PROTECŢIA INFRASTRUCTURILOR CRITICE MANAGEMENTUL SECURITĂŢII LA NIVELUL DEŢINĂTORILOR ŞI AL OPERATORILOR

Stelian Arion – Director General R.A. Rasirom, Vicepresedinte A.R.T.S.

Introducere

Modernizarea accelerată a mediului socio-economic din România, transformarea activităţilor, a relaţiilor dintre organizaţii, a mediului social şi a celui profesional, dar şi progresul tehnic, migraţia valorilor dinspre tangibil spre intangibil fac să apară modificări în contextul de ameninţări, să potenţeze vulnerabilităţi mai vechi sau mai noi, să conducă la noi riscuri de securitate legate de cerinţe care aparent au fost soluţionate.

În ultimele două decade definiţia securităţii a fost lărgită incluzând cele mai multe dintre circumstanţele care pot afecta bunăstarea naţională sau interesele comunităţii, într-o gamă de ameninţări pornind de la schimbările climatice şi dezastrele naturale şi până la atacurile teroriste.

Infrastructurile critice

Infrastructurile critice, a căror definire este în continuare larg dezbătută, constituie coloana vertebrală a ţărilor, regiunilor, continentelor. Delimitarea infrastructurilor critice generează încă controverse, elementul esenţial fiind amploarea impactului provocat de întreruperea funcţionării acestora sau de deteriorarea nivelului de serviciu furnizat. În corelaţie cu schimbările majore induse de fenomenul globalizării, mastermodelul care se dezvoltă sub conceptul de protecţie a infrastructurilor critice poate genera instrumente esenţiale de guvernare şi gestionare a problematicilor curente. Astfel elaborarea şi aplicarea unor metodologii de evaluare şi estimare a interdependenţelor poate asigura un suport important pentru decizie la nivelul statelor şi/sau regiunilor. Aş aminti spre exemplificare criza financiară care se încadrează, după toate criteriile, ca un incident major de infrastructură critică, iar impactul său este foarte greu de evaluat şi estimat, majoritatea statelor reacţionând reactiv prin eforturi considerabile.

Structurarea, introdusă de aceste modele, se aplică la nivel organizaţional dar şi naţional sau regional şi implică participarea tuturor părţilor interesate pe baza unor principii comune. Astfel în documentul „Carte verde pentru un program european privind protecţia infrastructurilor critice", prezentat de Comisia Europeană în noiembrie 2005, sunt enunţate principiile denumite subsidiaritate, complementaritate, confidenţialitate, cooperare, abordare sectorială şi proporţionalitate.

Infrastructurile critice şi securitatea energetică

Considerată ca problematică majoră în ultima perioadă, securitatea energetică are cel puţin două aspecte puternic relevate: securitatea canalului de aprovizionare, cu aspecte puternic geopolitice, respectiv securitatea infrastructurilor critice asociate.

Cuprinzând infrastructuri uşor de identificat şi binecunoscute opiniei publice, infrastructurile critice din domeniul energetic se află în atenţia specialiştilor de mai mult timp, sunt mai bine reglementate iar rolurile şi responsabilităţile sunt mai bine delimitate între stat (şi chiar la nivelul Uniunii Europene) şi, respectiv, deţinători, operatori, utilizatori. Trebuie menţionat că datorită complexităţii problematicii este important aportul fiecărei părţi precum şi parteneriatul dintre acestea.

Directiva Consiliului nr. 2008/114/EC din 8 decembrie 2008 instituie o procedură pentru identificarea şi desemnarea infrastructurilor critice europene şi o abordare comună în ceea ce priveşte evaluarea cerinţelor de îmbunătăţire a protecţiei acestor infrastructuri pentru a contribui la protecţia cetăţeanului.

Managementul securităţii la nivelul deţinătorilor şi operatorilor de infrastructuri critice

Fiabilitatea tehnică, cândva baza performanţei, nu mai este suficientă în ziua de azi. Alţi factori precum, compatibilitatea cu mediul, aplicabilitatea comercială şi securitatea naţională, trebuie incluşi în procesul de decizie. La nivelul organizaţiilor (societăţi comerciale, organizaţii non profit, instituţii etc.) se petrece o modificare semnificativă în perceperea securităţii de la o simplă activitate funcţională la statutul de valoare adăugată misiunii acesteia. Conceptul de Securitate poate fi utilizat ca un concept integrator, prin incorporarea tuturor celorlalte obiective.

Pe de altă parte la nivel regional, naţional sau continental se afirmă o serie de abordări globale (modele master) ale căror cerinţe trebuie satisfăcute de organizaţii în funcţie de specificul activităţii lor. Astfel discutăm azi de planificarea şi menţinerea continuităţii activităţii, de managementul situaţiilor de urgenţă şi criză, de supravieţuire, de revenire după dezastru, de rezilienţă a infrastructurilor critice.

Parte dintre aceste cerinţe de securitate sunt exprimate prin reglementări legale în vigoare şi este datoria managementului organizaţiei de a asigura confirmitatea cu acestea.

La nivel organizaţional, managementul modern se bazează pe abordarea procesuală a activităţilor pe baza unor modele unanim recunoscute, exprimate prin standarde internaţionale (de exemplu sistemul de management al calităţii prezentat în familia de standarde internaţionale ISO 9000). În cadrul acestor modele este inclus sistemul de management al securităţii informaţiilor (familia de standarde ISO 27000) prin care se instituie un proces de identificare şi evaluare a ameninţărilor şi vulnerabilităţilor, de estimare şi tratare a riscurilor, reunite sub numele de management al riscurilor de securitate.

Riscurile de securitate sunt estimate în baza unor metodologii adecvate şi apoi sunt reprezentate în modalităţi sugestive pentru a ilustra impactul pe care un incident îl poate avea şi frecvenţa estimată de producere a acestuia.

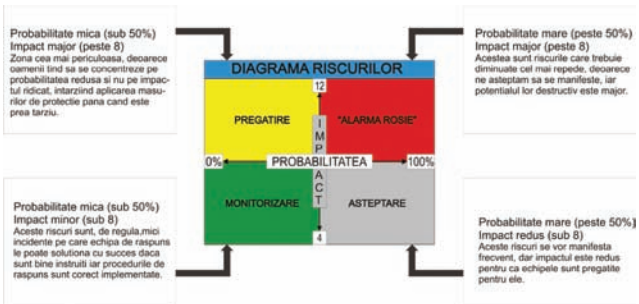

Fig.1 Matrice de reprezentare a riscurilor de securitate

Tratarea riscurilor reprezintă responsabilitatea organizaţiei în raport cu propriul acţionariat dar şi în raport cu administraţia de stat şi se realizează prin selectarea, instituirea şi menţinerea măsurilor de securitate adecvate – în raport cu un nivel de risc acceptabil formalizat la nivelul organizaţiei, respectiv cu cerinţele de conformitate legală şi de reglementare.

Din perspectiva protecţiei infrastructurilor critice, deţinător sau operator sunt acele entităţi cu responsabilităţi pentru investiţiile în sau operarea curentă a unui obiectiv particular, a unui sistem sau parte a sa identificate şi desemnate ca făcând parte din infrastructurile critice. Pornind de la conceptele introduse de Directiva Consiliului nr. 2008/114/EC indentificăm ca părţi ale cadrului organizatoric necesar planul de securitate al operatorului şi ofiţerul de legătură pentru securitate.

Planul de securitate al operatorului include identificarea principalelor active, evaluarea riscurilor, precum şi selecţia şi prioritizarea măsurilor şi procedurilor care trebuie instituite în toate infrastructurile critice, iar ofiţerul de legătură pentru securitate are rolul de a îmbunătăţi comunicarea şi cooperarea cu autorităţile statului cu atribuţii în protecţia infrastructurilor critice.

Selectarea măsurilor de securitate trebuie să acopere domenii organizaţionale - precum instituirea unui cadru organizatoric, adoptarea unei strategii şi a unor politici de securitate, securitatea personalului, securitatea relaţiilor cu terţii, tratarea incidentelor etc. - domeniul securităţii fizice şi cel al securităţii informatice, managementul situaţiilor de urgenţă şi criză, managementul dezvoltării.

În procesul de dimensionare a securităţii trebuie, de asemenea, avută în vedere asigurarea unui echilibru între măsurile proactive, reactive şi corective, asigurarea informării şi apoi a formării şi perfecţionării în domeniul securităţii, precum şi instituirea managementului în domeniul securităţii care trebuie integrat cu toate celelalte aspecte şi structuri de management ale organizaţiei.

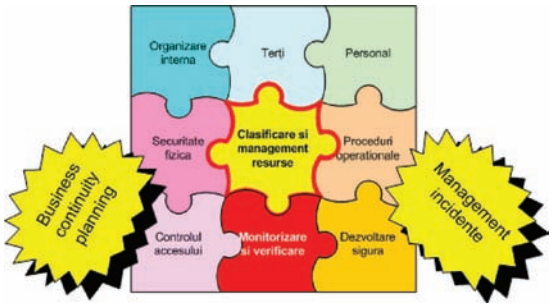

Fig.2 Puzzle exemplificativ asupra domeniilor din care trebuie alese măsuri de securitate adecvate

O atenţie deosebită trebuie acordată protecţiei informaţiilor sensibile, reprezentând acele informaţii despre infrastructurile critice care, în cazul divulgării, pot fi folosite pentru planificarea şi producerea unor acte care să ducă la perturbarea sau distrugerea acestora.

Concluzii

Complexitatea problematicii de protecţie a infrastructurilor critice impune o conlucrare echilibrată între instituţii, deţinător, operator, utilizator şi expertiză de terţă parte, materializată prin activitatea de consultanţă, activitatea de cercetare sau activitatea unor asociaţii profesionale.

La nivelul organizaţional managementul problematicii de securitate implică stabilirea unui cadru de funcţionare dedicat, elaborarea unei politici de securitate, cooperarea cu instituţiile cu atribuţii în domeniu şi conlucrarea cu specialişti în domeniu, interni sau externi. De asemenea, trebuie iniţiat un proces de constituire şi consolidare a expertizei de securitate la nivelul organizaţiei.

Activitatea de investiţii reprezintă o etapă majoră în protecţia obiectivelor, implică consum ridicat de resurse şi prezintă riscuri majore, mai ales atunci când instalaţii şi sisteme realizate în perioade lungi de timp trebuie să se integreze într-un "sistem de sisteme".

Instituirea unui proces holistic de management al riscului la nivelul organizaţiei asigură baza pentru gestionarea integrată a problematicii de securitate şi a celei de afaceri.

Rolul deţinătorului sau al operatorului de infrastructură critică în domeniul protecţiei acesteia este de a asigura o componenta semnificativă de securitate în îndeplinirea misiunii sale, prin instituirea şi menţinerea unui sistem de management adecvat bazat de mangementul riscurilor, în cadrul căruia să fie îndeplinite cerinţele de conformitate legală şi de reglementare naţionale şi regionale.