# Securitatea informației – *o problemă dificilă și costisitoare*

## *Câteva considerații generale*

În ultima perioadă de timp, asistăm la o avalanșă de atacuri împotriva unor companii cu mare vizibilitate în peisajul de afaceri internațional, precum Google, Facebook sau Twitter, dar și asupra unor instituții de stat printre care NASA sau FBI, cu rezultate îngrijorătoare la nivel de securitate al datelor și al reputației.

Datele sunt cele mai importante resurse pentru o companie așa că protejarea lor este un obiectiv primordial. Datele trebuie să fie bine structurate atât din punct de vedere a utilizării lor, cât și a securității lor. *Nu se poate proteja ceva ce nu se cunoaște*. Analiza datelor sensibile ale unei companii este esențială în drumul spre succes. În orice moment, trebuie să știi unde se află datele sensibile ori critice și deloc de ignorat, *cine are acces la ele*! Doar atunci când se cântărește cu exactitate valoarea datelor, putem ști cum se pot proteja.

Dificultatea protejării informaților a crescut în special datorită cantității de date care este îmbogățită în fiecare zi, dar și a modului de accesare al acestor informații care trebuie să fie rapid, eficient, optim din punct de vedere al timpului.

Din statistici rezultă că în aproximativ 95% din cazuri, abia după ce s-a consumat un eveniment ce a afectat în mod *negativ* activitatea companiei, managementul conștientizează cât de importantă este securitatea datelor.

Ce se întâmplă atunci când datele sunt „*atacate*", sau când există o *scurgere de informații* ? Ce se întâmplă atunci când datele cu care lucrezi zilnic, ajung în posesia *concurenților*? Sunt câteva întrebări la care încercăm să răspundem.

În niciun caz, nu trebuie să ne bazăm pe faptul că „ *nouă nu ni se poate întâmpla*!".

## *Care sunt principalii factori care afectează securitatea datelor?*

Companiile trebuie să se asigure că îndeplinesc și respectă cerințele necesare protejării propriilor date și să-și consolideze politica de securizare a informațiilor permanent, în funcție de următorii factori:

**Proprii angajați**. Este cel mai sensibil factor. Trebuie să luăm în calcul faptul că există angajați rău intenționați care profită de vulnerabilitatea sistemului IT din cadrul firmei. La fel de periculoasă este și nepăsarea angajatorilor care nu țin cont de erorile umane și de greșelile angajaților începători, chiar dacă ele sunt comise, de cele mai multe, ori involuntar.

Aproximativ 42% dintre cei care părăsesc o companie apreciază că măsurile de securitate sunt inexistente sau/și insuficiente sau/și total neadaptate specificului activității.

Pornind de la faptul că mulți angajați au recunoscut că au "păstrat" informații la schimbarea locului de muncă, 53% dintre organizațiile românești suspectează că datele ce țin de proprietatea intelectuală a companiei sunt folosite de concurență.

**Factori externi**. În cazul unui virus informatic, de exemplu, este posibil ca acesta să nu vizeze direct o anumită companie, dar „infectarea" cu un astfel de software poate perturba serios activitatea zilnică,

afectând sistemele și echipamentele IT. De asemenea, „infectarea” cu astfel de programe poate deschide o breșă de securitate permițând accesul intern a persoanelor neautorizate.

În plus, creatorii de „malware” s-au reorientat pe obținerea de profit și în prezent se concentrează asupra unui singur obiectiv - traficul cu informații, contra cost. Acest lucru este cunoscut drept atac de tip „spyware”. Se apreciază că aproape 82% dintre companiile din România se confruntă zilnic cu astfel de atacuri. Imaginați-vă cât valorează aceste date pentru concurența directă!

**Factori naturali**. Defecțiuni sau dezastre naturale ce afectează buna funcționare a infrastructurii IT. Un backup de date într-un DataCenter este obligatoriu și este singura modalitate prin care vă știți informațiile în siguranță și accesibile oricând, indiferent de integritatea echipamentelor dumneavoastră.

## *Ce soluții se pot aplica pentru îmbunătățirea securității datelor ?*

Nu trebuie să vă bazați doar pe o soluție de tip firewall sau pe un program de antivirus competitiv, deoarece acestea nu mai sunt suficiente pentru a asigura securitatea datelor organizației.

Soluțiile de IT, precum Business Intelligence (BI) sau planificarea resurselor întreprinderii (ERP), pentru companii devin din ce în ce mai complexe și mai integrate. Ele trebuie să fie completate cu soluții de tip Data Loss Prevention ( DLP). Cu ajutorul lor se creează anumite reguli și drepturi în cadrul departamentelor companiei. Acestea alertează administratorii în momentul în care un angajat încalcă anumite reguli și încearcă să sustragă informații din cadrul companiei. Fiecare angajat al unei companii trebuie să aibă acces doar la categoria de date necesară îndeplinirii sarcinilor și responsabilităților din fișa postului. De exemplu, departamentul marketing nu ar trebui să aibă acces la documentele financiare ale firmei.

Totuși, toate aceste măsuri nu sunt suficiente fără educarea utilizatorilor. Fiecare trebuie să știe și să recunoască un mesaj de tip „phishing”, să știe cum să trateze fișierele atașate în e-mail-uri, să le scaneze și să raporteze departamentului de IT orice incident sau situație care li s-a părut suspectă.

Educarea și instruirea continuă a utilizatorilor trebuie să fie percepută ca un “Cod de bună practică”. O soluție de clasificare de date vine în ajutorul utilizatorului de-al responsabiliza și conștientiza asupra faptelor sale.

În concluzie, orice utilizator trebuie să conștientizeze în orice moment că este responsabil și răspunzător de confidențialitatea informației cu care operează.

Chiar dacă nu există un sistem de protecție impenetrabil, marile companii din România au înțeles necesitatea unui sistem de securitate performant, pro activ și dinamic, alegând astfel să investească zeci de milioane de euro pentru a evita astfel de incidente.

**Andreea Elena AVRIGEANU**
**Director General *CRUCIAL SYSTEMS & SERVICES, CONSTANTA***
***Membru AGIR***