SECURITATEA INFRASTRUCTURII CRITICE DE INFORMAȚIE – SISTEME DE DETECȚIE A INTRUZIUNII ÎN REȚELELE DE CALCULATOARE

CRITICAL INFORMATION INFRASTRUCTURE SECURITY – INTRUSION DETECTION SYSTEMS IN COMPUTER NETWORKS

General-locotenent (r) prof. univ. dr. Cristea DUMITRU*

Securitatea infrastructurii critice de informație se va asigura întotdeauna cu dificultate, tocmai datorită caracteristicilor care o fac de neînlocuit în funcționarea altor infrastructuri critice. Aceasta este descentralizată, interconectată, interdependentă, controlată de o multitudine de actori (în principal privați) şi încorporează tipuri de tehnologii diverse. Este aproape o axiomă faptul că avarierea infrastructurii critice de informație afectează sisteme aflate la mare distanță, iar problemele din spațiul cibernetic au consecințe directe asupra lumii reale. Într-adevăr, internetul poate fi utilizat ca un multiplicator pentru a amplifica efectele unui atac asupra unor infrastructuri critice. Provocările la adresa securității sporesc odată cu progresul tehnologic.Una dintre ultimele linii de apărare care completează schema de securitate de ansamblu a infrastructurii critice de informație este reprezentată de sistemele de detecție a intruziunilor în rețelele de calculatoare.

Cuvinte cheie: *securitatea infrastructurii critice de informație; sisteme de detecție a intruziunii; SCADA; NIDS.*

* Profesor universitar doctor, Universitatea Națională de Apărare, Bucureşti, România, membru corespondent al Academiei Oamenilor de Știință din România, Secția Științe Militare, membru AFCEA (Armed Forces Communications and Electronics Association – Asociația Forțelor Armate pentru Comunicații şi Electronică), general-locotenent (r), fost şef al J6 (Direcția Comunicații şi Informatică din Statul Major General) - (e-mail: dumitru.cristea@computerland.ro).
Prof., PhD, National Defence University, Bucharest, Romania, corresponding member of the Academy of Romanian Scientists, Military Sciences Section, AFCEA (Armed Forces Communications and Electronics Association) member, Lieutenant General (ret.), former Chief of Romanian J6 (Directorate of IT&C in General Staff) - (e-mail: dumitru.cristea@computerland.ro)

Critical Information Infrastructure security will always be difficult to ensure, just because of the features that make it irreplaceable for other critical infrastructures normal operation. It is decentralized, interconnected, interdependent, controlled by multiple actors (mainly private) and incorporating diverse types of technologies. It is almost axiomatic that the disruption of the Critical Information Infrastructure affects systems located much farther away, and the cyber problems have direct consequences on the real world. Indeed, the Internet can be used as a multiplier in order to amplify the effects of an attack on some critical infrastructures. Security challenges increase with the technological progress. One of the last lines of defense which comes to complete the overall security scheme of the Critical Information Infrastructure is represented by the Network Intrusion Detection Systems.

Keywords: *Critical Information Infrastructure Security; Intrusion Detection Systems; SCADA; NIDS.*

1. Introducere

Societatea modernă a devenit din ce în ce mai dependentă de disponibilitatea, fiabilitatea, siguranţa şi securitatea multor infrastructuri tehnologice. Sistemele informatice reprezintă o necesitate pentru umanitate atât datorită importantelor beneficii sociale şi economice pe care le oferă, cât şi consecinţelor grave care apar în urma avarierii lor. Infrastructurile critice constau în acele tehnologii fizice şi de informaţii, reţele, servicii şi bunuri care, în cazul deteriorării sau distrugerii, ar putea avea un impact serios asupra sănătăţii, siguranţei şi securităţii sau bunăstării economice ale cetăţenilor, ori asupra funcţionării eficiente a guvernelor. [1] În opinia noastră, pentru ca societatea să supravieţuiască, următoarele infrastructuri critice trebuie să funcţioneze, cel puţin la un nivel minim:

- furnizarea de apă, energie electrică şi combustibil;
- sistemul de transporturi şi comunicaţiile;
- asigurarea hranei şi managementul deşeurilor;
- sistemul financiar şi de asigurări;
- reţelele informatice şi de telecomunicaţii;
- sistemele de apărare militare;
- serviciile de urgenţă, de sănătate şi de salvare;
- sistemul juridic, agenţiile publice şi administraţia publică etc.

Furnizarea de energie electrică, precum şi reţelele informatice şi de telecomunicaţii pot fi considerate ca fiind de o importanţă crucială, întrucât celelalte infrastructuri critice le datorează funcţionarea corespunzătoare. Apreciem că în ultimele decenii, infrastructurile critice au devenit dependente de tehnologia informaţiei şi comunicaţiilor, cum este cazul reţelelor fixe şi mobile de telefonie, Internetului sau a reţelelor terestre şi satelitare destinate managementului informaţiilor, comunicaţiilor şi funcţiilor de control. Infrastructura critică de

informaţie controlează managementul centralelor electrice, barajelor, sistemului energetic naţional, sistemelor de control ale traficului aerian, sistemelor de distribuţie a utilităţilor publice, sistemului financiar, pentru a numi numai câteva din elementele constituente ale infrastructurilor critice. Sprijinul acestor instalaţii fizice sensibile pe infrastructura critică de informaţie determină ca securitatea infrastructurii critice de informaţie să reprezinte un interes naţional.

Evaluarea gradului de securitate a infrastructurii critice de informaţie, precum şi o serie de analize şi rapoarte realizate de părţile interesate din sectorul public şi privat subliniază atât dependenţa socială, politică şi economică de tehnologia informaţiei şi comunicaţiilor a societăţii contemporane, cât şi creşterea constantă a numărului, amplorii, gradului de sofisticare şi a impactului ameninţărilor naturale sau generate de oameni. Asistăm în prezent la o tendinţă de utilizare a tehnologiei informaţiei şi comunicaţiilor în scopul obţinerii supremaţiei politice, economice şi militare, inclusiv prin capacităţi ofensive.

Guvernele şi ansamblul furnizorilor de servicii vitale nu fac cunoscute publicului deficienţele de securitate şi reziliență decât dacă sunt obligaţi să o facă. Chiar şi în aceste condiţii, se cunosc numeroase exemple de ameninţări la adresa infrastructurilor critice cauzate de deficienţele de securitate şi de reziliență de la nivelul infrastructurilor critice de informaţie:

- în 2007 şi 2008, au avut loc atacuri cibernetice de amploare în Estonia, Lituania şi Georgia;
- în 2008, întreruperea cablurilor submarine intercontinentale din Mediterana şi din Golful Persic a afectat traficul internet în numeroase ţări;
- în aprilie 2009, responsabilii federali cu securitatea din SUA au avertizat cu privire la pătrunderea în reţeaua electrică a SUA a unor „spioni cibernetici”, în urma cărora au rămas în reţea programe informatice care ar putea fi folosite pentru a perturba sistemul;
- în luna iulie 2009, SUA şi Coreea de Sud au fost nevoite să facă faţă unor întreruperi manifeste ale serviciilor (implicând preluarea controlului asupra unui număr de 100.000-200.000 de calculatoare, devenite „zombi”), ceea ce a afectat funcţionarea a numeroase site-uri guvernamentale.

În plus, după cum o arată şi recentele evenimente sud-mediteraneene, unele regimuri sunt pregătite şi capabile să interzică sau să submineze în mod arbitrar accesul propriilor lor cetăţeni la mijloacele informatice de comunicare, în special internetul şi comunicaţiile mobile, în scopuri politice. Astfel de intervenţii interne unilaterale pot avea consecinţe grave asupra altor părţi ale lumii. [2]

Pentru a înţelege şi mai bine aceste diferite ameninţări, acestea pot fi împărţite în următoarele categorii:

– pentru **exploatare**, cum ar fi ameninţările avansate persistente sau atacurile neîntrerupte şi coordonate împotriva agenţiilor guvernamentale, în scopul spionajului economic şi politic (de exemplu, Ghost Net [3]), furtul de identitate,

recentele atacuri împotriva sistemului de comercializare a cotelor de emisii sau împotriva sistemelor informatice guvernamentale;

– pentru **sabotaj**, cum ar fi atacurile de tip DDoS (Distributed Denial of Service – blocarea distribuită a serviciului) sau spamurile generate prin botneturi (de exemplu, reţeaua Conficker de 7 milioane de calculatoare şi reţeaua Mariposa din Spania de 12,7 milioane de calculatoare), Stuxnet şi întreruperea mijloacelor de comunicare;

– pentru **distrugere**. Acesta este un scenariu care încă nu s-a materializat, însă, dată fiind utilizarea crescândă a tehnologiei informaţiei şi comunicaţiilor în infrastructurile critice (de exemplu, reţelele inteligente şi reţelele de distribuţie a apei), el nu este exclus pentru anii care vin.[4]

Aşa cum menţionam anterior, infrastructura critică de informaţie joacă un rol fundamental în managementul unor infrastructuri critice, cum ar fi reţeaua de energie electrică, producţia de petrol şi gaze naturale, reţelele de alimentare cu apă etc. O trăsătură comună a acestor infrastructuri critice o reprezintă utilizarea largă a informaţiilor distribuite şi a sistemelor de comandă şi control, atât pentru a asigura servicii mai eficiente, cât şi pentru a satisface cerinţele consumatorilor. Pentru a conduce, controla şi supraveghea funcţionarea unor infrastructuri atât de complexe sunt utilizate în prezent sistemele de control SCADA (Supervisory, Control, and Data Acquisition – achiziţia de date, control şi supraveghere). Sistemele SCADA sunt sisteme informatice modeme, destinate urmăririi şi conducerii operative a proceselor industriale, pe baza datelor achiziţionate on line de la un număr foarte mare de unităţi echipate cu senzori capabili să colecteze informaţii despre starea infrastructurii şi dispozitivelor de acţionare.centralizate. Dar sistemele bazate pe SCADA nu sunt securizate, atât timp cât sistemele şi reţelele folosesc produse comerciale, echipamentele de reţea sunt bazate pe IP, iar interconectarea necesită serviciul de internet, care finalmente deschide uşa potenţialilor agresori.

2. Măsuri tehnice de asigurare a securităţii infrastructurii critice de informaţie

În urma analizării mai multor rapoarte asupra securităţii spaţiului cibernetic şi a lecţiilor învăţate rezultate în urma atacurilor cibernetice, apreciem ca fiind de maximă importanţă adoptarea următoarelor măsuri tehnice pentru asigurarea securităţii infrastructurii critice de informaţie:

- **Tehnologii de autentificare** – schemele de autentificare pentru elemente constitutive ale reţelelor, cum ar fi echipamentele hardware, aplicaţiile software, datele şi utilizatorii sunt necesare pentru o largă varietate de scopuri, ce includ identificarea, autentificarea şi verificarea integrităţii datelor. Aceste scheme trebuie să îşi dovedească siguranţa, să fie uşor de verificat, să poată fi utilizate de o multitudine de componente şi să fie executabile rapid. Metodele de criptografiere tradiţională s-au concentrat pe asigurarea securităţii, dar acestea nu pot fi suficient de eficiente în cazul utilizării extinse, în medii în care, de exemplu, un singur ruter

de reţea trebuie să autentifice milioane de pachete de date pe secundă. Rezultate mult mai bune au fost obţinute cu protocoalele criptografice.

- **Securizarea protocoalelor de bază** – puţine dintre protocoalele ce guvernează funcţionarea internetului au un grad de securitate adecvat. De exemplu, pentru a devia traficul de date pe un site alternativ, un atacator poate păcăli cu uşurinţă protocoale cum este şi Border Gateway Protocol (BGP) (care controlează traseele urmate de pachetele de date în circulaţia acestora pe internet) sau servicii de tipul Domain Name System (DNS) (care controlează destinaţia pachetelor de date). Astfel de atacatori pot intercepta, monitoriza, altera sau manipula traficul pe internet, adeseori fără a putea fi detectaţi. Pentru ca internetul să devină un mediu de comunicaţie de încredere, trebuie dezvoltate versiunile securizate ale protocoalelor de bază care să contracareze ameninţări cum ar fi interzicerea de servicii, alterarea datelor şi inducerea în eroare. Mai mult, apreciem că trebuie securizate protocoalele de bază împotriva atacurilor de incapacitare, care exploatează slăbiciunile protocoalelor.

- **Securizarea ingineriei software şi a asigurării software** – ingineria aplicaţiilor software comerciale suferă de lipsa unor controale ştiinţifice riguroase, necesare pentru producerea unor aplicaţii de calitate, securizate, la un cost acceptabil. Practicile de inginerie software obişnuite permit apariţia unor erori periculoase, care permit multor programe de atac să compromită, în fiecare an, funcţionarea a milioane de calculatoare.

- **Securitatea holistică a sistemului** – securitatea eficientă într-o infrastructură globală, stratificată şi complexă, cum este internetul şi nodurile sale, impune mai mult decât securizarea componentelor sale. Realizarea unor metode clare de autentificare, protocoale de securitate pentru operaţiunile Web de bază, precum şi îmbunătăţirea ingineriei software fac parte din ecuaţia care trebuie să rezolve problema securităţii pe internet. Cu toate acestea, cel mai important aspect pe care cercetătorii trebuie să îl ia în consideraţie îl reprezintă abordarea arhitecturală end-to-end a securităţii întregului, care transcede securitatea fiecărui element în parte. Cercetarea fundamentală trebuie să dezvolte arhitecturi de securitate holistică cu totul noi, care să includă echipamentele hardware, sistemele de operare, reţelele şi aplicaţiile software.

- **Monitorizarea şi detectarea** – indiferent de progresul realizat în cercetare, tot pot apărea evenimente neanticipate. Atunci când se întâmplă aşa ceva, sunt necesare instrumente care să permită monitorizarea şi înţelegerea evenimentului, precum şi adoptarea măsurilor defensive corespunzătoare. Capacitatea instrumentelor curente care monitorizează activităţile anormale din reţea de a identifica rapid cauzele este insuficient evoluată. Avantajul pe care îl au în prezent atacatorii va creşte pe măsură ce aceştia se perfecţionează, iar internetul devine tot mai vast şi mai complex.

- Metodologii de atenuare a efectelor atacurilor şi de recuperare – sistemele securizate trebuie să fie astfel proiectate încât să răspundă rapid la atacuri şi evenimente neprevăzute şi să aibă capacitatea de recuperare în urma oricărei avarii rezultate, o sarcină cu atât mai provocatoare atunci când este cazul unui sistem de amploarea şi complexitatea internetului şi nodurilor sale. Această problemă a fost abordată în sisteme de extraordinară complexitate, cum este cazul navetelor spaţiale, prin realizarea unor investiţii substanţiale pentru obţinerea unor fiabilităţi şi redundanţe maxime. Nici-un efort comparabil nu a fost investit în dezvoltarea metodelor de fiabilizare a internetului şi a sistemelor de calculatoare în faţa atacurilor.

- Prinderea atacatorilor şi descurajarea activităţilor informatice ilegale – arestarea şi condamnarea rapidă a atacatorilor constituie principalul obiectiv al aplicării legii şi serveşte, în egală măsură, şi ca o metodă de descurajare a activităţilor informatice ilegale. Capabilităţile curente de investigare a infracţiunilor informatice, identificarea făptaşilor, adunarea şi prezentarea probelor şi condamnarea atacatorilor sunt doar satisfăcătoare.

- Modelarea şi bancuri de probe pentru noile tehnologii – una dintre barierele în calea dezvoltării rapide a noilor produse de securitate cibernetică o reprezintă insuficienţa modelelor realiste şi a bancurilor de probă pentru testarea celor mai avansate tehnologii într-un mediu similar celui din realitate. Până acum au fost realizate unele cercetări de modelare a internetului, dar au fost oarecum simpliste şi cu un impact mic în practică. Problema este de mare dificultate din cauza complexităţii şi mărimii internetului.

- Probleme non-tehnologice ce pot compromite securitatea cibernetică – un mare număr de factori non-tehnologici – psihologici, societali, instituţionali, legali şi economici – pot compromite securitatea cibernetică într-un mod ce nu poate fi rezolvat doar de reţea sau ingineria software. Instalarea tehnologiilor ce nu ţine cont de aceşti factori poate agrava problemele ce se intenţionează a fi rezolvate. Cercetarea asupra aspectelor umane şi organizaţionale ale infrastructurii critice de informaţie poate explora soluţii ce vizează şi comportamentul uman.

3. Sistemele de detecţie a intruziunii – delimitări conceptuale

Tehnicile de prevenire tradiţionale, cum sunt autentificarea utilizatorilor, criptarea datelor, evitarea erorilor de programare şi firewall-urile fac parte din prima linie de apărare pentru securitatea reţelelor. Întrucât toate aceste metode au şi puncte slabe ce pot afecta securitatea de ansamblu a unei reţele, ne-am propus ca să abordăm şi să dezvoltăm în comunicarea noastră problematica sistemelor de detecţie a intruziunii în reţelele de calculatoare.

Detecţia intruziunilor este procesul de monitorizare a evenimentelor apărute la nivelul unui sistem de calcul sau al unei reţele, precum şi de analizare a acestora pentru a căuta semne de intruziuni. Intruziunile sunt încercările de realizare a unor acţiuni neautorizate de penetrare, prin ocolirea mecanismelor de securitate ale unui

sistem de calcul şi/sau reţele. Acestea sunt cauzate de atacatori care accesează sistemul din internet, utilizatori autorizaţi ai sistemului care încearcă să obţină privilegii suplimentare pentru care nu au permisiuni sau utilizatori autorizaţi care folosesc în mod inadecvat privilegiile care le sunt alocate. [5]

Un sistem de detecţie a intruziunilor (IDS - Intrusion Detection System) este un sistem software/hardware responsabil cu detectarea de date suspecte a căror prezenţă poate fi considerată neautorizată în reţea. Sistemul IDS inspectează toată activitatea reţelei şi identifică structuri de date suspecte ce pot indica un atac din partea cuiva care încearcă să se conecteze sau să compromită un sistem. Spre deosebire de un firewall, care limitează accesul în reţea pentru a preveni intruziunile fără a semnaliza însă un atac sau o conexiune neautorizată din interiorul reţelei, un IDS evaluează activităţile suspecte de intruziune şi le semnalizează. Sistemul IDS capturează şi inspectează tot traficul, indiferent dacă acesta este permis sau nu, urmând ca pe baza conţinutului pachetelor transmise în reţea, la nivel IP sau la nivel aplicaţie, să declanşeze o alarmă în momentul apariţiei unui eveniment suspect. Dezvoltând aceste procese, IDS analizează sursa de date, iar după preprocesarea intrărilor permite unui motor de detecţie să decidă, pe baza unui set de criterii de clasificare, dacă respectivele date sunt normale sau nu, în conformitate cu un model comportamental. Acest proces este, în mod evident, mult mai complicat în situaţia asigurării securităţii în timp real, întrucât analiza comportamentală a utilizatorului trebuie realizată cât mai repede posibil pentru a reduce pierderea pachetelor de date. Odată ce a fost determinat comportamentul utilizatorului, acesta este folosit pentru a defini un set de criterii de clasificare, necesar motorului de detecţie pentru a identifica activităţile anormale. [6]

Sistemele IDS sunt de regulă de trei tipuri: sisteme hardware de sine stătătoare care supraveghează traficul, aplicaţie software pentru un server dedicat sau un modul hardware de tip „add-in“, pentru firewall-ul existent. Sistemele IDS analizează traficul de date şi pot controla o gamă largă de tipuri de atacuri, inclusiv DoS (Denial of Service) sau DDoS (Distributed Denial of Service), care tind de obicei să blocheze activitatea în reţea sau accesul utilizatorilor la resursele necesare.

Astăzi există sisteme IDS dedicate monitorizării şi protecţiei atât la nivel de reţea, cât şi local, la nivel de server şi chiar de desktop. Soluţiile dedicate protecţiei la nivel de reţea se împart la rândul lor în două categorii:

- OnLine IDS - sisteme ce analizează traficul într-un nod de reţea, în mod ascuns, de la distanţă, fără ca traficul să treacă efectiv prin punctul în care acestea sunt instalate. OnLine IDS poate monitoriza tot traficul dintr-o reţea, atât extern, cât şi intern, el fiind conectat pe portul de monitorizare al switch-ului respectiv, punct în care poate fi colectat întreg traficul. Acest tip de IDS reuşeşte să analizeze traficul în întregime şi să alerteze asupra activităţilor neconforme politicii de securitate stabilite la nivel de reţea, putând chiar să ia măsuri de blocare a

conexiunilor sau sesiunilor respective, ori să administreze şi să modifice politicile pentru firewall.

- InLine IDS - sisteme ce monitorizează o anumită conexiune şi analizează traficul în mod direct, reprezentând un filtru instalat în spatele unui firewall şi în faţa serverelor şi sistemelor critice din reţea. InLine IDS monitorizează doar traficul din punctul de conexiune, traficul trecând chiar prin el, rolul său fiind acela de a recunoaşte atacurile şi acţiunile neconforme politicilor impuse şi de a filtra orice trafic neutorizat în acel punct.

Sistemele de detectare a intruziunilor pentru server (HIDS – Host-based Intrusion Detection Systems), monitorizează aplicaţii şi fişiere specifice, inclusiv setările regiştrilor, alertând în cazul accesării neautorizate, modificării, ştergerii, sau copierii datelor rezidente pe sistemul monitorizat. Rolul lor este de a menţine politicile (seturile de reguli) impuse respectivului server şi de a semnala orice încercare de accesare neautorizată, putând chiar înlocui automat fişierele deteriorate, pentru a asigura integritatea datelor. O alternativă a HIDS sunt sistemele centralizate de detectare a intruziunilor în reţele (CHIDS – Centralized Host-based Intrusion Detection Systems) care servesc aceluiaşi scop, dar realizează o analiză centralizată prin trimiterea tuturor datelor într-un nod central de analiză.

Capacitatea de a alerta numai în cazul unor atacuri reale şi cu adevărat periculoase pentru reţeaua informatică respectivă face diferenţa între un sistem IDS bun şi restul. De aceea, pentru a obţine o soluţie competitivă, un IDS bun trebuie dublat de o configurare specializată, de întreţinere şi adaptare realizate de profesionişti.

Multe dintre sistemele IDS dezvoltate până acum pentru a răspunde atacurilor cibernetice îndreptate asupra reţelelor întâmpină probleme în procesarea în timp real a volumului de trafic, care creşte în continuu. Pe cale de consecinţă, se impune adaptarea tehnicilor de analiză a securităţii pentru procesarea unui volum de trafic ridicat, în reţele de mare viteză, cum sunt reţelele Gigabit Ethernet.

4. Sisteme de detecţie a intruziunii în reţele de mare viteză

Sistemele de detecţie a intruziunilor în reţea (NIDS – Network Intrusion Detection Systems) reprezintă un instrument important şi practic pentru securitatea reţelei. Acestea efectuează analiza de securitate a pachetelor de date prin monitorizarea reţelei. Creşterea constantă a vitezei reţelelor şi volumului traficului de date a impus noi probleme acestor sisteme. În opinia noastră, pentru a avea garanţia unei detecţii de precizie a intruziunilor, NIDS trebuie să detecteze pachetele de date la viteza de transfer a datelor în reţea. Pentru a menţine performanţele şi eficienţa IDS şi având în vedere tendinţa de proliferare a reţelelor de mare viteză, studiile au arătat că se impune alegerea IDS cu arhitectură distribuită. [7] Într-o astfel de configuraţie, traficul de reţea este preluat de o multitudine de senzori care procesează, fiecare în parte, doar o fracţiune a traficului, reducând posibilitatea pierderilor de pachete de date din cauza

supraîncărcării. Fiecare senzor citeşte pachetele de date, le compară conţinutul cu baza de date a semnăturilor de atac şi transmite alarme către unitatea de management atunci când este detectat un atac sau un comportament ce contravine politicilor de securitate. Unitatea de management a NIDS recepţionează alarmele sau pachetele suspecte, le stochează într-un fişier şi lansează acţiunile corespunzătoare. Acţiunile de răspuns ale unităţii de management a NIDS pot fi: notificarea administratorului de reţea, reconfigurarea automată a sistemului pentru blocarea intruziunii sau implementarea unor mecanisme care să ofere suportul pentru intervenţia manuală asupra sistemului. [8]

Un astfel de NIDS are, în opinia noastră, următoarele caracteristici:

- utilizează servere obişnuite, fără cerinţe de hardware speciale;
- rulează pe reţele de mare viteză stabil şi asigură o rată mică de pierdere a pachetelor de date;
- asignează traficul spre noduri cât mai echilibrat posibil şi se adaptează varietăţii traficului din reţea;
- realizează un echilibru corespunzător între rata de pierdere a pachetelor de date şi complexitatea algoritmului de lucru;
- integrează mesajele de alertă emise la nivel de nod pentru a detecta atacurile multi-obiect îndreptate asupra întregii reţele;
- asigură simultan raportul de înalt nivel între obiectivul de analiză a tendinţei macroscopice a securităţii reţelei, sugestiile de răspuns şi cele de reacţie.

Având capabilitatea de a procesa şi analiza în timp real securitatea de reţea pentru reţelele de mare viteză, arhitectura distribuită a NIDS permite o mai bună scalabilitate şi flexibilitate a structurii ierarhice. [9] Pe baza acestei arhitecturi, NIDS va monitoriza cu eficienţă gradul de securitate al reţelelor infrastructurii critice de informaţie, oferind o mai bună evaluare şi predicţie a ameninţărilor şi atacurilor cibernetice.

5. Concluzii

Sistemele de control ale infrastructurilor critice sunt din ce în ce mai expuse ameninţărilor atacurilor cibernetice, datorită utilizării reţelelor informatice şi de comunicaţii tip IP. Mai mult, apreciem că informaţia digitală are o importanţă sporită pentru operarea infrastructurilor critice, iar ca rezultat, ceea ce numim infrastructura critică de informaţie condiţionează integrarea şi interoperarea elementelor ce compun fiecare infrastructură critică.

Demersul studiului nostru a avut drept scop evidenţierea noilor modalităţi de control şi management ale securităţii infrastructurii critice de informaţie prin utilizarea sistemelor de detecţie a intruziunii în reţelele de calculatoare.

NOTE BIBLIOGRAFICE

[1] Cf. Commission of the European Communities, *Critical Infrastructure Protection in the Fight Against Terrorism*, COM (2004) 702 final, Brussels, 20.10.2004, p.3.
[2] Comunicare comună privind Parteneriatul pentru democraţie şi prosperitate împărtăşită cu ţările sud-mediteraneene, COM (2011) 200, 08.03.2011.
[3] Rapoartele proiectului *Information Warfare Monitor*: "*Tracking Ghost Net: investigating a Cyber Espionage Network*" (2009) şi "*Shadows in the Cloud: Investigating Cyber Espionage 2.0*" (2010).
[4] World Economic Forum*, Global Risks 2011*.
[5] [8] Sorin SOVIANY, Sorin PUŞCOCI, Gheorghiţă PESCARU, Radu DRAGOMIR, *Sisteme de detecţie a intruziunilor*, Telecomunicaţii, Anul LI, nr.2/2008, p.45.
[6] Salvatore D'ANTONIO, Francesco OLIVIERO, Roberto SETOLA, *High-Speed Intrusion Detection in Support of Critical Infrastructure Protection*, Lecture Notes in Computer Science, Volume 4347/2006, p.224.
[7] Cristopher KRUEGEL, Fredrik VALEUR, Giovanni VIGNA, Richard KEMMERER, *Stateful Intrusion Detection for High-speed Networks*, Proceedings of IEEE Symposium on Security and Privacy, 2002.
[9] Zhi-Jun LU, Jing ZHENG, Hao HUANG, *A Distributed Real-Time Intrusion Detection System for High-Speed Network*, Journal of Computer Research and Development, 2004.

ABREVIERI

BGPBorder Gateway Protocol
CHIDSCentralized Host-based Intrusion Detection System
DDoSDistributed Denial of Service
DNSDomain Name System
DoSDenial of Service
HIDSHost-based Intrusion Detection System
IDSIntrusion Detection System
IPInternet Protocol
NIDSNetwork Intrusion Detection System
SCADA Supervisory, Control, and Data Acquisition