ÎMBUNĂTĂȚIREA PROTECȚIEI INFRASTRUCTURILOR CRITICE DIN SECTORUL TIC PRIN CREŞTEREA REZILIENȚEI

Dragoş Cătălin Barbu

dragos.barbu@ici.ro

Institutul Național de Cercetare-Dezvoltare în Informatică – ICI Bucureşti

Rezumat: La nivelul Uniunii Europene sunt întreprinse demersuri în privința adoptării unei strategii europene pentru securitatea cibernetică, care să armonizeze eforturile statelor membre în abordarea provocărilor de securitate din spațiul cibernetic şi protecția infrastructurilor critice. Este important de remarcat faptul că avariile sistemelor într-un sector specific al infrastructurilor critice pot produce efecte în lanț, datorită rolului lor strategic în contextul socio-economic, care pot avea un potențial impact în toate aspectele societății. Înțelegerea efectelor şi inter-conexiunilor strategice sunt esențiale atunci când se stabilesc modul de răspuns la evenimente şi când se stabilesc politici.

Cuvinte cheie: securitate, incidente, securitate cibernetică, reziliență, infrastructuri critice.

Abstract: At European Union level, there are many interventions underway in order to adopt a common European strategy for cyber-security that would bring to a common base the efforts of all Member States in dealing with security challenges related to cyber-space and protection of critical infrastructures. It is very important to notice the fact that damages implied on systems specific to critical infrastructures can produce chain-reactions, due to their strategic role in the social and economic areas that would potentially have a harmful impact on the entire society. Understanding the effects and the strategic inter-connections is essential when deciding on the response measures and policies.

Keywords: security, incidents, cyber security, resilience, critical infrastructures.

1. Introducere

Infrastructurile critice sunt coloana vertebrală a societății moderne asigurând funcționalitățile vitale care susțin interacțiunile economice şi sociale. Directiva Europeană 2008/114/CE (Europene, 2008) defineşte infrastructura critică ca fiind „un element, un sistem sau o componentă a acestuia, aflat pe teritoriul statelor membre, care este esențial pentru menținerea funcțiilor societale vitale, a sănătății, siguranței, securității, bunăstării sociale sau economice a persoanelor, şi a căror perturbare sau distrugere ar avea un impact semnificativ într-un stat membru ca urmare a incapacității de a menține respectivele funcții".

Infrastructurile critice, cum ar fi rețeaua electrică, conductele de petrol şi gaze, precum şi sistemele de distribuție a apei sunt fundamentale pentru societatea modernă. Astfel, protecția infrastructurilor critice este o chestiune de securitate națională. Cu toate acestea, recentele incidente care implică malware-ul Stuxnet (Hagerott, 2014), Dragonfly (Team, 2012) şi Flame (MacKenzie, 2014) au arătat că elementele de infrastructură critică sunt susceptibile la atacuri cibernetice. Cel mai alarmant a fost primul atac cibernetic raportat (Cherepanov, 2016) împotriva unei rețele electrice ce a avut loc în decembrie 2015. Malware-ul a infectat utilitățile electrice a cel puțin trei regiuni, lăsând fără energie electrică aproximativ jumătate din casele din regiunea Ivano-Frankivsk a Ucrainei.

Bunăstarea societății este tot mai dependentă de buna funcționare a infrastructurilor critice iar crizele care afectează infrastructurile critice agravează impactul lor asupra societății. Prin urmare, îmbunătățirea rezilienței infrastructurilor critice este unul din cel mai importante obiective ale proprietarilor/operatorilor/administratorilor pentru managementul crizei.

2. Conceptul de reziliență

Conceptul de reziliență a evoluat în mod considerabil de la definiția fundamentală a lui Holling (Holling, 1973) ca „o măsură a capacității unui sistem de a continua să funcționeze făcând față modificărilor variabilelor de stare, de conducere, precum şi a parametrilor". În (Francis & Bekera, 2014) a fost realizat un studiu asupra definițiilor de reziliență şi se prezintă o scurtă trecere în revistă a definițiilor rezilienței din diferite perspective disciplinare (sisteme de infrastructură: managementul siguranței, organizațional, socio-ecologic, economic şi social cu proprietățile lor cheie).

Literatura de specialitate conține mai multe definiții ale rezilienței precum şi mai multe dimensiuni, caracteristici şi principii care definesc acest concept. Unii din autori (Zobel, 2011), (MCEER, 2008) împart reziliența în patru dimensiuni:

- **reziliența tehnică**: se referă la capacitatea sistemului fizic al organizației de a se comporta în mod corespunzător în cazul unei crize;
- **reziliența organizațională**: se referă la capacitatea managerilor care se ocupă de criză să ia decizii şi măsuri care să conducă la evitarea unei crize sau de a reduce impactul acesteia;
- **reziliența economică**: se referă la capacitatea entității de a face față costurilor suplimentare care apar dintr-o criză;
- **reziliența socială**: se referă la capacitatea societății de a reduce impactul unei crize, de adaptare prin ajutorarea primelor persoane care intervin sau celor care acționează în calitate de voluntari.

Reziliența unui sistem porneşte de la premisa unei schimbări în mediul de operare normal al acestuia, care are potențialul, dacă nu şi efectul, de a perturba performanța normală a sistemului. În literatura de specialitate, definirea rezilienței unui sistem:

- are în vedere o întrerupere sau o pierdere în performanța temporară, urmată de o revenire rapidă la performanțele normale ale sistemului;
- vizează capacitatea unui sistem de a continua să funcționeze în timpul unor condiții schimbătoare, dar numai la un nivel diminuat, sau în cazul în care performanța sistemului scade gradual spre deosebire de situația în care aceasta scade brusc;
- se concentrează pe capacitatea sistemului de a se adapta la schimbarea condițiilor pentru a funcționa la un nivel acceptabil sau sustenabil.

Departamentul pentru Securitate Internă (Department of Homeland Security-DHS) al Statelor Unite ale Americii[1] consideră că reziliența înseamnă capacitatea (unei entități) de a se pregăti şi a se adapta la schimbarea condițiilor precum şi de a rezista şi a se recupera rapid în urma unei perturbări şi include abilitatatea de a rezista şi a se recupera în urma unor atacuri deliberate, accidente sau amenințări ori incidente având cauze naturale.

3. Reziliența infrastructurilor critice

Reziliența infrastructurilor critice se defineşte de NIAC (National Infrastructure Advisory Council) (NIAC, 2010) ca fiind capacitatea de a reduce amplitudinea şi/sau durata unor evenimente perturbatoare. NIAC consideră că eficacitatea rezilienței unei infrastructuri sau organizații depinde de capacitatea sa de a anticipa, de a absorbi, de a se adapta la, şi/sau de a îşi reveni rapid, în urma apariției unui eveniment perturbator.

Protecția şi reziliența infrastructurilor critice sunt concepte complementare şi necesare pentru realizarea unei strategii cuprinzătoare de gestionare a riscurilor. Creşterea rezilienței reprezintă o condiție esențială pentru succesul activităților de protecție a infrastructurilor critice. Reziliența infrastructurii este strâns legată de modul în care organizațiile îşi gestionează riscurile strategice, operaționale şi financiare şi de modul în care guvernele absorb şocurile la nivelul societății, ca urmare a unor dezastre.

Definițiile specifice ale rezilienței sunt mai puțin importante decât conceptele fundamentale ale rezilienței. Caracteristicile cheie ale infrastructurilor critice definite în (NIAC, 2010), concepute inițial de către Stephen Flynn, sunt următoarele:

- **robustețea** – capacitatea de a menține operațiunile şi funcțiile critice în cazul unei crize: reflectată în construcția fizică şi proiectarea infrastructurii (clădiri de birouri, poduri,

[1] Reziliență, Department of Homeland Security, https://www.dhs.gov/topic/resilience

baraje, diguri) sau în redundanța și capacitatea de substituție a sistemelor (rețele de transport, de alimentare cu energie electrică și de comunicații);

- **capacitatea de reacție** – abilitatea de a se pregăti corespunzător, de a răspunde și de a gestiona activitățile în cazul apariției unei crize sau perturbări: presupune identificarea modului de evoluție a crizei sau perturbării, planificarea continuității afacerii, managementului lanțului de aprovizionare, prioritizarea acțiunilor pentru controlul și reducerea pagubelor.
- **capacitatea de recuperare rapidă** – abilitatea de a reveni la și/sau reconstitui operațiunile normale cât mai repede și mai eficient posibil, după o întrerupere. Aceasta include planuri de urgență atent elaborate, operațiuni de urgență corespunzătoare, precum și modalitățile de a avea resursele necesare la locul potrivit.
- **adaptabilitatea** – modul de absorbție a noilor lecții care pot fi extrase dintr-o catastrofă. Implică revizuirea planurilor, proceduri de modificare și introducerea de noi instrumente și tehnologii necesare îmbunătățirii robusteței, capacității de reacție și de a celei de recuperare rapidă înainte de următoarea criză.

4. Măsurarea rezilienței infrastructurilor critice

Centrul Multidisciplinar pentru Cercetări în Ingineria Seismică al Universității Buffallo a dezvoltat o metodologie (MCEER, 2008) pentru măsurarea rezilienței care ia în considerare următoarele:

- Proprietăți ale rezilienței:
  - **robustețea** – rezistența sau capacitatea elementelor, sistemelor și ale altor unități analizate de a rezista la un anumit nivel de stres sau de solicitare, fără a suferi degradarea sau pierderea funcționalităților;
  - **redundanța** - măsura în care elemente, sisteme sau alte unități analizate care sunt substituibile, adică, capabile să satisfacă cerințele funcționale în cazul unor evenimente de perturbare, degradare sau pierdere a funcționalității;
  - **capacitatea de reacție** – capacitatea de a identifica probleme, de a stabili priorități și de a mobiliza resurse, atunci când există condiții care amenință să perturbe unele elemente, sisteme sau alte unități analizate;
  - **capacitatea de recuperare rapidă** – capacitatea de a îndeplini prioritățile și de a atinge obiectivele, în timp util, pentru a limita pierderile și pentru a evita perturbări viitoare.
- Dimensiuni ale rezilienței:
  - **tehnică** – exprimă capacitatea sistemelor fizice (inclusiv toate componentele interconectate) de a performa la niveluri acceptabile/dorite, atunci când sunt supuse la dezastru;
  - **organizatorică** – exprimă capacitatea organizațiilor (în special cele care gestionează facilități critice și funcții legate de dezastre) de a lua decizii și măsuri care contribuie la reziliență;
  - **socială** – aceasta constă în măsuri special concepute pentru a diminua dezastrele care afectează negativ comunitățile și jurisdicțiile guvernamentale din cauza pierderii serviciilor critice datorate dezastrelor, și
  - **economică** – exprimă capacitatea de a reduce pierderile economice atât directe cât și indirecte rezultate în urma dezastrelor.

Ca și abordări ale măsurării rezilienței sunt: timpul necesar sistemului pentru a reveni la nivelul de funcționare normal; pierderea totală de performantă (diferența între performanța în timpul funcționării normale și cea din perioada manifestării perturbării).

Obiectivul programului ECIP[2] (Enhanced Critical Infrastructure Program) al Departamentul pentru Securitate Internă (DHS) al Statelor Unite ale Americii este colectarea de informații privind vulnerabilitatea şi criticalitatea unei varietăți de infrastructuri critice şi resurse cheie.

Inițial, programul ECIP a fost folosit pentru colectarea informațiilor despre vulnerabilitate (Index de vulnerabilitate) şi securitate (Index de măsurare a protecției). Totuşi, aceste măsuri nu oferă un indiciu despre posibilele urmări în cazul unei perturbări sau a unui dezastru asupra infrastructurile critice şi resurselor cheie. Pentru a depăşi acest fapt, Departamentul de Securitate Internă (DHS) împreună cu Centrul de asigurare a infrastructurii[3] (din cadrul laboratorului național Argonne) au dezvoltat un indice de măsurare a rezilienței (Fisher, Bassett, Buehring, Collins, Dickinson, & al., 2010). Obiectivul principal al Indicelui de Măsurare a Rezilienței este de a măsura capacitatea unei infrastructuri critice de a reduce magnitudinea şi/sau durata impacturilor unor fenomene perturbatoare. Indicele este folosit ca punct de referință pentru direcționarea investițiilor în infrastructură pentru îmbunătățirea rezilienței infrastructurii.

Indicele de măsurare a rezilienței (IMR) se bazează pe o analiză a deciziilor şi pe teoria utilității multi-atribut. Fiecare componentă a rezilienței este descompusă în subcomponentele sale individuale, care sunt apoi organizate pe cinci niveluri de informație. Al cincilea nivel de informație grupează datele care trebuie să fie colectate pentru a calcula IMR. Acesta este definit prin agregarea mai multor indici care caracterizează componentele şi subcomponentele. Deşi are în vedere componentele tradiționale ale rezilienței (anticipare, absorbție, adaptare şi recuperare), organizează măsurile de reziliență în concordanță cu procesele de managementul riscului şi a situațiilor de urgență.

5. Proiecte europene de creştere a rezilienței infrastructurilor critice

Uniunea Europeană prin intermediul programului de cooperare FP7-Security a sponsorizat, începând cu martie 2013, proiectul Rețelei de cercetare a pregătirii şi rezilienței Infrastructurilor Critice[4] (CIPRNet - Critical Infrastructure Preparedness and Resilience Research Network) prin intermediul căruia se realizează un Centru European de simulare şi analiză a infrastructurii critice. Acest centru va determina o îmbunătățire substanțială a răspunsurilor rapide şi adecvate din partea autorităților şi proprietarilor/operatorilor/administratorilor de infrastructuri critice în cazul unor situații de urgență complexe.

Rețeaua de cercetare va integra cunoştințe şi tehnologii pentru a creea capabilități suport pentru decizii cu valoare adăugată privind managementul situațiilor de urgență naționale şi multinaționale.

Consorțiul CIPRNet va implementa modele avansate şi capabilități de simulare şi analiză pentru documentarea unor răspunsuri mai eficiente la dezastre şi situații de urgență care afectează sau provin din infrastructurile critice complexe.

Proiectul CRISADMIN[5] (*Critical Infrastructure Simulation of Advanced Models on Interconnected Networks Resilience*) este un instrument capabil să evalueze impactul unor evenimente catastrofice şi/sau atacuri teroriste asupra infrastructurilor critice. Proiectul CRISADMIN studiază efectele produse de evenimente critice într-un mediu în care interdependențele dintre mai multe sectoare de infrastructură critică sunt modelate folosind o abordare de dinamică a sistemelor şi simulat într-un mediu sintetic. În lucrarea (Cavallini, et al., 2014) se discută despre caracteristicile cheie ale metodologiei. Scopul este acela de a oferi cercetătorilor şi profesioniştilor o metodologie pentru managementul crizei.

---

[2] ECIP - Enhanced Critical Infrastructure Protection, https://www.dhs.gov/ecip

[3] Decision and Information Sciences Division (actualmente Global Security Sciences), Argonne National Laboratory, http://www.gss.anl.gov/

[4] CIPRNet – Critical Infrastructure Prepardness and Resilience Research Network - https://www.ciprnet.eu/summary.html

[5] CRISADMIN - http://ec.europa.eu/dgs/home-affairs/financing/fundings/projects/stories/crisadmin_en.htm

În cadrul proiectului se constituie un sistem de suport decizional, folosit pentru a experimenta şi analiza interdependenţele dintre infrastructurile critice, precum şi modalităţile prin care acestea sunt afectate de evenimente catastrofale previzibile şi imprevizibile (atacuri teroriste, dezastre naturale şi industriale) şi investighează impactul posibilelor măsuri de contracarare şi politici de prevenire.

6. Concluzii

Infrastructurile critice devin indispensabile pe măsură ce populaţia solicită servicii noi şi diversificate. În mod evident, societatea modernă nu poate funcţiona, în cazul în care componentele majore ale infrastructurilor critice sunt deteriorate sau distruse. Marea majoritate a activelor de infrastructură critică nu pot fi în măsură să facă faţă ameninţărilor cibernetice sofisticate şi evolutive. Infrastructurile critice sunt active mari, complexe şi scumpe. Din moment ce nu este posibil să fie reconstruite aceste active pentru a ne asigura de o securitate concepută în interior, singura opţiune este aceea de a ne concentra pe integrarea mecanismelor convenţionale şi inovatoare de securitate în abordări de apărare bazate pe managementul riscului şi pe reziliență pentru a ne asigura că atacurile cibernetice reuşite nu duc la catastrofe.

Bunăstarea societăţii este tot mai dependentă de buna funcţionare a infrastructurilor critice iar crizele care afectează infrastructurile critice agravează impactul lor asupra societăţii. Prin urmare, îmbunătăţirea rezilienţei infrastructurilor critice este unul din cel mai importante obiective ale proprietarilor/operatorilor/administratorilor pentru managementul crizei.

Confirmare

Această lucrare a fost sprijinită din proiectul de cercetare CS146/2015, Plan Sectorial MCSI.

BIBLIOGRAFIE

1. **CAVALLINI, S.; D'ALESSANDRO, C.; VOLPE, M.; ARMENIA, S.; CARLINI, C.; BREIN, E.; ş.a:** A System Dynamics Framework For Modeling Critical Infrastructure Resilience. În I. I. 2014, Critical Infrastructure Protection VIII (pp. 141-154). J. Butts and S. Shenoi (Eds.): Critical Infrastructure Protection VIII, IFIP AICT 441.
2. **CHEREPANOV, A.:** BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry. Bratislava, 2016, Slovakia: http://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry.
3. **EUROPENE, C. U.:** Directiva 2008/114/CE privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesităţii de îmbunătăţire a protecţiei acestora. 2008, Jurnalul Oficial al Uniunii Europene.
4. **FISHER, R.; BASSETT, G.; BUEHRING, W.; COLLINS, M.; DICKINSON, D.E. ş.a.:** Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program. Chicago: Argonne National Laboratory, Decision and Information Sciences Division, 2010.
5. **FRANCIS, R.; BEKERA, B.:** A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliability Engineering and System Safety 121, 2014, pp. 90-103.
6. **HAGEROTT, M.:** Stuxnet and the vital role of critical infrastructure operators and engineers. International Journal of Critical Infrastructure Protection, vol. 7(4), 2014, pp. 244-246.
7. **HOLLING, C. S.:** Resilience and Stability of Ecological Systems. Institute of Resource Ecology, University of British Columbia, Vancouver, Canada, 1973.
8. **MACKENZIE, H.:** How Dragonfly Hackers and RAT Malware Threaten ICS Security. Belden, Indianapolis, Indiana: Industrial Security Blog, 2014.

9. **MCEER, M. C.:** *Engineering Resilience Solutions.* University of Buffallo, 2008.

10. **NIAC:** A Framework for Establishing Critical Infrastructure Resilience Goals. National Infrastructure Advisory Council, 2010.

11. **TEAM, S. A.:** sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks. Budapest, Hungary: Laboratory of Cryptography and System Security (CrySyS Lab), 2012.

12. **ZOBEL, C. W.:** Representing perceived tradeoffs in defining disaster resilience. Decision Support Systems, 2011, pp. 394-403.