

# PROTECȚIA INFRASTRUCTURILOR CRITICE MANAGEMENTUL SECURITĂȚII LA NIVELUL DEȚINĂTORILOR ȘI AL OPERATORILOR

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

## Introducere

Modernizarea accelerată a mediului socio-economic din România, transformarea activităților, a relațiilor dintre organizații, a mediului social și a celui profesional, dar și progresul tehnic, migrația valorilor dinspre tangibil spre intangibil fac să apară modificări în contextul de amenințări, să potențeze vulnerabilități mai vechi sau mai noi, să conducă la noi riscuri de securitate legate de cerințe care aparent au fost soluționate.

În ultimele două decade definiția securității a fost lărgită incluzând cele mai multe dintre circumstanțele care pot afecta bunăstarea națională sau interesele comunității, într-o gamă de amenințări pornind de la schimbările climatice și dezastrelor naturale și până la atacurile teroriste.

## Infrastructurile critice

Infrastructurile critice, a căror definiție este în continuare larg dezbătută, constituie coloana vertebrală a țărilor, regiunilor, continentelor. Delimitarea infrastructurilor critice generează încă controverse, elementul esențial fiind amploarea impactului provocat de întreruperea funcționării acestora sau de deteriorarea nivelului de serviciu furnizat. În corelație cu schimbările majore induse de fenomenul globalizării, master-modelul care se dezvoltă sub conceptul de protecție a infrastructurilor critice poate genera instrumente esențiale de guvernare și gestionare a problematicilor curente. Astfel elaborarea și aplicarea unor metodologii de evaluare și estimare a interdependențelor poate asigura un suport important pentru decizie la nivelul statelor și/sau regiunilor. Aș 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 și estimat, majoritatea statelor reacționând reactiv prin eforturi considerabile.

Structurarea, introdusă de aceste modele, se aplică la nivel organizațional dar și național sau regional și implică participarea tuturor părților interesate pe baza unor principii comune. Astfel în documentul „Carte verde pentru un program european privind protecția infrastructurilor critice”, prezentat de Comisia Europeană în noiembrie 2005, sunt enunțate principiile denumite subsidiaritate, complementaritate, confidențialitate, cooperare, abordare sectorială și proporționalitate.

## Infrastructurile critice și securitatea energetică

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

Cuprinzând infrastructuri ușor de identificat și binecunoscute opiniei publice, infrastructurile critice din domeniul energetic se află în atenția specialiștilor de mai mult timp, sunt mai bine reglementate iar rolurile și responsabilitățile sunt mai bine delimitate între stat (și chiar la nivelul Uniunii Europene) și, respectiv, deținători, operatori, utilizatori. Trebuie menționat că datorită complexității problematicei este important aportul fiecărei părți precum și parteneriatul dintre acestea.

Directiva Consiliului nr. 2008/114/EC din 8 decembrie 2008 instituie o procedură pentru identificarea și desemnarea infrastructurilor critice europene și o abordare comună în ceea ce privește evaluarea cerințelor de îmbunătățire a protecției acestor infrastructuri pentru a contribui la protecția cetățeanului.

Managementul securității la nivelul deținătorilor și operatorilor de infrastructuri critice

Fiabilitatea tehnică, cândva baza performanței, nu mai este suficientă în ziua de azi. Alți factori precum, compatibilitatea cu mediul, aplicabilitatea comercială și securitatea națională, trebuie incluși în procesul de decizie. La nivelul organizațiilor (societăți comerciale, organizații non profit, instituții etc.) se petrece o modificare semnificativă în perceperea securității de la o simplă activitate funcțională 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, național sau continental se afirmă o serie de abordări globale (modele master) ale căror cerințe trebuie satisfăcute de organizații în funcție de specificul activității lor. Astfel discutăm azi de planificarea și menținerea continuității activității, de managementul situațiilor de urgență și criză, de supraviețuire, de revenire după dezastru, de reziliență a infrastructurilor critice.

Parte dintre aceste cerințe de securitate sunt exprimate prin reglementări legale în vigoare și este datoria managementului organizației de a asigura confirmarea cu acestea.

La nivel organizațional, managementul modern se bazează pe abordarea procesuală a activităților pe baza unor modele unanim recunoscute, exprimate prin standarde internaționale (de exemplu sistemul de management al calității prezentat în familia de standarde internaționale ISO 9000). În cadrul acestor modele este inclus sistemul de management al securității informațiilor (familia de standarde ISO 27000) prin care se instituie un proces de identificare și evaluare a amenințărilor și vulnerabilităților, de estimare și tratare a riscurilor, reunite sub numele de management al riscurilor de securitate.

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

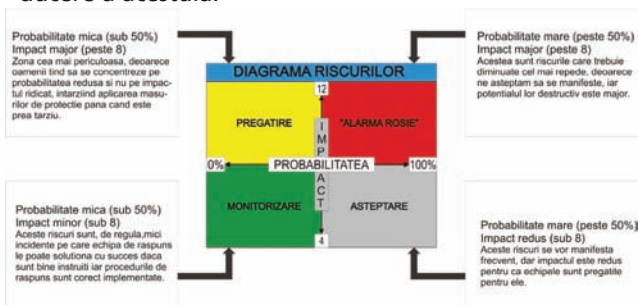


Fig.1 Mătrice de reprezentare a riscurilor de securitate

Tratarea riscurilor reprezintă responsabilitatea organizației în raport cu propriul acționariat dar și în raport cu administrația de stat și se realizează prin selectarea, instituirea și menținerea măsurilor de securitate adecvate – în raport cu un nivel de risc acceptabil formalizat la nivelul organizației, respectiv cu cerințele de conformitate legală și de reglementare.

Din perspectiva protecției infrastructurilor critice, deținător sau operator sunt acele entități cu responsabilități pentru investițiile în sau operarea curentă a unui obiectiv particular, a unui sistem sau parte a sa identificate și desemnate ca făcând parte din infrastructurile critice. Pornind de la conceptele introduse de Directiva Consiliului nr. 2008/114/EC indentificăm ca părți ale cadrului organizatoric necesar planul de securitate al operatorului și ofițerul de legătură pentru securitate.

Planul de securitate al operatorului include identificarea principalelor active, evaluarea riscurilor, precum și selecția și prioritizarea măsurilor și procedurilor care trebuie instituite în toate infrastructurile critice, iar ofițerul de legătură pentru securitate are rolul de a îmbunătăți comunicarea și cooperarea cu autoritățile statului cu atribuții în protecția infrastructurilor critice.

Selectarea măsurilor de securitate trebuie să acopere domeniul organizațional - precum instituirea unui cadru organizatoric, adoptarea unei strategii și a unor politici de securitate, securitatea personalului, securitatea relațiilor cu terții, tratarea incidentelor etc. - domeniul securității fizice și cel al securității informatice, managementul situațiilor de urgență și criză, manage-

mentul dezvoltării.

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

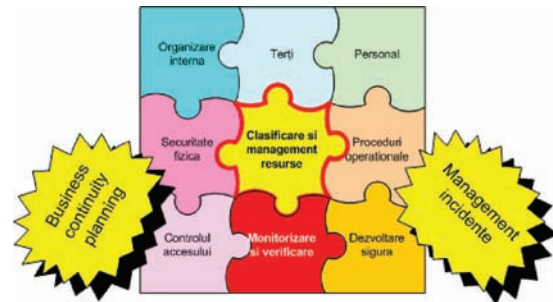


Fig.2 Puzzle exemplificativ asupra domeniilor din care trebuie alese măsuri de securitate adecvate

O atenție deosebită trebuie acordată protecției informațiilor sensibile, reprezentând acele informații despre infrastructurile critice care, în cazul divulgării, pot fi folosite pentru planificarea și producerea unor acte care să ducă la perturbarea sau distrugerea acestora.

### Concluzii

Complexitatea problematicei de protecție a infrastructurilor critice impune o conlucrare echilibrată între instituții, deținător, operator, utilizator și expertiză de terță parte, materializată prin activitatea de consultanță, activitatea de cercetare sau activitatea unor asociații profesionale.

La nivelul organizațional managementul problematicei de securitate implică stabilirea unui cadru de funcționare dedicat, elaborarea unei politici de securitate, cooperarea cu instituțiile cu atribuții în domeniu și conlucrarea cu specialiști în domeniu, interni sau externi. De asemenea, trebuie inițiat un proces de constituire și consolidare a expertizei de securitate la nivelul organizației.

Activitatea de investiții reprezintă o etapă majoră în protecția obiectivelor, implică consum ridicat de resurse și prezintă riscuri majore, mai ales atunci când instalații și 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 organizației asigură baza pentru gestionarea integrată a problematicei de securitate și a celei de afaceri.

Rolul deținătorului sau al operatorului de infrastructură critică în domeniul protecției acesteia este de a asigura o componentă semnificativă de securitate în îndeplinirea misiunii sale, prin instituirea și menținerea unui sistem de management adecvat bazat de managementul riscurilor, în cadrul căruia să fie îndeplinite cerințele de conformitate legală și de reglementare naționale și regionale.