SECURITATEA INTEGRATĂ

Ing. Marius DUMITRU, PhD

Securitatea – acea stare de bine dorită, (subiectivă sau normată) – se obține printr-un proces sistematic și continuu care are ca scop menținerea acestei stări la nivelul dorit.

Complementar, nivelul global de risc al entității în analiză trebuie menținut în domeniul acceptabil și monitorizat permanent.

Realizarea și menținerea acestei stări de bine nu este un process simplu și nici gratuit. Securitatea costă! Dacă o implementezi costurile se reflectă în investițiile făcute. Dacă nu, mai devreme sau mai târziu, vei plăti lipsa ei – iar costurile pot fi foarte mari, ducând până la faliment uneori sau mai rău.

Securitatea are mai multe subdomenii: fizică, cibernetică, personal, documente, procedură-juridică sau industrială. Managementul securității presupune armonizarea tuturor acestor subdomenii într-o manieră sinergică.

Obținerea stării de securitate dorite (sau normate) se realizează astăzi în România prin abordarea secvențială a securității. Pentru fiecare subdomeniu implicăm echipe (interne sau externe) separate, care fac evaluarea nivelului de securitate după metode specifice. Rareori echipele comunica una cu alta. Adeseori recomandările din rapoartele de audit (măsurile propuse de control al riscurilor) sunt contradictorii și produc confuzie în organizația beneficiarului. Din aceste motive caracterul inerțial al securității se accentueaza și în locul dezvoltării culturii de securitate, prin creșterea conștientizării și acceptării voluntare a măsurilor impuse, apare o rezistență la schimbare și bineînțeles o creștere a vulnerabilității organizației.

De exemplu, evaluatorul de risc la securitate fizică recomandă, la un moment, ca o ușă să fie închisă/ blocată iar evaluatorul de risc la incendiu impune, în alt moment, ca aceeiași ușă să fie deschisă. Amândoi au dreptate din perspective proprii, însă nimeni nu i-a pus față în față pentru a-și armoniza pozițiile într-o perspectivă comună.

Implementări ale diverselor subsisteme de securitate la momente diferite de timp atrag și costuri mai mari, precum și interferențe prelungite în core business-ul organizației.

Se impune astfel o nouă abordare a securității într-o manieră integrată care să propună măsuri convergente, să reducă cheltuielile de audit, implementare și suport logistic integrat, precum și timpii de disturbare a activităților curente ale organizațiilor.
Pentru acest lucru legile specifice ale securității trebuie actualizate iar auditorii să renunțe la ego. O echipă de securitate integrată ar trebui să facă un singur audit și să-și sincronizeze propunerile de măsuri pentru controlul riscurilor. Seria de standarde ISO 27000 poate constitui un bun punct de start.

Cel mai simplu pot fi integrate subdomeniile securității fizice cu cel al securității cibernetice și securității documentelor: sistemele anti-efracție (control acces, detecție efracție, supraveghere video), sistemele BMS (Building Management System) și/sau software comportamental (behavior sw) pot fi intregrate cu sub-sistemele DMZ (DeMilitarized Zone), Document Management, precum și cu cele de management de rețea, ERP (Enterprise Resource Planning) sau CRM (Customer Relationship Management). Prin această integrare se pot monitoriza mai bine evenimentele din organizație și se poate adapta răspunsul la amenințările specifice mai rapid.

Instruirea continuă a personalului (manageri, utilizatori finali, personalul din IT&C și securitate) trebuie să se realizeze astfel încât să se obțină eficacitatea scontată a măsurilor de securitate realizate.

În concluzie abordarea integrată a securității conduce la creșterea eficienței și eficacității acestei componente a calității prin reducerea timpilor de realizare a măsurilor de control a riscurilor, a costurilor și a timpilor de răspuns la incidente.