IMPACTUL REVOLUŢIEI INFORMAŢIONALE ASUPRA INDUSTRIEI DE SECURITATE

Ing. Laurențiu Popescu
Lector A.R.T.S. *Sisteme de securitate antiefracție*

Aflăm din Wikipedia și nu numai că suntem în plină revoluție informaționala. Conform sursei citate:

- *Capacitatea tehnologică mondială de a recepționa informație printr-un canal unidirecțional (rețele radio – tv) a crescut cu o rată susținută anuală de 7% în perioada 1986 – 2007.*
- *Capacitatea tehnologică mondială de a stoca informație a crescut cu o rată susținută anuală de 25% în perioada 1986 – 2007.*
- *Capacitatea tehnologică mondială de a schimba informație prin rețele de telecomunicație bisens a crescut cu o rată susținută anuală de 30% în perioada aceloraşi două decade.*
- *Capacitatea tehnologică mondială de a procesa informație cu ajutorul computerelor de uz general asistate de factor uman a crescut cu o rată susținută anuală de 61% în aceeași perioadă.*

Nu este de mirare că dezvoltarea sistemelor de securitate începând cu anii 90 a fost „împinsă" de noile tehnologii din lumea IT. O analiză rapidă a dezvoltării subsistemelor de securitate începând cu anii 90 ne arată că:

- Evoluția senzorilor a fost marcată de trecerea la procesarea digitală a semnalelor în condiițiile în care principalele tehnologii de detecție erau deja puse la punct din anii 80.
- Apariția și dezvoltarea PC-ului a facilitat programarea centralelor prin porturi de comunicație ce au evoluat de la portul serial RS 232 la portul Ethernet de mare viteză.
- Trecerea în noul mileniu a fost marcată de apariția înregistrării digitale a ceea ce a permis o creștere calitativă extraordinară prin abandonarea unui standard ce avea rădăcinile undeva în perioada celui de-al doilea război mondial.
- Au fost dezvoltate și extinse atât funcțiile ce au legătură directă cu aplicațiile de securitate cât și cele auxiliare legate de funcționarea inteligentă a clădirilor.
- A fost posibilă integrarea subsistemelor de securitate și centralizarea evenimentelor în baze de date cu posibilități de apelare sincronă a informației provenite de la varii subsisteme în cazul declanșării unui eveniment de securitate.
- Ca o consecință a dezvoltării rețelelor de date atât fixe cât și mobile, accesarea informațiilor de securitate de la distanță a devenit un lucru banal.
- Informația în suport digital a devenit un bun care trebuie păzit.

Pe lângă securitatea fizică s-a dezvoltat un nou domeniu, securitatea informației, cu alți actori, mijloace și proceduri. Una din intrebările fundamentale care se ridică în acest context se referă la gradul de colaborare dintre cele două domenii: ce tehnologii IT sunt utile în asigurarea securității fizice și ce proceduri utilizate în asigurarea securității fizice merită a fi implementate în asigurarea securității informației? Există sau nu o competiție între cele două domenii? Dacă gradul de creștere al nivelului de informatizare al sistemelor utilizate în asigurarea securității fizice va crește în același ritm susținut, vor deveni firmele de IT un competitor de temut pentru cei ce se ocupă de securitatea fizică?

Un prim răspuns poate veni din faptul că nu există informație fără un suport fizic. Acest fapt crează o vulnerabilitate a cărei rezolvare vine din asigurarea securității fizice. De asemenea, informația existentă în sistemele de securitate fizică nu are relevanță fără suportul fizic al sistemelor. Pentru a prognoza însă viitorul trebuie să privim atent la noile modele economice aduse

de revoluția informațională. Societatea informațională este în esență o societate colaborativă în care nivelul de specializare este și mai ridicat decât în societatea industrială iar modelul de asigurare a securității (atât fizice cât și informaționale) va necesita o sumă de competențe în continuă creștere.

Modelul actual de implementare a soluțiilor de securitate în care sunt necesari cablori, tehnicieni de sisteme de securitate (incluzând tehnicienii specializați în soluții mecanice), ingineri de sisteme de securitate trebuie completat cu specialiști din domeniul IT cu pregătire în: implementarea de soluții server - client, aplicații de baze de date, rețele de date securizate și comunicații. Volumul de lucrări cu un grad de complexitate atât de ridicat nu este suficent de mare încât să necesite existența unui departament IT într-o firmă instalatoare de sisteme de securitate (cu excepția cazurilor în care departamentul IT este creat din considerente de management al organizației și, de regulă, nu este implicat în crearea de produse și servicii destinate clienților externi) iar varietatea de probleme este atât de mare încât modalitatea cea mai indicată pentru a ține pasul cu dezvoltarea tehnologică este de a crea parteneriate pe fiecare specializare în vastul domeniu al IT-ului cu entități dedicate.

Schimbările aduse de revoluția informațională sunt însă mult mai profunde. Nu numai aspectele tehnice sunt afectate ci și modelul de business. O nouă generație de clienți se pregătește astăzi. Sunt tineri care caută informațiile aproape exclusiv în mediul virtual. Companiile trebuie să se adapteze la acest nou model de economie și să reconsidere prezența on-line. Paginile web ale firmelor vor evolua probabil de la advertising și suport tehnic la adevărate instrumente de educare a potențialilor clienți. Forța schimbării este atât de mare încât pune presiune inclusiv pe factorul legislativ, obligat să creeze reglementări pentru noile forme de business (a se vedea modelul Uber și nu numai).

În aceste condiții, pregătirea continuă a personalului este o necesitate evidentă pentru toți actorii din vastul domeniu al asigurării securității. Un model interesant de organizare pe lanț vine de la o activitate cu riscuri de securitate foarte mari: personalizarea de carduri bancare. Aceasta poate fi făcută direct de bănci sau de către companii specializate. Acestea din urmă sunt auditate și certificate de operatori internaționali de carduri cum ar fi: VISA, Mastercard, AMEX etc.. Criteriile de auditare se modifică continuu, auditorii entităților sus-amintite evaluează permanent noile tehnologii de securitate și funcțiunile acestora chiar în procesul de auditare al clienților (firmele care personalizează cardurile). Pe scurt, la evaluarea fiecărui nou centru de producție, prin simpla implementare a unei soluții noi de securitate, operatorul Mastercard spre exemplu intră în contact cu o nouă soluție și trebuie să certifice conformitatea acestuia cu standardul propriu. În condițiile în care soluția aduce funcțiuni noi acestea sunt preluate și introduse în standardele viitoare. Un astfel de model de colaborare va trebui implementat și în relația legiferată în momentul de față în România între evaluatorii de risc la securitate fizică, companiile de specialitate și clienții acestora, deoarece un specialist format ieri nu va înțelege și nu va promova decât soluțiile trecutului în care acesta s-a format, ceea ce duce la o scădere de competitivitate într-un domeniu în care nu suntem - din fericire - pe ultimile locuri în spațiul european. Dacă vom reuși să păstrăm dinamica de până acum putem transforma amenințările viitorului în adevărate oportunități.