TENDINŢE ÎN EVALUAREA RISCULUI DE SECURITATE

Stelian ARION,
Vicepreşedinte ASOCIAŢIA ROMÂNĂ
PENTRU TEHNICĂ DE SECURITATE

Introducere

Proces fundamental pentru îndeplinirea misiunii şi atingerea obiectivelor, managementul riscului este încă privit de unii ca parte a managementului securităţii. Prin extensie se poate spune că orice abatere de la mersul firesc al activităţilor, afectează îndeplinirea obiectivelor şi a misiunii în general şi constituie o afectare a securităţii. Spre exemplu sistemele de management al securităţii informaţiei includ printre categoriile de mijloace de control al riscurilor informaţionale unele care se adresează mai degrabă proceselor operaţionale decât celor de securitate: managementul resurselor, achiziţia, dezvoltarea şi mentenanţa sistemelor, conformitate[1].

Dacă ne îndreptăm spre infrastructurile critice, este evident că această abordare este necesară, deoarece obiectivul principal este disponibilitatea serviciului esenţial. Astfel, dincolo de măsurile menite să prevină sau să răspundă eficient unor atacuri maliţioase, trebuie puse în practică măsuri de evitare a întreruperii activităţii, dincolo de nivelul optim cerut de profitabilitatea operatorului. De asemenea, incidentele de infrastructură critică pot avea consecinţe grave rezultate din pierderea accidentală sau provocată a controlului asupra tehnologiei, iar eficienţa răspunsului în astfel de situaţii este de maximă importanţă.

Unele surse consideră securitatea ca starea de a fi protejat împotriva pericolului sau pierderii şi care se realizează prin atenuarea consecinţelor negative asociate cu acţiuni intenționate şi iraţionale ale altora[2]. Această definiţie aşează principiile pentru domenii aplicative precum securitatea fizică, securitatea cibernetică, securitatea personalului etc. Apare o diferenţă de abordare care induce confuzii şi neclarităţii cu privire la unele procese, dacă acestea sunt de securitate sau sunt operaţionale, de exemplu procesul de management al continuităţii sau procesul management al capacităţii.

Evaluarea riscului sau managementul riscului?

În contextul în care separarea dintre procesele operaţionale şi cele de management al securităţii este nerecomandată şi oricum dificil de gestionat, procesul de management al riscului trebuie să fie global. Această abordare este ilustrată şi de cea mai nouă ediţie a standardului ANSI/ASIS/RIMS RA.1-2014 dezvoltat cu participarea ASIS International, asociaţie profesională de renume în domeniul securităţii, care a trecut de la evaluarea riscurilor de securitate la evaluarea globală a riscurilor unei organizaţii. Conform acestui standard, evaluarea riscului înseamnă identificarea, analiza şi estimarea incertitudinilor cu privire la rezultate şi obiective. Aceasta furnizează o comparaţie între rezultatele dorite şi nedorite, precum şi între recompensele şi pierderile asociate cu realizarea obiectivelor. Evaluarea riscului analizează dacă incertitudinea se găseşte în limite acceptabile şi în domeniul de acţiune a capacităţii organizaţiei de a controla riscului. Rezultatele evaluării riscului informează persoanele de decizie asupra variantelor disponibile pentru gestionarea riscului. Evaluarea riscului reprezintă o examinare atentă, fundamentată metodologic, asupra a tot ceea ce poate cauza incertitudini şi oferă o bază pentru a determina dacă au fost luate suficiente măsuri pentru a preveni efectele negative sau pentru a spori oportunităţile pentru rezultate pozitive. Riscurile şi incertitudinile nu pot fi eliminate total, astfel încât evaluarea riscului ajută la ierarhizarea riscurilor care au impact asupra îndeplinirii obiectivelor organizaţiei.

Cele mai multe dintre metodologiile de evaluare a riscului pornesc de la identificarea, caracterizarea şi evaluarea resurselor organizaţiei, înţelese ca orice are valoare pentru organizaţie, în domeniul de aplicare al evaluării. Nivelul riscului este determinat în etapa de analiză pornind în general de la analiza ameninţărilor şi a oportunităţilor, analiza vulnerabilităţilor şi a capabilităţii, respectiv analiza impactului şi a criticităţii. Nivelul de risc, exprimat prin plauzibilitate si consecinţe este ponderat prin nivelul de eficacitate al mijloacelor de control al riscului aplicate şi funcţionale.

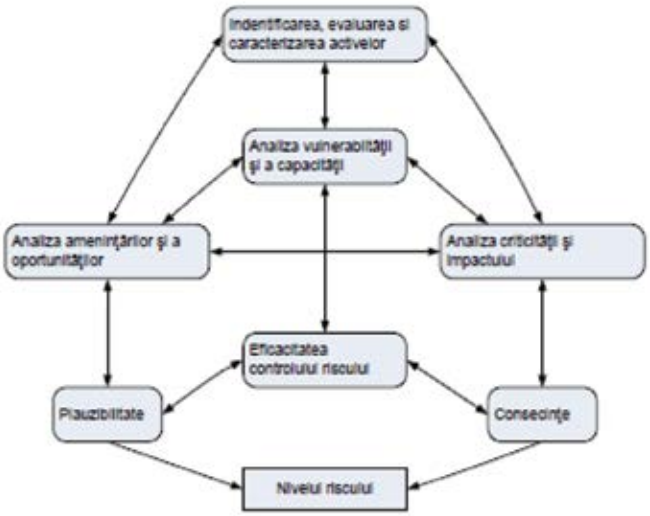

Fig. 1 Determinarea indicelui de risc

Odată acceptată abordarea evaluări globale a riscurilor se pune problema modalităţilor şi resurselor necesare pentru a obţine rezultate optime pentru toate categoriile de riscuri implicate, precum şi pentru diferitele unităţi în care poate fi descompusă organizaţia.
În special, o organizaţie mare, care poate avea mai multe proiecte, poate considera că este mai adecvată stabilirea mai multor secvenţe pentru procesul său decât stabilirea unei singure secvenţe. De aceea, cadrul său organizaţional ar trebui să includă elemente pentru a menţine o coerenţă corespunzătoare între secvenţe, pentru iniţierea şi terminarea acestora atunci când se cere (de exemplu la începutul unui nou proiect sau atunci când o nouă unitate de activitate este creată sau achiziţionată) şi pentru a promova comunicarea. Acestea nu sunt necesare pentru o organizaţie mică în care se aşteaptă să funcţioneze o singură secvenţă a procesului.

Aplicarea mai multor secvenţe de management al riscului permite, de exemplu, integrarea activităţilor externalizate în domeniul de aplicare, cum este situaţia multora dintre organizaţiile moderne.

Se poate merge însă mai departe, în a considera că, în ultimă instanţă, serviciul esenţial este rezultatul unui lanţ de activităţi întreprinse de diferite organizaţii într-un lanţ de dependenţa una faţă de cealaltă.

Schema din figura 2 sugerează lanţul de secvenţe al procesului de management al riscului, în cadrul unui flux global care porneşte de la materii prime sau orice alte elemente de intrare, până la furnizarea produsului sau al serviciului. Se observă complexitatea, multidisciplinaritatea şi contribuţia mai multor actori, precum şi necesitatea de comunicare şi coordonare între secvenţe.

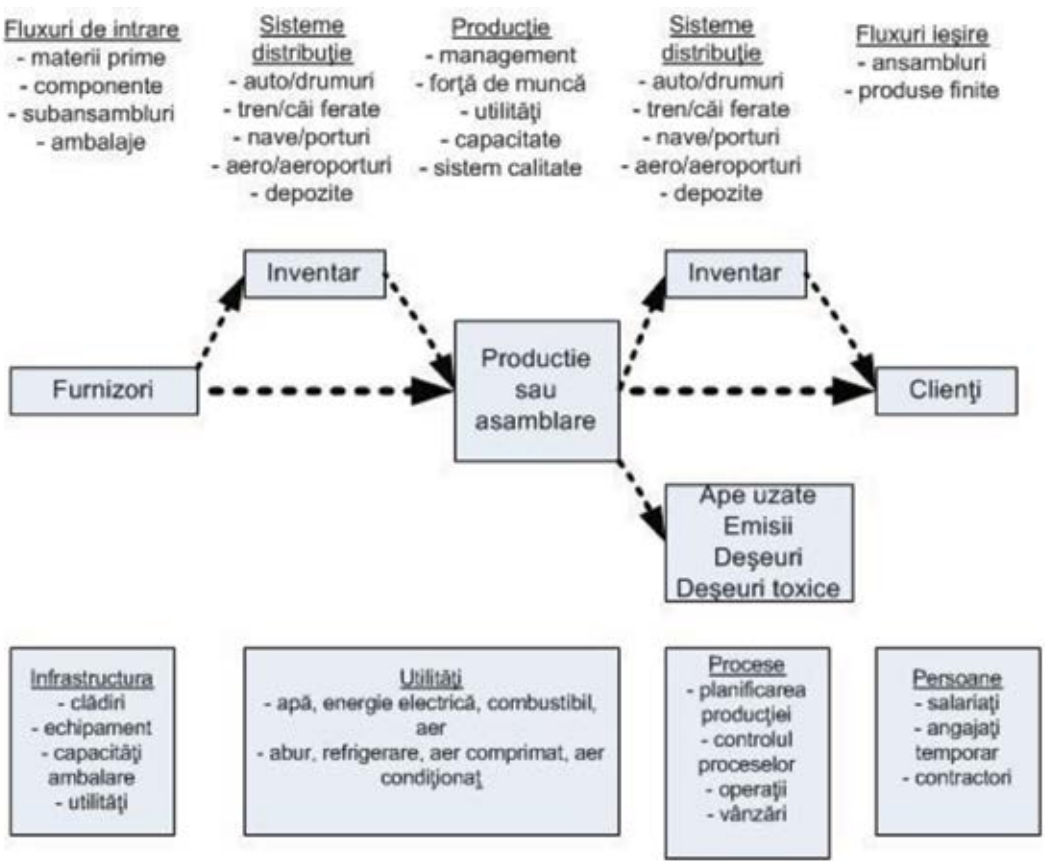

Figura 2 - Fluxul de procese ale unui lanţ de aprovizionare tip

O analiză în timp a unei soluţii de securitate va arăta de fiecare dată diferenţe între soluţia proiectată şi cea reală. Aceste diferenţe au cauze multiple pornind de la percepţii sau evaluări greşite în etapa de evaluare a riscului, erori în implementarea sau operarea măsurilor de securitate, până la modificări în contextul extern sau intern. Rezultă un grad de perimare în timp a rezultatelor evaluării, ceea ce impune repetarea periodică a activităţii de evaluare a riscului. Se ajunge astfel la ciclul Deming care caracterizează orice sistem şi proces de management şi care conduce în timp la îmbunătăţirea continuă a rezultatelor.

Este evident că, pentru a se asigura protecţia, este nevoie de un proces de management al riscului, cu toate secvenţele necesare. Procesul de management al riscului este cel care adaptează permanent capacitatea organizaţiei de a răspunde la riscurile cu care se confruntă aspect mult mai important decât asigurarea unei protecţii adecvate numai la momentul implementării măsurilor de securitate.

O organizaţie care operează corect un proces de management al riscului este de preferat uneia care a implementat o soluţie de securitate corectă la un moment dat şi apoi nu s-a mai preocupat de aceasta.

Tehnici de analiză a riscului de securitate

Pentru a obţine cele mai bune informaţii disponibile prin obiectivarea activităţii lor, evaluatorii de risc trebuie să utilizeze tehnici de analiză a riscului relevante pentru gama de riscuri, aplicate în cadrul unui proces recunoscut (de exemplu ISO 31000:2009). Tehnicile de analiză a riscului au fost dezvoltate singular sau în pachete, iar cele mai generale şi cunoscute dintre ele sunt prezentate în ISO 31010:2009.

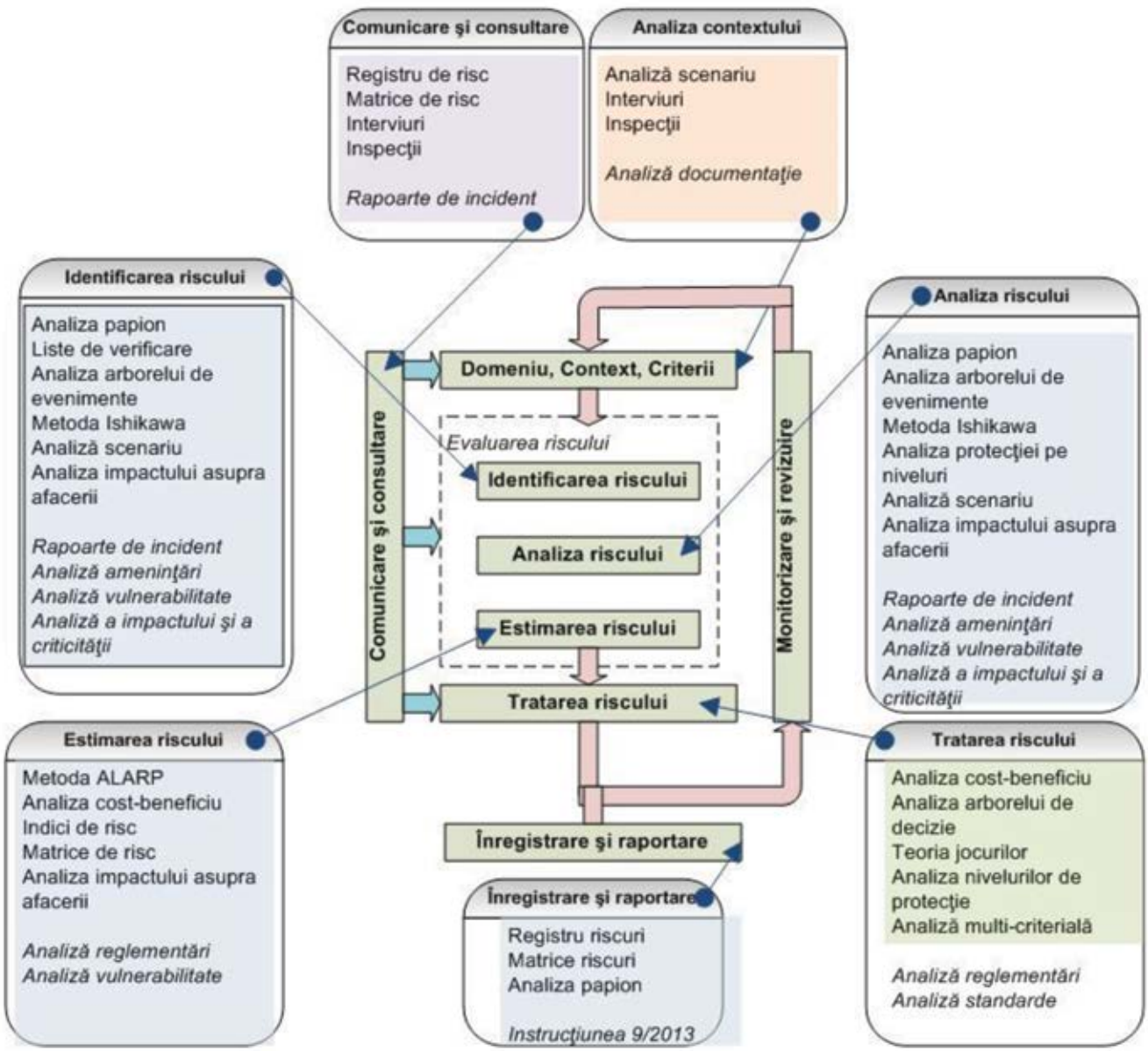

Figura 3 - Tehnici de analiză a riscului de securitate

În domeniul riscului de securitate se dovedesc necesare tehnici suplimentare de analiză, atât în privinţa evaluării expunerii la risc, cât şi în privinţa tratării riscului. Spre exemplu evaluarea ameninţărilor ia în discuţie motivaţii, intenţii şi capabilităţi, modalităţile şi scenariile de atac fiind definitorii pentru aplicarea unor mijloace de control. Pe de altă parte analiza vulnerabilităţilor este utilizată larg pentru a dimensiona soluţiile de securitate, iar în unele abordări evaluarea criticităţii consecinţelor şi a capacităţii de răspuns la incident sunt de asemenea luate în consideraţie.

Pentru exemplificare am asociat tehnici de analiză a riscului, dintre cele menţionate în ISO 31010:2009 dar şi dintre cele specifice practicanţilor în domeniul securităţii (cu caractere italice) pentru fiecare dintre fazele procesului de management al riscului. Menţionez introducerea fazei de ,'Înregistrare şi raportare'' având în vedere necesitatea de a dialoga cu autorităţile de profil, de regulă într-un cadru reglementat.

Nu pot să las deoparte contribuţia standardelor tehnice care se adresează tehnologiilor utilizate în aplicaţii de securitate şi care, la rândul lor, au în vedere capacitatea de a răspunde la riscuri mai mari sau mai mici. la rândul său legislaţia de profil, existentă în unele state poate introduce elemente specifice care trebuie luate în consideraţie în evaluarea riscului. Este cazul României în care pentru categorii de activităţi bine definite se impun măsuri de securitate obligatorii.

Practica în România

Am clarificat ce reprezintă şi care sunt principalele caracteristici ale activităţii de evaluare riscului. Se pune acum întrebarea cine poate realiza o evaluare SMART - specifică, măsurabilă, realizabilă, încadrată în timp pe întreg fluxul procesului de furnizare a produsului sau serviciului esenţial.

In Codul ocupaţiilor din România se pot întâlni ocupaţii şi profiluri profesionale pentru managementul sau evaluarea riscului. În plus există domenii în care sunt definite cadre de reglementare a activităţii şi autorizare a evaluatorilor, fie acestea publice sau private. Dintre acestea pentru analiza riscului la securitate fizică există un cadru bine definit prin Instrucţiunea 9/201310.

Pentru alte domenii de securitate reglementate (informaţii clasificate, infrastructuri critice, securitatea reţelelor informatice etc.) , legislaţia nu merge până la definirea unor ocupaţii privind evaluare riscului, această activitate fiind lăsată în responsabilitatea conducătorilor unităţilor care deţin activele critice. Corespunzător educaţia şi formarea de profil sunt minime, realizate de regulă în cadrul unor cursuri cu aplicabilitatea generală. Această situaţie de fapt, precum şi experienţa redusă a organizaţiilor privind managementul riscului în general, limitează adecvarea şi eficacitatea soluţiilor de securitate.

Concluzii

Societatea modernă se caracterizează prin creşterea şi diversificarea ameninţărilor care pot conduce la consecinţe negative, uneori catastrofale. În paralel cu această tendinţă, Uniunea Europeană a dezvoltat şi recomandă să fie aplicate modele de protecţie care au ca scop concentrarea pe o anumită gamă de ameninţări, sector de activitate sau categorie de măsuri de protecţie, aspect care generează la nivelul statelor membre legislaţie, autorităţi şi activităţi specifice.

Rapiditatea evoluţiei face ca aceste modele să nu fie complet şi corect aplicate, apar suprapuneri dar şi zone neacoperite, societăţile trebuie răspundă la cerinţe fragmentate, iar cheltuielile nu se regăsesc de fiecare dată în efectele scontate. Spre exemplu Directiva NIS8, acoperă o zonă consistentă privind protecţia infrastructurilor critice, dar după părerea mea nu va genera efectele scontate dacă cadrul legislativ şi de autoritate va fi diferit de cel privind protecţia infrastructurilor critice.

De asemenea asigurarea necesarului de competenţe poate fi deficitar atât timp cât nu sunt valorificate realizările mediului profesional din alte sectoare. În acest moment în România există o expertiză consistentă în domeniul securităţii fizice şi al securităţii informaţiei care poate contribui efectiv la îmbunătăţirea protecţiei infrastructurilor critice sau a securităţii cibernetice. Rămâne numai ca autorităţile publice responsabile să găsească cadrul adecvat pentru aceasta.

Bibliografie

1. SR EN ISO 27002:2013 Tehnologia informaţiei. Tehnici de securitate. Cod de bună practică pentru managementul securităţii informaţiei
2. J. Talbot, M. Jakeman - Security Risk Management. Body of Knowledge, Whiley 2009
3. SR BS 31100:2013 Managementul riscului. Cod de practică şi îndrumare pentru implementarea standardului SR ISO 31000
4. ANSI/ASIS/RIMS RA.1-2015 Risk Assessment
5. ANSI/ASIS SCRM.1-2014 Supply Chain Risk Management. Compilation of Best Practices
6. Peace, C. (2015). Risk assessment: is there a Goldiloks technique? http://www.riskmgmt.co.nz/publications
7. UNI/PdR 6:2014 Critical infrastructures - Resilence management system - Requirements
8. Directiva (UE) 2016/1148 a Parlamentului European privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice în Uniune
9. Ministerul Afacerilor Interne Instrucţiuni nr. 9 privind efectuarea analizelor de risc la securitatea fizică a unităţilor ce fac obiectul Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor