării
- Telefonul - instrument de comunicare
- Şedinţe - avantaje şi dezavantaje
- Prezentările publice
- Interviul
- Tehnici de negociere
- Tehnici de vânzări
- Recapitulare

### 2. FINANŢAREA IMM-URILOR ŞI A MICROÎNTREPRINDERILOR

**Tematica pachetului de curs**

- Întreprinderile mici şi mijlocii
- Capitalul - Dimensiune, structură, rotaţie
- Creditul - Principala sursă de finanţare a IMM
- Planul de afaceri
- Garanţia creditelor
- Subvenţiile şi programele de finanţare din fonduri europene

**GRUP ŢINTĂ**

persoane cu atribuţii în finanţarea întreprinderilor mici şi mijlocii din cadrul societăţilor bancare, a IFN-urilor sau persoane juridice/fizice autorizate interesate.

### 3. MANAGEMENTUL PROIECTELOR DE INVESTIŢII

**Tematica pachetului de curs**

- Proiectul de investiţii - componenta cheie a deciziei de investiţii
- Valoarea unui proiect de investiţii
- Analiza proiectelor investiţionale în mediul cert
- *Studiu de caz*: Impactul modului de finanţare asupra evaluării proiectelor investiţionale
- *Studiu de caz*: Evaluarea unui proiect de investiţii cu finanţare eşalonată în timp
- *Studiu de caz*: Elaborarea planului de finanţare în vederea adoptării unui proiect de investiţii
- Analiza proiectelor investiţionale în mediul probabilistic
- *Studiu de caz*: Analiza senzitivităţii unui proiect de investiţii
- Tratarea impactului inflaţiei asupra proiectelor de investiţii
- Tratarea impactului crizei financiare asupra proiectelor de investiţii

### 4. TRANZACŢIILE CU NUMERAR ÎN SISTEMUL BANCAR -

**Tematica**

- Organizarea tezaurului
- Tranzacţii numerar cu alte instituţii
- Organizarea casieriei
- Tranzacţii în numerar cu clienţii
- Deschiderea şi închiderea casieriei, procesarea numerarului, reconcilieri
- Formulare, registre, rapoarte
- Clienţii, politica de cunoaştere a clientelei
- Elemente de risc în tranzacţiile cu numerar
- Rolul şi responsabilităţile casierului. activităţi conexe pentru casieri

# Radiografia crizei mondiale

CĂTĂLINA CHICU,
ŞEF DEPARTAMENT
DEZVOLTARE PRODUSE NOI
ALPHA BANK ROMANIA

Sfârşitul de an marchează încheierea unui ciclu economic, fundamentând necesitatea de a privi înapoi, de a elabora statistici, de a trage concluzii. Evenimentele din ultimii ani sunt de importanţă istorică în economia mondială. Situaţia economică globală cu impact la nivel naţional generează ajustări radicale în strategiile de risc, de finanţare şi de dezvoltare la nivel de instituţie.

Care au fost cele mai importante evenimente financiar-bancare din aceşti doi ani de criză? Ce a marcat trendul economic? Care sunt soluţiile? Articolul încearcă să efectueze o radiografie generală a crizei economice mondiale, utilizând ca surse principale de informaţii publicaţiile "GTnews", "Financial Times" şi "Frankfurter Allgemeine Zeitung".

## Cum a început?

Pe 18 februarie 2008 banca engleză Northern Rock este naţionalizată, după ce s-a decis că cele două oferte de preluare nu ofereau suficientă valoare plătitorilor de taxe. În martie 2008, Bear Stearns este cumpărată de JPMorgan Chase. În septembrie, după căutări frenetice de cumpărători, Lehman Brothers devine cea mai mare bancă de investiţii ce intră în faliment. Urmează un lanţ întreg de fuziuni, achiziţii şi naţionalizări.

## Ce strategii au abordat ţările afectate?

În octombrie 2008 **Germania** aprobă un plan de restabilire a lichidităţii şi de injectare de capital în sectorul bancar în valoare totală de 470 mld. euro. Planul **Franţei** se ridică la 340 mld. euro. **Olanda** propune un plan de salvare de 199 mld. euro. **Austria** aprobă un pachet similar în valoare de 85 mld. euro. **Spania** pune deoparte 100 mld. euro, iar **Portugalia** 20 mld. euro. **Italia** a promis băncilor că le va aloca atâtea fonduri, câte vor fi necesare. **Rusia** aprobă un plan în valoare de 86 mld. dolari pentru a ajuta băncile lovite de îngheţarea creditării. 50 mld. dolari din aceşti bani au fost puşi la dispoziţia băncilor şi firmelor pentru refinanţarea creditelor externe. **Marea Britanie** aprobă un plan de salvare în valoare de 400 mld. lire. **Ţările nordice** declară disponibilitatea de a ajuta **Islanda** în lupta contra crizei. Fondul Monetar Internaţional (FMI) acordă **Ucrainei** un credit de 16,5 mld. dolari pentru resuscitarea economică. Reprezentanţii **G7** (SUA, Japonia, UK, Germania, Franţa, Italia şi Canada) s-au întâlnit la Washington şi au emis un plan cu cinci măsuri decisive pentru deblocarea creditării.

În noiembrie 2008 Banca Centrală Europeană (BCE) acordă **Ungariei** o linie de credit de 5 mld. euro, urmând ca în aceeaşi lună FMI, Uniunea Europeană (UE) şi Banca Mondială să acorde ţării un credit de 25 mld. dolari. Statul **suedez** garantează toate datoriile noi ale băncilor până în 117 mld. lire. **Japonia** adoptă un plan de stimulare economică de 50 mld. dolari şi creşte cotizaţia la FMI în scopul susţinerii celor mai afectate ţări. **China** adoptă un plan de dezvoltare economică în valoare de 586 mld. dolari. În aceeaşi lună, FMI aprobă acordarea unui credit *standby* pentru **Pakistan**, evitându-se astfel *default*-ul ţării din cauza datoriilor externe. **Comisia Europeană** anunţă un plan de recuperare în valoare de 200 mld. euro cu scopul de a salva milioane de locuri de muncă din Europa. Planul urmăreşte şi consolidarea încrederii consumatorilor în sistemul bancar.

În decembrie 2008 **Franţa** adoptă încă un plan de stimulare a economiei în valoare de 26 mld. euro. Fondurile sunt destinate în special dezvoltării întreprinderilor mici şi sectorului de construcţii. **India** creşte pachetul de 56 mld. dolari cu încă 4 mld. dolari, bani destinaţi să susţină stimularea exporturilor, sectorului imobiliar

și a infrastructurii. Guvernul **japonez** dublează valoarea planului de restabilire economică la 171 mld. lire. **Irlanda** recapitalizează băncile listate la bursă cu suma de 9 mld. lire.

În ianuarie 2009 **Spania** devine prima țară care pierde *rating-ul* de triplu A de la agenția S&P. În încercarea de a evita recesiunea, **Danemarca** oferă credite în valoare de 13 mld. euro pentru recapitalizarea băncilor și pentru reactivarea creditării. **Germania** comunică completarea planului de stimulare economică cu 50 mld. euro. Rata numărului de falimente în rândul companiilor **japoneze** crește cu 24% față de aceeași perioadă a anului trecut. **Marea Britanie** anunță noi măsuri de încurajare a activității de creditare. Băncii Naționale i se atribuie un nou rol, ce îi permite achiziționarea de active în valoare de 50 mld. lire direct de la firme. Guvernul **francez** alocă 6 mld. euro pentru finanțarea sectorului auto. **Islanda** este paralizată de criza economică și de tumultul politic intern. Rata șomajului se situează la cel mai înalt **nivel** de după al doilea război mondial. SUA adoptă planul de revigorare economică *Troubled Asset Relief Program* (TARP) în valoare de 819 mld. dolari și deblochează 350 mld. dolari pentru utilizare imediată.

În februarie 2009, în **China** exportul scade cu 17,5% iar importul cu 43% comparativ cu aceeași perioadă a anului precedent. **Australia** adoptă un plan în valoare de 27 mld. euro. Președintele **SUA** anunța plafonul de 500.000 dolari pentru firmele care au nevoie de ajutor de la stat.

În martie 2009 Banca Mondială acordă 2 mld. dolari **Indoneziei**. Banca **Angliei** tipărește 75 mld. lire bani noi pentru a fi pompați în economie. Conform reprezentanților Băncii **Angliei**, această măsură "neortodoxă" era inevitabilă, după ce rata de referință a fost diminuată până aproape de zero. Banca Națională a **Japoniei** anunță disponibilitatea de a acorda 10 mld. dolari băncilor comerciale sub formă de credite subordonate. **SUA** anunță planul de achiziționare de active toxice ale băncilor în valoare de 1 trilion dolari. **România** primește un împrumut de 20 mld. euro, din care 12,95 mld. euro de la FMI, 5 mld. de la UE și 1,1 mld. de la Banca Mondială.

În aprilie 2009 la Londra are loc întâlnirea **G20**, în care se decide alocarea a 1 trilion dolari pentru criza financiară globală. **FMI** primește suplimentar 750 miliarde dolari în scopul susținerii statelor puternic lovite de criză. În plus, **G20** aprobă următoarele măsuri: alocarea a cca. 250 mld. dolari pentru intensificarea comerțului mondial; consolidarea reglementărilor fondurilor mutuale și a agențiilor de *rating*; adoptarea unei abordări comune de curățare a activelor toxice; acordarea de 50 mld. dolari ca ajutor pentru țările sărace. **Mexic** primește de la FMI o linie de credit de 47 mld. dolari. Exportul din **Marea Britanie** scade cu 30% comparativ cu aceeași perioadă a anului precedent.

În mai 2009 **Japonia** oferă 100 mld. dolari asistență financiară țărilor lovite de criză din Asia. **Germania** adoptă schema "bad bank", pentru a permite băncilor înlăturarea activelor toxice din bilanțuri. Conform acestui plan, băncile pot opta să schimbe activele toxice pe obligațiuni guvernamentale garantate. Economiile celor 16 țări din **zona Euro** scad în medie cu 2,5%, cel mai important factor de declin fiind scăderea abruptă a exporturilor din **Germania**. Producția auto din **SUA** scade într-o singură lună cu 55%.

În iunie 2009, în **China** exportul scade cu 26% iar importul cu 25%, comparativ cu aceeași perioadă a anului precedent. În **Japonia** exportul se diminuează cu 41%. La întâlnirea **G8** se concluzionează că cele mai mari economii mondiale încep să se stabilizeze, dar încă se confruntă cu riscuri majore. Consolidarea este justificată de creșteri bursiere, diminuarea fluctuației ratelor de dobândă de referință și redobândirea încrederii consumatorilor în sistemul financiar. FMI estimează că economia **SUA** va crește în 2010 cu 0,75% față de prognoza anterioară de 0%. **BCE** acordă credite în valoare de 442,2 mld. euro pentru 12 luni la o dobândă de referință de 1%.

În iulie 2009 Camera de Comerț a **Marii Britanii** anunță că vârful recesiunii a fost depășit. Un studiu efectuat de BBC asupra 5.600 companii reflectă începutul revenirii economice. **China** înregistrează o creștere de 7,9%, cifră ce se situează peste estimările inițiale. **SUA** emite un act legislativ, conform căruia fondurile mutuale cu active de peste 30 mln. dolari vor fi înregistrate și administrate de *Securities and Exchange Commission*. **Sri Lanka** primește un credit de 2,5 mld. dolari de la

FMI. **SUA** prezintă raportul TARP cu cele mai negre scenarii posibile ce ar putea influența economia țării, generând o expunere totală de 23,7 trilioane dolari. **FMI** anunță planificarea următoarelor măsuri: creșterea creditării până în 2014; suspendarea dobânzilor pentru unele credite acordate țărilor sărace; vinderea unei părți din rezervele de aur pentru obținerea de fonduri pentru credite.

În august 2009 Banca **Angliei** decide tipărirea și injectarea în economie a încă 50 mld. lire. Se votează unanim menținerea dobânzii de referință la 0,5%. **BCE** decide menținerea dobânzii de referință la 1%, cu toate că, atât economia **Germaniei**, cât și cea a **Franței** înregistrează creșteri de 0,3% în trimestrul doi. Economia **Italiei** scade doar cu 0,5%, mult mai puțin decât era prognozat inițial. **Hong Kong** revine din recesiune, înregistrând o creștere de 3,3% în trimestrul doi. **Japonia** înregistrează prima creștere economică de după recesiune (0,9%). În aceeași perioadă, economia Mexicului scade cu 10,3%. Banca Națională a **Israelului** este prima care decide creșterea dobânzii de referință de la 0,5% la 0,75%. **FMI** anunță că guvernele au cheltuit peste 10 trilioane dolari pentru diminuarea efectelor generate de criza mondială.

În septembrie 2009 Banca Națională a **Japoniei** decide păstrarea ratei de referință la 0,1% cu mențiunea că economia dă semne clare de revigorare. Președintele **FED** spune că "recesiunea a ajuns la final, dar probabil că economia va fi slabă în următoarea vreme". Președintele Bundesbank menționează că economia **Germaniei** "și-a oprit căderea liberă, dar recuperarea va dura". La *summit-ul* de la Pittsburg, **G20** a decis să-și asume noul rol de organism permanent de coordonare a economiei mondiale.

În octombrie 2009 **Australia** crește dobânda de referință de la 3% la 3,25%, fiind prima țară din G20 care întreprinde o astfel de acțiune în această perioadă. Cifrele comerciale ale **Chinei** reflectă îmbunătățirea economiilor din restul lumii: atât exportul cât și importul marchează cea mai mică scădere din ultimul an (15% respectiv 3,5%). **Marea Britanie** continuă să fie în recesiune, înregistrând o scădere de 0,4% în perioada iulie-septembrie. După patru trimestre de recesiune, economia SUA înregistrează o creștere a PIB-ului de 3,5%.

În noiembrie 2009 **Australia** crește dobânda de referință de la 3,25% la 3,5%. **FED-ul** semnalizează că în următoarele 6 luni intenționează să mențină dobânda de referință aproape de zero. Banca **Angliei** pompează încă 25 mld. lire în economie. Extensia programului de recuperare economică a Marii Britanii se ridică astfel la 200 mld. lire. **China** estimează că va atinge obiectivul de 8% creștere a PIB-ului în 2009. Statele din **Zona Euro** înregistrează o creștere medie de 0,4% în perioada iulie-septembrie. **Germania** și **Franța** înregistreaza creșteri economice timp de două trimestre consecutive, confirmând astfel ieșirea din recesiune. Economia **Japoniei** crește în trimestrul trei cu 4,8%. **Rusia** înregistreaza o creștere economică de 13,9% între iulie și septembrie. Tot în trimestrul trei, economiile celor 30 de țări din Organizația pentru Cooperare și Dezvoltare Economică (**OCDE**) cresc în medie cu 0,8%.

În decembrie 2009 Banca **Japoniei** anunță noi măsuri de luptă cu deflația: injectarea a 10 trilioane yeni în economie prin oferirea de credite ieftine pe termen scurt băncilor. Președintele **SUA** anunță că programul TARP adoptat în ianuarie a fost "mult mai ieftin", astfel încât banii rămași vor fi folosiți pentru diminuarea deficitului bugetar și crearea de locuri de muncă. **Australia** crește rata dobânzii de referință de la 3,5% la 3,75%. Pentru prima dată după șapte luni, **zona Euro** înregistrează o creștere a prețurilor de consum (+ 0,6%). **Ucraina** solicită FMI 2 mld. dolari sub formă de credite de urgență pentru achitarea datoriilor externe și evitarea pericolului „contagierii" celorlalte state vulnerabile din regiune.

Federația Bancară Europeană (FBE) a publicat în luna noiembrie 2009 raportul *Overcoming the crisis and moving beyond*, în care sumarizează problemele generate de criză. Conform acestui raport, guvernele din zona Euro au alocat aproximativ 35% din PIB pentru măsurile de susținere a sectorului financiar. Raportul include propuneri de soluții de ieșire din criză și recomandările FBE pentru integrarea pieței europene de servicii financiare. ■

*(urmare din pag. 14)*

## Transpunerea în România

Băncile din România, realizând importanța Directivei, au demarat activitatea de identificare a impactului încă de la începutul anului 2009, când nu exista proiect de lege pentru Titlul III și IV. În faza inițială, băncile au fost puse în situația de a jongla cu ipoteze și cu posibile elemente de impact, deoarece nu se știa cum va fi textul de lege final. Pe 12 octombrie 2009 a fost publicată OUG 113/2009, băncile având la dispoziție jumătate de lună pentru implementarea acesteia. Cea mai mare problemă în procesul de transpunere, în toate cele 30 de țări, a fost interpretarea Directivei. Unii termeni permit interpretări multiple, chiar dacă sunt definiți în textul Directivei. Probabilitatea de interpretări eronate generează riscuri. Modul de soluționare în diferite țări a fost diferit:

- Unele țări au emis un ghid cu explicații pentru termenii interpretabili, în baza căruia se va evalua și conformitatea. Băncilor li s-au creat condiții să-și adapteze sistemele, procedurile și contractele în timp util. Una dintre țările care a adoptat această abordare a fost Marea Britanie.
- În alte țări, problemele de interpretare au fost soluționate prin dialog.
- În țările cu transpunere întârziată, unele bănci au decis să aplice Directiva, total sau parțial, asumându-și riscuri de interpretare.
- În alte țări nu a existat dialog între instituțiile responsabile de transpunere națională și bănci privind problemele de interpretare. Printre aceste țări se numără și România, deoarece încercarea de a dialoga cu autoritățile naționale a eșuat. În mod evident s-a decis ca dialogul privind interpretarea să fie lăsat în seama băncilor și a clienților, ceea ce, în final, este în defavoarea relației de afaceri bancă-client.

În concluzie, se poate constata o eterogenitate în modul de transpunere a Directivei în legislațiile naționale. Rămâne de văzut cum își va produce efectele Directiva, dacă va aduce cu sine armonizare și standardizare și dacă va reuși integrarea pieței unice de plăți. ■

# Danubius - Exim

*urează tuturor colaboratorilor și partenerilor*

*Sărbători fericite*

*și Un An Nou plin de realizări!*


**DANUBIUS EXIM**
Str. Vasile Gherghel nr.12, sector 1, București
Tel: 021/ 224.55.24; Fax: 021/ 224.22.28
CALL CENTER: 021 200 6000
www.danubius-exim.ro
www.ingenico.com
office@danubius-exim.ro

MARCELINA JOAVINĂ

# Prezență și viitor în criza financiară

## Colaj de date și impresii

*(continuare din numărul anterior )*

O caracteristică a sistemului financiar care a evoluat de-a lungul anilor este identificarea cu precizie a entității care preia riscul. În trecut, ***fluiditatea piețelor venea de la investitori şi speculatori. Aceştia riscau banii proprii.*** În 2007, creșterea continuă a riscului instituțional, suportat de propriul capital (și îndatorare) a transferat o mare parte din acest risc către sistemul bancar însuși. ***Intermediarii financiari au devenit deținători principali de risc.***

*Cu această nouă axiomă la drum,*

### Cât de serioasă va fi restrângerea creditului?

Tot căutând date suport, necesare pentru a interpreta situația și a înțelege propunerile specialiștilor, am găsit estimări furnizate de către Boston Consulting Grup, care prevedea că pierderile instituțiilor financiare vor atinge 1500 miliarde de dolari, deoarece pierderile aferente împrumuturilor acordate persoanelor fizice și companiilor pot chiar să depășească pierderile ipotecare. La un raport active/capital de 12.5/1, această pierdere va însemna o reducere în capacitatea de creditare de 19 000 miliarde dolari – o contractie neta de 7% a nivelului actual de creditare. Dat fiind că în medie sunt necesari 4 dolari în credit pentru fiecare dolar de creștere a PIB, o astfel de contracție va duce la o încetinire economică globală masivă, reducând în mod direct creșterea globală cu aproape 2 puncte procentuale – înainte de orice alte efecte secundare (sau terțiare).

*Și atunci, ca un corolar, putem vorbi de:*

### Sfârşitul Cererii susținută prin Credit?!

Cum arăta evoluția indicatorilor relevanți în Statele Unite la începutul crizei?

Pe de o parte, am asistat la diminuarea drastică a creditului în timp ce, aparent paradoxal, se generalizează creșterea pe termen lung a îndatorării consumatorilor din Statele Unite.

De ani de zile, consumatorii americani trăiesc peste posibilitățile lor financiare.

De exemplu, între 1972 și 2008 îndatorarea a crescut de la 60% la 120% din PIB. Creșterea explozivă a creditului ipotecar a fost generată de consumatori, care s-au folosit de creșterea în prețurile imobiliare pentru a se angaja în credite de consum și mai mari. Accesul practic nelimitat la creditele ieftine a fost un factor cheie în creșterea economiei SUA și a economiei mondiale, având în vedere rolul SUA ca motor al expansiunii economice globale. Consumul gospodăriilor, reprezentând un procent nesustenabil de 70% din PIB-ul SUA, a avut ca și consecință reducerea ratei de economisire la puțin peste zero, reprezentând cel mai redus nivel de la Marea Criză din 1929.

Însumând la creditul gospodăriilor, creditul corporatist și guvernamental, asistăm la o escaladare a volumului de credit la 350 procente raportat la PIB, iar pentru că instituțiile financiare au apelat la rândul lor la credit pentru a-și creste veniturile, se înregistrează și o creștere a creditului în sectorul financiar de 16 000 miliarde dolari în 2007. Mai adăugați aici că firmele au folosit creditarea pentru a-și finanța expansiunea iar guvernul pentru a-și finanța cheltuielile, menținând taxele la nivel scăzut.

Chiar cu riscul unui truism financiar, trebuie să menționăm o dată în plus: creditul nu poate crește infinit mai repede decât veniturile. Toți participanții la acest fenomen au trebuit să reducă îndatorarea.

*Dar, dincolo de o pictură macroeconomică,*

### Ce înseamnă Criza pentru Economia Reală?

Combinația dintre un credit puțin accesibil și o cerere redusă a lovit chiar și în companiile sănătoase, conducand la un cerc vicios prin limitarea investițiilor și având ca și consecință ulterioară stagnarea economică.

Sectorul financiar a avut o contribuție mai mica în PIB, pentru că a trebuit să renunțe (parțial) la activele problematice și

nu mai are apetit pentru împrumuturi, nici chiar către clienți solvabili.

În acest sens, băncile vor diferenția clienții de calitate față de ceilalți (pe care îi vor finanța foarte selectiv).

*QED: trebuie să facem față unui mediu aspru de recesiune, și atunci,*

## Cât de severă va fi recesiunea?

Va fi scurtă, datorită flexibilității economiei SUA și mult promisei intervenții rapide a guvernului American? Se va dovedi această intervenție una de succes?

Nu prea, întrucât dacă definim succesul ca limitarea recesiunii la SUA, e clar că acest obiectiv nu a fost atins, deși firmele s-au străduit să facă față aversiunii la risc și standardelor ridicate ale băncilor.

*Deci, nu mai este credibil un scenariu de recesiune ușoară,*

## În atare situație ce zic experții?

De exemplu, FMI a studiat mai bine de 100 recesiuni petrecute în lume în trecut și a ajuns la concluzia că recesiunile generate de crize financiare sunt mai grave și durează mai mult decât altele. În actuala situație, a expunerii datorate unui foarte ridicat nivel de creditare, combinată cu balonul ipotecar și cu creditarea exagerată a consumului, avem toate motivele unei serioase îngrijorări.

Realist, companiile trebuie să fie pregătite pentru o recesiune serioasă, în care băncile vor falimenta în continuare, cererea scazută a clienților va persista și țările dezvoltate vor intra în recesiune. Deși creșterea non-export în țările în curs de dezvoltare va fi oarecum protejată, creșterea bazată pe export va fi înjumătățită.

*Iar dacă discutăm de plan de acțiune,*

## Care sunt cele mai probabile situații la care firmele trebuie să facă față?

**1. Acces redus la fonduri**

Trezorierii firmelor fac față tot mai greu nevoilor de finanțare pe termen scurt. Datorită ratelor de dobandă interbancare ridicate, băncile reduc liniile de credit și renegociază termenii împrumuturilor. Piața titlurilor comerciale s-a contractat cu 11% și securizarea titlurilor este practic închisă pentru mulți creditori. Companiile vor trebui să-și refacă strategiile de finanțare și să se asigure că pot să-și reînnoiască creditele, ceea ce va fi destul de greu în condițiile unui gap între investiții și surse proprii de 327 miliarde euro numai în Europa.

Ca o consecință, băncile vor rămâne foarte conservative în practicile de creditare și vor competiționa pentru clienți cu profil de creditare foarte bun.


**2. Cost ridicat al capitalului**

Investitorii pot cere premii de risc tot mai ridicate, astfel că asistăm la creșterea spread-ului de dobandă (diferența între dobanda cerută la împrumuturi față de dobanda la titlurile non-risk).

**3. Piața de capital slabă**

Scăderea indicilor bursieri face mai puțin atractivă finanațarea prin piața de capital, așa că firmele vor apela la forme alternative; fonduri de Private Equity sau fondurile marilor investitori, care sunt la rândul lor scumpe.

**4. Reducere de cash flow**

Afectarea companiilor de încetinirea economică va fi directă prin reducerea cantităților de bunuri cu până la – 20% și în plus o reducere de prețuri de -10%.

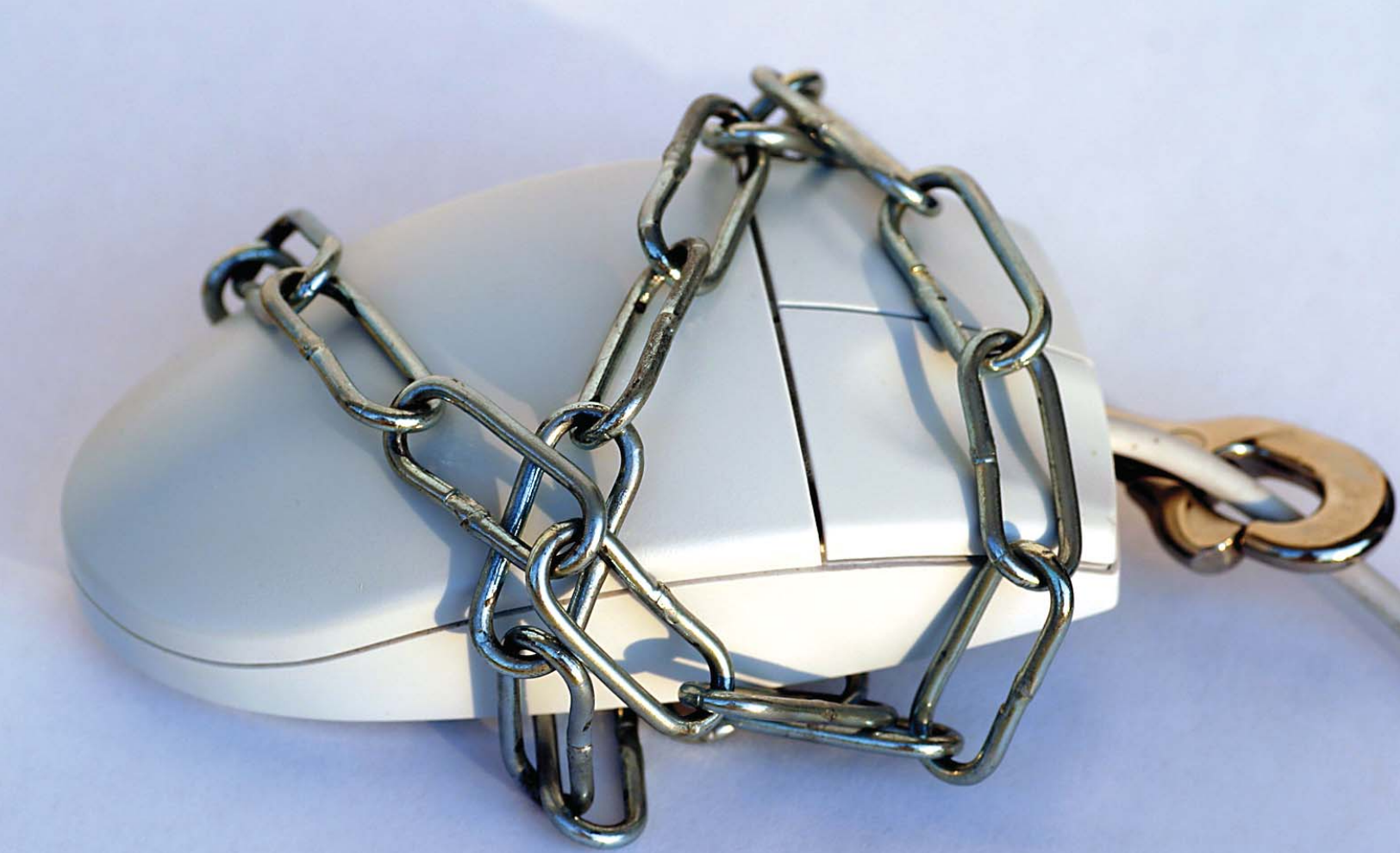
**5. Pierderi din credite**

Vânzarea pe credit va avea drept efect imediat pierderi datorită falimentelor clienților acestor firme.

**6. Riscuri mărite în bilanțul companiilor**

Deprecierea activelor va impacta nu numai colaterale de tip imobiliar (care au căzut deja cu peste 30%) ci și balanța băncilor sau companiilor de asigurare. Va impacta de asemenea și companiile din alte industrii (ca să nu spunem toate industriile) și nu numai activele tangibile dar și cele intangibile, de exemplu cele de brading, dat fiind volatilitatea cererii piețelor, care în lanț vor afecta și achizițiile.

*(continuare în pag. 26)*



# Impactul legii SARBANES-OXLEY asupra companiilor românești

Prăbușirea companiei Enron în octombrie 2001, urmată de o serie de scandaluri financiare implicând companii precum Qwest Communications, Global Crossing, WorldCom, Adelphia sau Tyco (2002), a declanșat o serie de inițiative legislative în guvernul american în vederea protejării investitorilor. Inițiativele s-au concretizat prin Legea Sarbanes-Oxley (SOX).

SOX cere companiilor listate la bursele din Statele Unite să manifeste transparență față de investitori și să dezvolte un sistem de controale interne, care să asigure acuratețea raportărilor financiare. Inițiativa legislativă a aparținut senatorului democrat Paul Sarbanes și a celui republican Michael Oxley.

Conformarea la SOX nu se referă doar la aspectele financiare ale companiilor, ci și la aspecte ale departamentelor de IT, precum deținerea drepturilor de acces sau modul de protejare a înregistrărilor electronice ale companiei.

Legea, a cărei aplicare este dificilă și necesită investiții de până la câteva zeci de milioane de dolari pentru marile corporații, nu afectează însă doar companiile de pe bursele americane, ci și filialele lor din străinătate sau deținătorii străini de titluri de valoare americane.

Cu toate acestea, există și câștigători, cum ar fi companiile de consultanță financiară, deoarece firmele care intră sub incidența SOX trec invariabil pe la un astfel de birou de consultanță.

Neputând fi modificată decât printr-o altă lege a Congresului American, SOX se limitează la trasarea principiilor, lăsând autoritatea stabilirii reglementărilor propriuzise asupra Securities and Exchange Commission (SEC). SEC a început procesul de reglementare în august 2002 și a luat în considerare comentariile publice și părerile factorilor implicați până în iunie 2004, la definitivarea acestora. Intenția tuturor acestor reglementări, aceea de a crește încrederea investitorilor în companiile listate, a fost transpusă de SEC printr-un sistem riguros de control intern asupra raportărilor financiare, supravegherea sporită a firmelor de audit, precum și posibilitatea ca acționarii să contribuie la alegerea membrilor independenți din consiliul de administrație, influențând ast-

fel decizii, cum ar fi stabilirea salariilor directorilor executivi sau gradul de corelare a beneficiilor acestora cu profitul raportat.

Pentru a creşte şi mai mult nivelul de protejare a acţionarilor, chiar şi după delistarea companiilor de la bursă, acestea sunt obligate să se conformeze standardelor SOX atât timp cât investitorii deţin acţiunile.

În România, printre companiile care au trebuit să implementeze reglementările SOX în ultimii patru ani se numără Romtelecom, Vodafone, Orange, Coca-Cola, ArcelorMittal, Bunge Romania, Autoliv Romania, Fiat, Delphi-Packard, Avon Cosmetics etc.

## Cât costă reglementarea?

**Liviu Mihăileanu, Consultant Senior în cadrul Departamentului de Consultanţă pentru Îmbunătăţirea Performanţei al PricewaterhouseCoopers România** spune că, încă de la început, au existat două puncte de vedere contradictorii cu privire la reglementările SOX.

*„Suporterii vedeau în SOX o soluţie menită să asigure transparenţa şi corectitudinea raportărilor financiare, precum şi diminuarea considerabilă a fraudelor, în ciuda costurilor semnificative ale reglementării care, la finalul primului an de conformare (2005) au atins 6,1 miliarde de dolari, dintre care 28% au fost alocate cheltuielilor în tehnologie şi alte 29% consultanţei externe”*, menţionează **Mihăileanu**.

De cealaltă parte a baricadei s-au situat părerile conform cărora SOX creează un raport inechitabil între diminuarea valorii fraudelor şi efortul financiar depus pentru obţinerea acestui beneficiu.

*„Datorită situaţiei specifice a SUA, unde activitatea de lobby este reglementată prin lege, grupurile de interes au fost înregistrate, declarându-şi intenţiile şi sumele plătite în acest sens firmelor specializate de lobby”*, adaugă **Liviu Mihăileanu.**

Un studiu publicat de National Bureau of Economic Research (NBER) în martie 2007 arată că, dintr-un total de 2.689 de scrisori adresate SEC cu privire la SOX în perioada de stabilire a reglementărilor (2002-2004), cele mai multe au fost adresate de contabili, avocaţi, grupuri academice (30,3%) şi companii (29,5%).

*„Conform NBER, 78% dintre opiniile persoanelor fizice şi 88% dintre cele ale grupurilor de investitori s-au exprimat în favoarea creşterii nivelului de detaliu a raportării financiare şi a responsabilizării companiei. De asemenea, s-au arătat fervenţi susţinători ai clauzelor de independenţă a auditorului companiei. Însă, 82% dintre opiniile managerilor sau directorilor de companii şi 72% dintre grupurile de non-investitori au argumentat împotriva tuturor reglementărilor de mai sus.*

*Totuşi, merită menţionat faptul că 7% dintre companii au făcut lobby în favoarea implementării reglementărilor SOX”*, mai spune **Mihăileanu**.

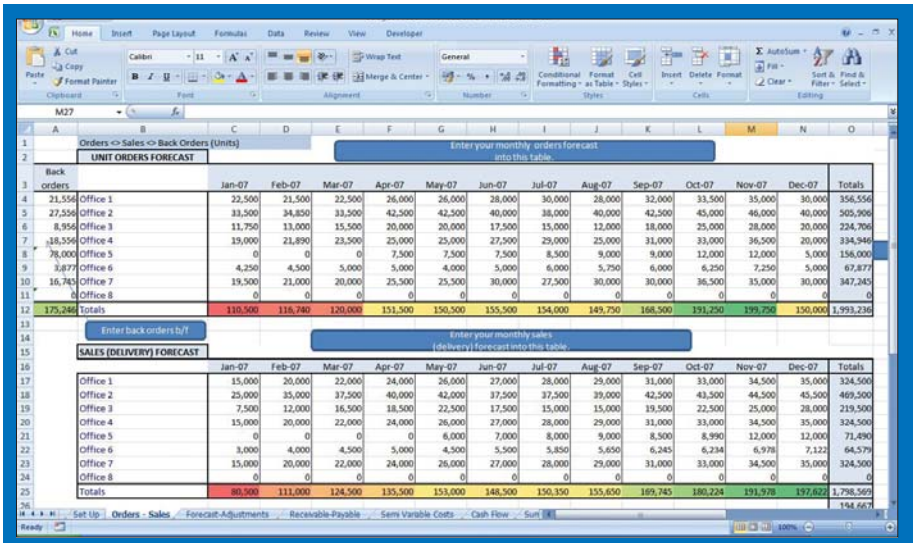
## Controlul intern în companiile româneşti

O mare parte a companiilor private au un sistem de control intern la nivel informal, mai mult cu caracter detectiv decât preventiv. Cu alte cuvinte, controalele interne sunt concepute să rezolve efectele problemelor după apariţia lor, mai degrabă decât să fie gândite astfel încât să prevină apariţia acestora sau să remedieze cauzele care stau la baza erorilor.

Consultantul PwC atenţionează că lipsa controalelor interne sau funcţionarea lor necorespunzătoare lasă companiile vulnerabile la o serie de riscuri, precum înregistrarea necorespunzătoare a tranzacţiilor contabile, efectuarea de tranzacţii neautorizate, fraudă, toate acestea reflectându-se în profitabilitate scăzută şi competitivitate redusă pe piaţă.

*„După mai bine de patru ani de reglementări SOX, opiniile cu privire la necesitatea şi eficienţa acestora sunt încă împărţite. În prima etapă, companiile au privit cu scepticism eficienţa cerinţelor SOX şi s-au arătat nemulţumite de eforturile pe care au trebuit să le depună pentru conformare şi de creşterea onorariilor auditorilor. Ulterior însă, au observat beneficiile acestora, cele mai vizibile fiind îmbunătăţirea procesului de raportare financiară şi creşterea încrederii în corectitudinea situaţiilor financiare”*, spune **Liviu Mihăileanu.**

Printre deficienţele constatate de companiile care s-au conformat reglementărilor se numără abordarea reactivă a deficienţelor în controalele interne finan-



**Efectele benefice ale reglementărilor, observate în cadrul companiilor româneşti care s-au conformat cerinţelor grupurilor listate la bursa de la New York, au început deja să fie vizibile prin:**

- creşterea capacităţii de management al riscurilor
- creşterea credibilităţii în faţa băncilor, a partenerilor de afaceri, a investitorilor sau agenţiilor guvernamentale
- relaţii de afaceri stabile, bazate pe un cod etic în afaceri asumat atât prin reglementare, cât şi prin integrarea valorilor în cadrul culturii organizaţionale
- îmbunătăţirea procesului de prevenire a fraudelor, ceea ce a redus expunerea la litigii
- îmbunătăţirea corelării proceselor în cadrul afacerii şi eliminarea proceselor redundante identificate în urma documentării acestora

ciare, de cele mai multe ori identificate în urma misiunilor de audit extern; lipsa controalelor IT la nivel de aplicație; lipsa controalelor interne la folosirea foilor de calcul tabelar; lipsa documentării proceselor financiare și de raportare contabilă.

## Impactul SOX asupra companiilor românești

Companiile românești care fac parte din grupurile listate la bursa de la New York au trebuit să implementeze reglementările SOX, ceea ce a implicat identificarea și documentarea controalelor interne asupra raportării financiare.

Liviu Mihăileanu spune că, printre problemele cu care s-au confruntat companiile în procesul de implementare a cerințelor SOX, se remarcă inexistența unor resurse interne suficiente pentru complexitatea procesului de implementare, costurile ridicate de conformare, creșterea gradului de birocratizare a activităților companiei precum și inexistența anterioară a unei culturi efective de control intern.

Totuși, datorită caracterului lor preventiv, în final au dus la un management mai performant al raportării financiare și al afacerii în general. Practic, efectul pe termen mediu al reglementărilor a îmbunătățit și a structurat modul în care companiile își desfășoară activitatea.

*„Evoluția mediului de afaceri arată că, din diverse motive (costuri interne mai mari, dorința de focalizare asupra ariilor de competență etc.), tendința multor companii este de externalizare a serviciilor complementare, situație care solicită furnizorului de servicii implementarea unui set de controale care să garanteze desfășurarea în bune condiții a parteneriatului. Acest lucru a transformat reglementările SOX dintr-o conformare coercitivă într-un model de control intern aplicabil nu doar în companiile publice listate la bursa de la New York, ci și companiilor care vor să crească nivelul de control al afacerii și a raportărilor financiare”*, menționează **Liviu Mihăileanu.**

Un aspect actual al pieței muncii, în condițiile restructurărilor operaționale, este dat de migrarea personalului calificat, lăsând „goluri” în structura operațională sau managerială a companiei. Ca urmare a implementării cerințelor SOX, companiile dețin o documentare detaliată a fluxului operațional și a atribuțiilor angajaților, putând astfel furniza informații critice succesorilor. În felul acesta, companiile își micșorează timpul și efortul depus pentru integrarea noilor angajați în companie.

*„Din punctul de vedere al departamentelor de IT, documentarea proceselor și a controalelor interne aferente reprezintă un instrument obiectiv de planificare a dezvoltării departamentelor și de aliniere a acestora la obiectivele de management ale companiei. Acest lucru este cu atât mai important, cu cât investițiile în echipamentele IT sunt recunoscute a fi printre cele mai mari în majoritatea companiilor, iar cheltuielile necorelate cu obiectivele de management duc la o profitabilitate redusă și o competitivitate scăzută pe piață”*, menționează **Liviu Mihăileanu.**

În evaluarea riscului folosirii foilor de calcul tabelar, fie că sunt folosite în scopuri operaţionale, de raportare managerială sau de raportare financiară, trebuie luate în calcul următoarele aspecte:
- complexitatea tabelelor şi a formulelor
- numărul de utilizatori ai fişierului
- volumul de date înregistrate
- beneficiarii finali ai fişierului
- frecvenţa şi consistenţa modificărilor aduse fişierului
- expertiza dezvoltatorului, gradul de instruire al utilizatorului şi modul de testare a fişierului înainte de a fi folosit de către companie

## Foile de calcul tabelar – exemplu de risc

Consultantul PwC avertizează că, deși pare un lucru banal, controlul inadecvat asupra foilor de calcul tabelar poate avea efecte devastatoare. Spre exemplu, dintr-o eroare a unei astfel de foi de calcul dintr-o instituție financiară, a rezultat o diferență de 1 miliard de dolari în raportările financiare ale acesteia. Eroarea a fost generată de o modificare neaprobată a unei formule care a generat apoi calcule eronate.

Un alt exemplu este cel al funcționarului unei bănci care a fraudat banca la care lucra prin includerea unor tranzacții fictive într-o foaie de calcul, deși nu ar fi trebuit să aibă permisiunea de a introduce astfel de înregistrări. Din cauza lipsei controalelor interne pentru foile de calcul, fraudarea a continuat timp de mai multe luni.

*„Riscurile pentru companiile românești cu privire la lucrul cu foile de calcul tabelar sunt cu atât mai mari, cu cât acestea sunt folosite la scară largă pentru realizarea situațiilor financiare și a raportărilor aferente. De cele mai multe ori, raportările conform Standardelor Internaționale de Raportare Financiară (IFRS) sunt elaborate folosind acest tip de fișiere, adesea relativ complicate și greu de gestionat”*, spune **Mihăileanu**.

În anul adoptării Legii Sarbanes-Oxley (2002), The Journal of Property Management publica un studiu conform căruia 90% dintre foile de calcul tabelar conțin erori majore chiar și la tabelele care conțin mai puțin de 200 de linii.

*„Folosirea elementelor macro și a desemnării tastelor care execută automat o serie de comenzi sunt exemple ale modului în care valorile din tabel pot fi modificate substanțial în mod voit sau accidental”*, adaugă **Mihăileanu**.

Reglementările pot fi folosite nu doar de companiile în care cerințele SOX sunt obligatorii, ci pot servi ca model oricărei companii care dorește să se raporteze la un cadru de bune practici în privința controlului intern asupra raportărilor financiare, precum și companiilor care intenționează să se listeze în viitor la bursa de la New York sau să-și vândă afacerea.

■ Luiza Sandu

Companiile românești care implementează un sistem de control intern după modelul SOX pot beneficia de avantaje precum:
- creşterea încrederii conducerii şi acţionarilor în raportarea financiară
- atragerea investiţiilor de capital de pe o rază teritorială mai mare, la costuri mai mici, datorită existenţei unui set de controale interne care creşte încrederea investitorilor
- o mai bună înţelegere a fluxului de activităţi, pe baza cărora managementul companiilor poate lua decizii strategice mai bune, datorită existenţei unor controale interne documentate, identificarea deficienţelor şi corectarea acestora
- reducerea efortului şi a onorariilor auditului extern care se poate baza, într-o măsură importantă, pe sistemul de control intern, ducând astfel la reducerea volumului testelor de audit

# Spălarea banilor.

## Concept și evoluție.

EC. DR. BOGDAN MIHAI MARTIMOF
SENIOR MEMBER OF THE BOARD
REPREZENTANT ARB
OFICIUL NAȚIONAL DE PREVENIRE ȘI COMBATERE A SPĂLĂRII BANILOR

Fenomenul spălării banilor a apărut cu mult timp în urmă, fiind legat de istoria comerțului și apariția sistemului bancar, fiind consacrat în timpul prohibiției din SUA anilor 30'.

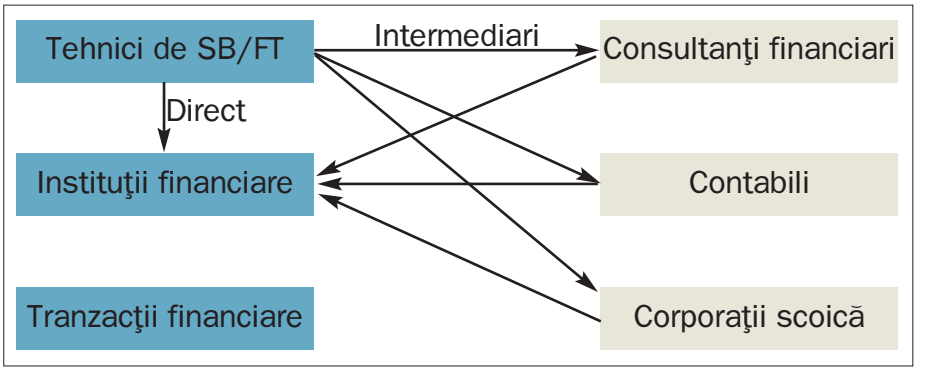
Vom încerca succint să explicăm fenomenul spălării banilor și modalitățile prin care se realizează acesta, atât la nivelul societății în ansamblu cât și la nivelul instituțiilor financiar bancare.

De peste 4 milenii, principiile care au stat la baza fenomenului nu s-au schimbat, dar mecanismele au devenit din ce în ce mai complexe, mai sofisticate, iar odată cu dezvoltarea tehnologică, au luat un caracter universal.

În USA, prohibițiile și retricțiile impuse de stat asupra jocurilor de noroc au condus la îmbogățirea infractorilor și a mafiei și, în general, a celor care nu respectau interdicțiile impuse. Astfel, aceștia, s-au trezit cu sume imense de bani cash. Al Capone ținea stivuiți pe rafturile dintr-o cămară din casa sa din Chicago câteva milioane de dolari și care începeau să constituie o mare problemă. Deschiderea unor afaceri paravan, din care se câștigau bani cash, a constituit rezolvarea. Astfel, aceștia și-au deschis spălătorii de mașini și de haine și astfel, realitate sau ficțiune, "spălarea" banilor a fost consființită ca terminologie.

În general, infractorii caută să-și investească întotdeauna banii în afaceri care aduc imediat profit cash. Aceștia au întemeiat case de avocatură, firme de contabilitate, studiouri de film, bănci, societăți de intermediere etc, prin care încearcă să dea un caracter licit fondurilor obținute din infracțiuni. Astfel, putem defini spălarea de bani ca procesul prin care infractorii creează iluzia că banii pe care-i dețin sau cheltuiesc sunt obținuți legal.

Pentru majoritatea țărilor, problemele privind spălarea banilor și finanțarea terorismului sunt legate de prevenirea, detectarea și incriminarea infracțiunilor generatoare de bani murdari. Tehnicile sofisticate utilizate în spălarea banilor și finanțarea terorismului se adaugă la aceste probleme.




Aceste tehnici pot fi realizate direct, prin implicarea a diferite tipuri de instituții financiare și multiple tranzacții financiare, cât și prin intermediari, precum consultanți financiari, contabili, corporații scoică și alți furnizori de servicii; transferuri către/prin/și din diferite țări; folosirea de diferite instrumente financiare sau alte tipuri de active de valoare.

Majoritatea țărilor subscriu la definiția dată în *"Convenția Națiunilor Unite Împotriva Traficului Ilicit de Droguri și Substanțe Psihotronice"* din 1998, cunoscută și sub denumirea de **Convenția de la Viena** și *"Convenția Națiunilor Unite Împotriva Crimei Organizate Transnaționale"* din 2000, cunoscută sub denumirea de **Convenția de la Palermo.**

Există trei abordări pentru definirea spălării banilor și anume:

*Într-o primă abordare, prin spălarea banilor se înțelege **conversia sau transferul proprietății,** cunoscând că această proprietate derivă din infracțiuni sau orice act de participare la infracțiuni, în scopul ascunderii sau disimulării originii ilicite a proprietății sau ajutarea oricărei persoane care este implicată în comiterea acestor infracțiuni, în vederea sustragerii de la consecințele legale ale acțiunilor.*

*A doua abordare constă în **ascunderea sau disimularea** adevăratei naturi, surse, locații, dispoziții, mișcări, drepturi ale destinatarului proprietății, cunoscând că astfel de bunuri rezultă din infracțiuni sau din participarea la astfel de acțiuni.*

*În final, dar nu ultima abordare, spălarea banilor constă în "**deținerea, posesia sau utilizarea** bunurilor, cunoscând în momentul dobândirii că aceste câștiguri/bunuri derivă din infracțiuni sau dintr-un act de participare la astfel de infracțiuni".*

Pentru a exista spălare de bani, trebuie să avem o infracțiune generatoare de "bani murdari", denumită infracțiune "predicat". Ca terminologie, Convenția de la Viena

limitează infracțiunea "predicat" la traficul de narcotice. Drept consecință, infracțiunile subrogate traficului de narcotice, precum frauda, furtul și răpirea, nu constituiau infracțiune "predicat" pentru spălarea banilor. De-a lungul anilor, comunitatea internațională și-a dezvoltat viziunea asupra infracțiunilor "predicat" de spalare a banilor, care a excedat traficul de droguri.

Astfel, FATF și alte organisme internaționale au extins definiția infracțiunii "predicat" din Convenția de la Viena, prin includerea și a altor tipuri de infracțiuni. De exemplu, Convenția de la Palermo cere tuturor statelor participante să aplice termenul de infracțiune de spălare a banilor unei arii largi de infracțiuni "predicat".

În cele 40 de Recomandări privind combaterea spălării banilor, FATF încorporează din punct de vedere tehnic și juridic definițiile din Convenția de la Viena și Convenția de la Palermo și evidențiază 20 de categorii de infracțiuni care trebuie incluse în categoria infracțiunilor "predicat" pentru spălarea banilor.

În multe jurisdicții, cei care ajută infractorii să spele bani proveniți din infracțiuni sunt ei înșiși considerați infractori. Aceasta înseamnă că bancherii, avocații, contabilii, dealerii de mașini și alții participanți la circuitele economice sunt considerați "spălători de bani" dacă permit ca afacerile lor să fie utilizate de către altcineva pentru spălarea banilor proveniți din infracțiuni. Deasemenea, în multe țări, oamenii, alții decât afaceriștii și infractorii, pot deveni spălători de bani numai prin posesia veniturilor din infracțiuni sau a activelor care reprezintă venituri din infracțiuni (este și cazul României). Cel mai elocvent exemplu este cel al soției sau prietenei infractorului care știu sau bănuie că acesta utilizează venituri ilicite pentru a cumpăra case, mașini sau bijuterii. **Clasa finală** a spălătorilor de bani este formată din **cei care ajută la realizarea schemei,** chiar dacă aceștia nu participă fizic la spălare de bani.

Astăzi, pretutindeni în lume, legislațiile naționale obligă dealerii de mașini, operatorii de cazinouri, dealerii de bijuterii și pietre prețioase de a-și identifica clienții în majoritatea cazurilor. Aceasta înseamnă că tuturor operatorilor li se cere să-și instruiască angajații în concordanță cu legea și cu măsurile de prevenire și combatere a spălării banilor. ■

*(urmare din pag. 21)*

**7. Spargerea balonului de profit**

Profiturile ca și componentă a PIB sunt cu 40% peste tendință. Conform statisticii, cum dupa o âsupraîncălzire urmează o corecție, în anii următori vor fi profituri la nivel redus.

**8. Volatilitate mărită în prețul mărfurilor și valutelor**

Presiunea asupra prețurilor va crește atât în zona resurselor naturale (am văzut ce se poate întâmpla cu fluctuația prețului petrolului!) cât și în zona produselor finite, cu impact asupra evoluțiilor valutelor.

**9. Protecționism**

Deocamdată nu s-au înregistrat schimbări majore în ceea ce privește libertatea comerțului. Totuși, sunt multe voci care invocă ridicarea unor bariere în această direcție.

**10. Consolidarea industriilor**

Din păcate, asistăm la multe falimente de companii mici, mijlocii și mari și la achiziții și consolidări "de restructurare" la companii gigant. Primele care au dat tonul au fost tot băncile.

**11. Intervenție susținută a statului**

Guvernele au promis intervenții chiar în cadrul Summiturilor guvernamentale - ca ultimul Summit al statelor G20, pentru a stopa adâncirea și derapajul crizei, a limita falimentele și a crea investiții tipice pentru perioadele economice critice, precum cele în infrastructură.

**12. Reglementare**

Tot la capitolul intervenții, re-reglementări, standarde de monitorizare și conformitate sunt o preocupare continua. Domeniul bancar din nou deține rolul fruntaș, dar toate industriile (telco, utilități, extractive, farmaceutice) sunt intensiv și extensiv presate de nevoia de reglemenatare sporită.

**13. Schimbare în comportamentul consumatorului**

Cine ar fi crezut că economisirea va deveni mai la modă decât consumerismul? Ei da, iată că se întâmplă, dincolo de presiunea pe venituri, de la descreșterea până la inexistența lor, apare un fenomen psihologic în lanț de incertitudine, care stopează apetitul (crescând până la exagerare și risipă, din ultimii 20 de ani) către ceea ce-mi place să numesc "luxul de larg consum" și re-îndreaptă cumpărătorii către "obligatoriu" sau esential.

**14. Impact generalizat**

Pe scurt și ca o concluzie, criza pare că va afecta înteaga economie mondială, toate industriile, chiar dacă acum cel mai vizibile sunt cea financiară (în componentele bancare, asigurări și piețe de capital) și cea imobiliară. Următoarele, care s-au și evidențiat deja, sunt cele producătoare de bunuri de folosință îndelungată (autoturisme, echipamente etc.)

Dar și sănătatea, de exemplu, ca și utilitățile, prin mecanismele de reglementare și corecție ale statului, vor avea de suferit, adaptându-se noilor condiții de piață.

*Cu cele de mai sus*

## Pictăm deci în culori întunecate viitorul?

Nu chiar, toate aspectele de mai sus pot fi privite ca provizioane de vești bune, ele nereprezentând, din fericire, pierderi întâmplate și asumate (hm, de către cine?) ci mai degrabă riscuri. Așa că bancile pot, cu un evident efort, să transforme aceste provizioane de risc în viitoare capitalizări de oportunitate. Mai mult, cu toate criticile, economia americană prezintă o flexibilitate remarcabilă pentru gigantul pe care încă îl reprezintă și pentru impactul pe care îl are în economia mondială. O altă formă de flexibilitate americană o reprezintă capacitatea de repliere conformă cu disponibilul forței de muncă. Aceste tipuri de agilitate ar trebui să dea de gândit dacă și cum pot fi urmate de alte mari economii afectate de criză dar mai rigide în anumite aspecte: Japonia, Germania, UK, Spania, Franta, Irlanda. ■

# TELEPREZENŢA
## VĂ ECONOMISEŞTE BANI ŞI TIMP

Prima companie comercială care a oferit soluții de teleprezență, Teleport (denumire care ulterior a fost schimbată cu TeleSuite), a fost înființată în 1993, de David Allen și Harold Williams. Înainte de TeleSuite, cei doi au administrat o afacere hotelieră și de aici a pornit conceptul de teleprezență.

Allen și Williams au observat că oamenii de afaceri, din cauză că erau obligați să participe la întâlniri importante, își scurtau șederea în stațiunea lor. Așa că s-au gândit să dezvolte o tehnologie care să le permită acestora să participe la întâlnirile programate fără a părăsi stațiunea, astfel încât durata șederii lor să se prelungească.

Lanțul hotelier Hilton a marșat la ideea celor doi și a introdus sistemul în toate hotelurile pe care le deținea în SUA și în afara lor, însă gradul de utilizare era scăzut. În cele din urmă, Hilton s-a retras din afacere, compania s-a prăbușit, iar David Allen a cumpărat activele TeleSuite și a înființat o nouă companie, pe care a numit-o Destiny Conferencing.

Deși compania a supraviețuit pe piață, ideea originală nu a prins decât atunci când s-au implicat companii gigant precum Cisco și HP, care au lansat sisteme similare pe la mijlocul anilor 2000. David Allen a vândut Destiny Conferencing în 2007 companiei Polycom, pentru 60 de milioane de dolari. Polycom este al doilea producător mondial de soluții de videoconferință, cu o cotă de piață de 30%.

La începutul lunii octombrie, Cisco a lansat o ofertă de achiziționare a companiei norvegiene Tandberg, lider global în comunicații video, la un preț total de achiziție de aproximativ 3 miliarde de dolari. Cu această achiziție în perspectivă, Cisco își va extinde portofoliul pentru a oferi mai multe soluții unui număr mai mare de clienți, accelerând apoi adoptarea pe piață la nivel global. Tandberg a anunțat pentru trimestrul al treilea din 2009 un venit de 234,7 de milioane de dolari și un profit operațional de 50 de milioane de dolari.

### De ce teleprezență?

Sistemul de teleprezență este, în esență, o tehnologie nouă și revoluționară, care creează senzația de întâlnire „față-în-față" celor care iau parte la o întâlnire desfășurată prin acest sistem de colaborare. Pentru a crea această senzație sunt combinate diverse tehnologii video și audio de ultimă generație.

Experiența de comunicare este extrem de apropiată de cea oferită de interacțiunea personală: imaginea este de înaltă definiție, persoanele sunt vizibile la dimensiuni reale, iar sunetul este spațial, optimizat, astfel încât sunt activate toate componentele non-verbale ale comunicării, care lipsesc din tehnologia tradițională de întâlniri online.

Spre deosebire de soluțiile tradiționale, sistemul de teleprezență nu necesită echipe dedicate pentru programare și operare, oricine poate face o programare în Outlook, iar inițierea comunicării se face printr-o singură apăsare pe butonul telefonului IP.

Soluția permite comunicarea în timp real între două sau mai multe puncte în care este instalat sistemul. Comutarea este automată, astfel încât persoana care vorbește, activând microfonul, apare și pe ecran. De asemenea, soluția permite partajarea de documente pe ecran în timp real.

## Cine foloseşte teleprezenţa?

De regulă, este folosită de resursele scumpe ale unei organizații, cum ar fi executivii sau specialiștii.

Teleprezența nu concurează însă cu soluțiile de videoconferință. Glumind, oarecum, soluțiile de teleprezență fac concurență liniilor aeriene, fiind o alternativă la deplasarea cu avionul. Călătoria de afaceri este o cheltuială majoră și o sursă de emisii de gaze cu efect de seră. Teleprezența poate foarte bine înlocui acele deplasări care presupun costuri mari de călătorie sau care nu ar putea fi organizate din cauza agendei încărcate a participanților. Uneori, interacțiunile prin teleprezență reprezintă singurul mod în care poate avea loc o întâlnire.

Cisco are aproximativ 40.000 de sesiuni de teleprezență pe lună, având instalate peste 650 de sisteme de teleprezență. De la introducerea sistemului în 2006 până în prezent, Cisco a realizat o economie estimată la 330 de milioane de dolari la nivel global.

HP a lansat în 2005 studioul colaborativ Halo, realizat împreună cu DreamWorks Animation SKG. Există peste 120 de studiouri Halo instalate în întreaga lume. Departamentul de imprimare și imagistică al HP a realizat o reducere de 8% cu cheltuielile de călătorie în 2005 folosind studiourile Halo. Utilizarea camerelor a crescut cu 25% într-un an.

Pentru a se conecta prin această tehnologie, companiile trebuie să achiziționeze cel puțin două camere Halo, fiecare proiectată pentru șase persoane. În fiecare cameră există trei ecrane cu plasmă, lumini și sisteme audio, cu o calitate de studio, iar participanții folosesc o interfață simplă on-screen, pentru a putea începe comunicarea prin doar câteva clicuri de mouse.

Cisco a implementat soluția de teleprezență în România în februarie 2009, iar sistemul este complet funcțional din luna martie. În București sunt două birouri de teleprezență, în sediul companiei.

### APLICAŢII ALE SOLUŢIEI DE TELEPREZENŢĂ:

- servicii de sănătate: HealthPresence
- audiţii muzicale
- bancar
- învăţământ
- administraţie publică etc.

## Cât costă o soluție de teleprezență?

În ceea ce privește costurile de implementare a serviciilor de teleprezență, o cifră exactă este dificil de estimat. Implementarea unui astfel de sistem de colaborare depinde de mai mulți factori, cum ar fi dimensiunea companiei sau numărul de birouri ale companiei în care se dorește instalarea unei astfel de soluții. De asemenea, în funcție de sistemul de colaborare ales, este nevoie ca incinta în care este instalat să aibă dimensiuni variabile și să fie adaptată din punct de vedere vizual, fonic și al mobilierului. Prețul de listă al unui sistem de teleprezență de la Cisco, de exemplu, poate varia între 33.900 de dolari și 340.000 de dolari, în cazul versiunii de top a sistemului de colaborare. Aceste costuri reprezintă exclusiv valoarea echipamentului oferit de Cisco, fără alte costuri adiacente. Amortizarea medie a costurilor acestui sistem a fost, în unele situații, de 14 luni. Există însă și companii care au reușit acest lucru în 6 luni. Sunt companii care folosesc sistemul de teleprezență pentru interviurile de angajare pe care le organizează.

Piața soluțiilor de teleprezență va ajunge la 4,7 miliarde de dolari până în 2014, conform unui raport al Frost & Sullivan. Regiunea Asia-Pacific va totaliza mai bine de o treime din toată piața de soluții de teleprezență, adică 1,7 miliarde de dolari.

Teleprezența oferă experiențe care depășesc cu mult tehnologiile tradiționale de videoconferință și rezultă în îmbunătățirea colaborării, accelerarea luării deciziilor, implementarea strategiilor ecologice și reducerea cheltuielilor de deplasare.

■ Luiza Sandu

# Externalizare IT

## în administrația publică – de la tehnologie la managementul schimbării

CĂTĂLIN HRISTEA,
DIRECTOR GENERAL
PMSOLUTIONS

Proiectele majore de informatizare a administrației publice centrale și locale nu mai sunt o noutate, iar dificultățile inerente implementării unui astfel de proiect au constituit subiect de analiză în cadrul rubricii "Opinia Consultantului", unde am insistat mai ales asupra componentei nontehnice, metodologice, a unei astfel de implementări. Externalizarea activităților de analiză, dezvoltare și configurare din cadrul etapei de implementare a proiectelor IT derulate în cadrul administrației publice este frecvent întâlnită și se datorează lipsei resurselor specializate în cadrul autorităților contractante, care să poată gestiona efortul de implementare a unor proiecte noi, în paralel cu operarea sistemelor existente.

După finalizarea unor proiecte majore de informatizare în ultimii ani și după retragerea echipelor de implementare ale furnizorilor, multe autorități ale administrației publice se confruntă acum cu problema administrării și a întreținerii cu resurse proprii a sistemelor informatice pe care le-au implementat, în paralel cu efortul continuu de îmbunătățire și de modernizare a acestor sisteme informatice. În contextul reducerii personalului din unitățile administrației publice și a cheltuielilor salariale asociate, administrația publică are reale dificultăți de a atrage și de a păstra în cadrul personalului propriu resursele tehnice calificate care să administreze, să întrețină și să îmbunătățească infrastructura informatică existentă.

### Externalizarea gestionării infrastructurii IT

Externalizarea completă a administrării și întreținerii infrastructurii informatice este des întâlnită la firmele private și începe să fie considerată ca o alternativă viabilă și de către unele autorități ale administrației publice, câteva astfel de contracte fiind deja în derulare. În acest context, am considerat util să prezentăm câteva aspecte specifice acestui gen de contracte, aspecte care, din experiența noastră, pot face diferența între o poveste de succes și una ratată...

### De ce să externalizăm?

Decizia de externalizare a serviciilor informatice trebuie să fie rezultatul unui proces serios de analiză, realizat de preferință de către un consultant specializat, analiză care să plece de la identificarea problemelor cu care instituția respectivă se confruntă din punctul de vedere al operării sistemelor sale informalice și care, apoi, să analizeze atent avantajele și dezavantajele pe care externalizarea le poate avea. Printre avantajele tipice pe care factorii de decizie le iau în calcul atunci când analizează oportunitatea externalizării serviciilor informatice se numără:

- acoperirea unei lipse de resurse, sau de capabilități tehnice, sau a inabilității de a atrage resurse tehnice calificate datorită concurenței firmelor private;
- creșterea substanțială a calității serviciilor;
- posibilitatea controlului foarte eficient asupra calității serviciilor, prin stabilirea unor acorduri asupra nivelului de furnizare a serviciilor (Service Level Agreements);
- plata serviciilor efectiv prestate, fără necesitatea angajării cu normă întreagă sau pe termen nelimitat a unei resurse tehnice specializate care este necesară doar în regim, part-time sau pe o perioadă limitată de timp;
- punct de contact unic, cu un singur furnizor, cu transferul complet al riscurilor către furnizor;
- posibilitatea concentrării resurselor umane proprii către activitățile de bază ale instituției;
- creșterea flexibilității serviciilor (prin accesul la o gamă largă de servicii externalizate, pe diferite perioade de timp);
- lipsa bugetelor de investiții, dar disponibilitatea bugetelor pentru cheltuieli de operare.

Chiar dacă aspectul financiar nu se află de obicei pe primul loc în topul primelor trei motive pentru care organizațiile iau decizia externalizării serviciilor informatice (conform statisticilor realizate în Statele Unite și țările vest-europene), acest aspect nu este deloc de neglijat în cazul unei autorități

publice din România. Din acest motiv, decizia de externalizare trebuie să aibă la bază și o analiză cost-beneficiu, care trebuie să cuantifice atât beneficiile monetare, cât și pe cele ne-monetare și să realizeze un numitor comun între acestea, care să constituie baza de comparație cu costul asociat externalizării.

În final, decizia externalizării este întotdeauna una strategică și care trebuie să aibă sprijinul managementului instituției.

## Scenariu posibil de externalizare

Un posibil scenariu de externalizare pentru o instituție publică poate avea următoarele componente:

- servicii de hosting data center
- servicii de comunicații de date (LAN, VPN, Internet)
- servicii de furnizare echipamente (prin închiriere)
- servicii de administrare sisteme (servere, baze de date, aplicații)
- servicii de suport (nivel 1 – call center și nivel 2, precum și nivel 3 și 4 pentru echipamentele și aplicațiile furnizate)
- preluarea unei părți a angajaților structurii de IT a beneficiarului
- servicii de implementare proiecte noi (analiză, proiectare, dezvoltare, instalare, testare, roll-out)
- servicii de instruire.

## Durata contractului de externalizare

Realizarea unui contract de externalizare nu este un obiectiv ușor de atins, mai ales în cazul unei autorități publice. Din experiența proprie, procesul de încheiere a unui astfel de contract (pentru o autoritate publică cu acoperire națională) poate dura peste 12 luni, începând din momentul în care decizia de externalizare a fost deja luată. Etapele care trebuie parcurse includ pregătirea unui caiet de sarcini detaliat, demararea și finalizarea procedurii de achiziție publică și negocierea contractului cu ofertantul câștigător.

Având în vedere atât efortul necesar pentru finalizarea unui astfel de demers, cât și faptul că un contract de externalizare demarează cu o perioadă de cel puțin 6 luni de acomodare a furnizorului cu organizația pentru care va presta serviciile (perioadă în care se realizează inventarul infrastructurii preluate, se face transferul infrastructurii și a responsabilității întreținerii acesteia, se organizează structura de suport tehnic, se stabilesc regulile de organizare și de comunicare cu organizația beneficiară etc.), interesul beneficiarului este ca acest proces să nu se reia în fiecare an. Din acest motiv, se preferă ca durata contractelor de externalizare să fie de cel puțin 3 ani. În cazul în care se recurge la un contract cadru de servicii, limita legală a duratei contractului este de 4 ani.

*„...decizia externalizării este întotdeauna una strategică și trebuie să aibă sprijinul managementului instituției..."*

## Managementul schimbării și rolul beneficiarului

Externalizarea serviciilor IT aduce schimbări importante în statutul și rolul membrilor vechii organizații IT a beneficiarului. În cazul în care se stabilește acest lucru și cu aceptul personalului beneficiarului, o parte a acestuia poate fi preluat de către furnizorul de servicii. De obicei, acest lucru se realizează în urma unui proces de evaluare a personalului și trebuie să se țină cont de prevederile legislației muncii privind restructurările de personal, precum și de statutul special al funcționarilor publici (dacă este cazul). În orice caz, trebuie ținut cont de faptul că un contract de externalizare a activităților curente de administrare și întreținere poate atrage după sine reducerea numărului de personal specializat al beneficiarului, deoarece activitățile realizate până în acel moment de către respectivul personal vor fi în continuare în responsabilitatea furnizorului extern.

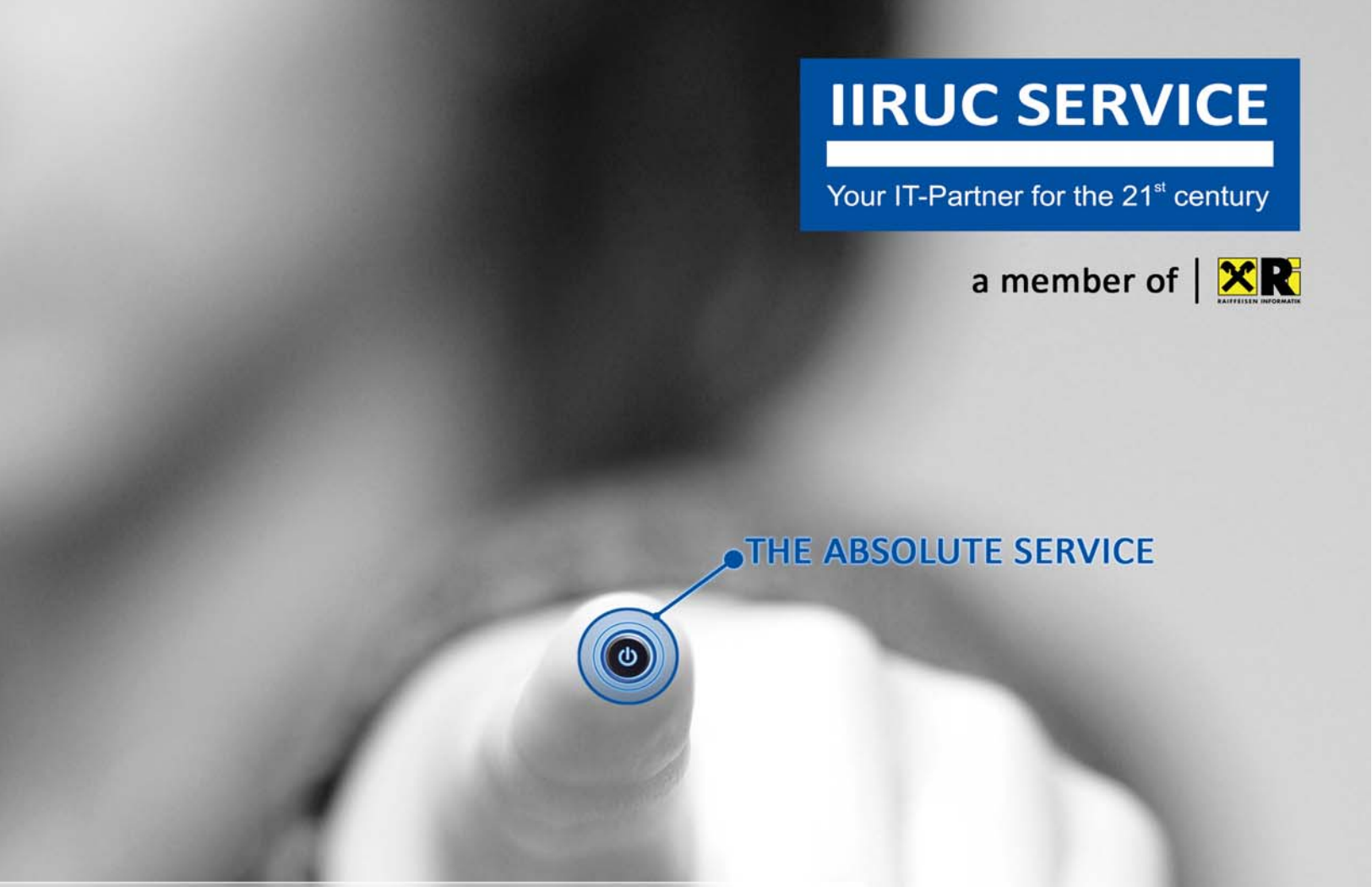
Rolul personalului IT care va rămâne în organizația care a externalizat serviciile IT se modifică substanțial, de la unul predominant tehnic și de execuție, la unul de planificare strategică, de supervizare a calității serviciilor și de interfață între direcțiile "de business" ale organizației și furnizorul de servicii externalizate. Această tranziție nu este una ușoară, deoarece necesită o schimbare de mentalitate în rândul personalului beneficiarului. Schimbarea fundamentală este aceea că responsabilitatea pentru calitatea serviciilor este a furnizorului extern, care trebuie să întreprindă orice măsură administrativă, organizatorică sau tehnică pentru a se asigura că serviciile informatice furnizate se încadrează în limitele aprobate ale SLA-ului. Din acest motiv, furnizorul este cel care decide asupra celor mai bune metode și tehnologii pe care le utilizează pentru furnizarea serviciului, astfel încât acesta să respecte SLA-ul agreat. Problema care se întâlnește însă în astfel de situații este că personalul beneficiarului este obișnuit cu un rol de execuție și cu implicarea tehnică în soluțiile alese și are tendința de a păstra acest rol de supervizare și de aprobare a tuturor aspectelor de natură tehnică, ceea ce creează un conflict între beneficiar și furnizor, din motive evidente: nu este posibil ca furnizorul să fie responsabil final pentru calitatea serviciilor furnizate, atâta timp cât beneficiarul are drept de "veto" cu privire la soluția tehnică.

Vom continua în numerele viitoare prezentarea aspectelor fundamentale care însoțesc procesul de externalizare, inclusiv: dependența de furnizor și modalități de gestionare a acesteia, strategia de exit, SLA și penalități, drepturi de proprietate intelectuală pentru dezvoltarea de software. ■

# IIRUC SERVICE

Your IT-Partner for the 21st century

a member of | RAIFFEISEN INFORMATIK




## Unique Competitive Advantages

- National coverage for Client Management / Field Services
- Maximum 2 hour for reaching the client anywhere over Romania
- Repairing Center facilities with skilled employees for major brands
- Just-in-time answer - thanks to the Call Center implementation and a modern ticketing and call management SaaS-Solution
- Prime-Contractor capabilities based on extended partnerships, HW/SW/networking equipment delivery

Contact:
S.C. IIRUC SERVICE S.A.
Sos. Fabrica de Glucoza nr. 7
020331 Bucuresti, Sector 2
Tel: +40-21-232.25.21
Fax: : +40-21-232.25.26
E-mail: office@iirucservice.ro
Web: www.iirucservice.ro

NEW ADDRESS

NEW APPROACH

NEW FOCUS

SIMTEX-OC

| | |
|---|---|
| ISO 9001 REGISTERED | C.1097.1 |
| ISO 14001 REGISTERED | M.440 |
| ISO 27001 REGISTERED | I.007 |

DELL
BUSINESS

# THEY'RE HERE

Introducing the affordable NEW Dell Vostro 1014 and 1015.

## NEW VOSTRO 1014

**MOBILITY WITHOUT THE BAGGAGE.**

**$659***

- Intel® Core™ 2 Duo processor T5870 (2.0GHz,800MHz FSB ,2MB L2 Cache)
- Ubuntu Edition Version 8.10
- 2048MB (1x2048) 800MHz DDR2 Dual Channel
- 250GB Serial ATA (5400RPM) Hard Drive
- 8X DVD+/-RW Drive
- 14.0" Widescreen WXGA (1280x800) WLED with Truelife
- Wireless 1397 (802.11 b/g), Bluetooth
- 3Years Carry In Warranty

## NEW VOSTRO 1015

**BREAK OUT OF THE OFFICE WITHOUT BREAKING YOUR BUDGET.**

**$659***

- Intel® Core™ 2 Duo processor T5870 (2.0GHz, 800MHz FSB,2MB L2 Cache)
- Ubuntu Edition Version 8.10
- 2048MB (1x2048) 800MHz DDR2 Dual Channel
- 250GB Serial ATA (5400RPM) Hard Drive
- 8X DVD+/-RW Drive
- 15.6" Widescreen WXGA (1280x800) WLED Anti Glare
- Wireless 1397 (802.11 b/g), Bluetooth
- 3Years Carry In Warranty

GENESYS
Value-added Distribution
*Let's Grow Together!*

* Price does not include VAT.
For more information and orders contact ***GENESYS DISTRIBUTION*** via e-mail sales@genesys.ro or telephone 0372 187 800, 021 242 05 42.
The offer is available through local partners (access www.genesys.ro).

**București:** Emag 021-2005200, TULIP COMPUTERS 021-2234242, TERRABYTE 021-2527275, CORSAR GRUP, POWER NET CONSULTING 021-2019481; **Bacău:** DEDEMAN 0234-513330, CYBERNET 0234-570892; **Botoşani:** ICE COMPUTERS 0231-536777; **Braşov:** EXPERT SERVICE IT 0268-410898, B2B DIGITAL 0268-317472; **Cluj Napoca:** TERABIT 0264-433993; **Constanţa:** BLUE PRINT 0241-520278, IIRUC-suc. DOBROGEA 0241-634595; **Craiova:** VERASYS INTERNATIONAL 0251-306016; **Focşani:** SECRET SERVICES 0237-237094; **Galaţi:** NEXIAL RESEARCH 0236-319120; **Iaşi:** BLUENOTE COMMUNICATIONS 0232 – 265995; **Mediaş:** BIROTEC 0269-845777; **Piteşti:** FAST ELECTRIC 0248-210037; **Suceava:** NETCOM ACTIV 0230-521268; **Timişoara:** SARATOGA 0256-499780.

The best-performing business PCs have Intel® Core™ 2 processors inside.



intel CORE 2 Duo inside
Look for Intel Inside®