DEZVOLTAREA DURABILĂ A AGENȚILOR ADAPTIVI PENTRU IDENTIFICAREA INTRUZIUNILOR ÎN SISTEME ȘI REȚELE INFORMAȚIONALE

Andrei ȘESTACOV, doctorand

Academia Militară „Alexandru cel Bun”

Rezumat. În prezenta lucrare se cercetează dezvoltarea durabilă a agenților adaptivi pentru identificarea intruziunilor în sistemele şi rețelele informaționale fiind structurată în: introducere; dezvoltarea durabilă a agenților adaptivi la identificarea intruziunilor în rețele informaționale; procesul de integrare a agenților adaptivi la identificarea intruziunilor în rețele informaționale; monitorizarea şi analiza activității agenților adaptivi în rețele informaționale; concluzii și bibliografie.

Cuvinte cheie: identificarea intruziunilor, sisteme si rețele informaționale, dezvoltare durabilă, societate informațională, economie digitală, securitate informațională, Sisteme de Detecție și Prevenire a Intruziunilor.

SUSTAINABLE DEVELOPMENT OF ADAPTIVE AGENTS FOR THE IDENTIFICATION OF INTRUSIONS IN SYSTEMS AND INFORMATION NETWORKS

Abstract. In the present paper is researching sustainable development of adaptive agents to identify intrusion in systems and information network and it is structured in: introduction; sustainable development of adaptive agents to identify intrusion in information network; integration of adaptive agents to identify intrusion in information network; monitoring and analysis activities of adaptive agents in information network; conclusions and bibliography.

Keywords: identify intrusions; systems and information network; sustainable development; information society; digital economy; information security; Intrusion Detection-Prevention Systems.

Introducere

În condițiile modificării tehnologiei informaționale, globalizării mediului informațional și creșterii explozive a fluxului informațional devine tot mai evident rolul securității informaționale. În acest sens, conținutul lucrăriii aduce în atenție şi deschide noi oportunități de abordare a unor idei şi perspective de dezvoltare durabilă a sistemelor informatice, propune soluții realiste şi viabile în măsură să asigure identificarea intruziunilor în sisteme și rețele informaționale.

Identificarea intruziunilor este o problemă actuală majoră cu care se confruntă societatea electronică, care se referă la asigurarea integrității, confidențialității şi disponibilității informației. Lucrul în rețea şi conectarea la Internet induc riscuri suplimentare, de acces neautorizat la date sau chiar fraudă pentru care organizațiile trebuie să implementeze noi măsuri de control și protecție potrivită atacurilor din ce în ce mai sofisticate la nivel de rețea și nivel de aplicație [2, 5].

Este important ca organizațiile să conştientizeze riscurile asociate cu utilizarea tehnologiei şi gestionarea informațiilor, să abordeze pozitiv acest subiect printr-o conştientizare în rândul angajaților a importanței securității informațiilor, înțelegerea

tipologiei ameninţărilor, riscurilor şi vulnerabilităţilor specifice mediilor informatizate şi aplicarea practicilor de control [1, 3, 4, 6 – 14].

În Republica Moldova există mai multe instituţii implicate în procesul de detectare şi identificare a intruziunilor în sisteme si reţele informaţionale, fiecare cu atribuţiile şi responsabilităţile sale: Serviciul de Informaţii şi Securitate, Ministerul Afacerilor Interne, Procuratura, Ministerul Tehnologii Informaţiilor şi Comunicaţiei, Centrul de Telecomunicaţii Speciale, Centru Naţional de Protecţie a Datelor cu Caracter Personal [15, 16].

Societatea informatică integrează obiectivele dezvoltării durabile, bazată pe dreptate socială şi egalitate a şanselor, protecţie ecologică, libertate, diversitate culturală şi dezvoltare inovativă, restructurarea industriei şi a mediului de afaceri.

Schimbările majore din ultimii ani - creşterea exponenţială a comunicaţiilor mobile şi a utilizatorilor de Internet, contribuţia sectorului Tehnologiei Informaţiei şi Comunicaţiilor (TIC) la creşterea economică şi la crearea locurilor de muncă, restructurarea/reingineria companiilor şi a business-ului în general pentru a beneficia mai eficient de noile tehnologii, dezvoltarea accelerată a comerţului electronic - susţin tranziţia de la era industrială la cea post-industrială, trecerea la „noua economie”.

Noile tehnologii digitale fac ca accesul, stocarea şi transmiterea informaţiei să fie din ce în ce mai facile şi mai accesibile ca tarife. Dispunând de informaţia digitală, aceasta poate fi transformată în noi valori economice şi sociale, creând imense oportunităţi pentru dezvoltarea de noi produse şi servicii. Informaţia devine resursa-cheie şi factor de producţie pentru economia digitală.

Începând cu anii '90 penetrarea rapidă a calculatoarelor personale (PC), evoluţia tehnologiilor software, dezvoltarea explozivă a reţelelor de comunicaţie de date şi a serviciilor bazate pe Internet au produs schimbări profunde la scară mondială.

Comerţul electronic la scară globală, inter-companii (de tip „business-to-business”) a atins în anul 2016 valoarea de 844 miliarde euro şi se estimează să ajungă la 12.869 miliarde euro în 2017, adică cu o rată de creştere anuală de 73% .

Aceste evoluţii s-au datorat în mare măsură atât progreselor tehnologice cât şi promovării unor politici noi privind privatizarea şi promovarea competiţiei pe piaţa TIC, noilor reglementări tehnice şi juridice în domeniu, noilor strategii naţionale şi regionale de dezvoltare a societăţii informatice. Toate ţările dezvoltate şi-au elaborat şi implementat politici guvernamentale susţinute privind cercetarea, dezvoltarea şi adoptarea noilor tehnologii, consolidarea infrastructurilor informaţionale naţionale, formarea şi atragerea de specialişti în domeniul TIC (inclusiv din alte ţări), educarea populaţiei adulte, cooperarea cu sectorul privat şi încurajarea investiţiilor în această nouă ramură economică, promovarea de proiecte guvernamentale menite să demonstreze utilitatea serviciilor specifice societăţii informatice.

Construirea noului model de societate ridică astfel probleme socio-politice majore - atât la scară națională, cât şi internațională - de atenuare a fenomenului de excludere de la beneficiile noilor tehnologii a unor categorii sociale şi a unor regiuni/zone geografice şi de coeziune socială, de conservare şi promovare a culturii specifice fiecărei națiuni şi comunități locale, de protecție a cetățeanului şi consumatorului. Soluționarea acestor probleme nu se poate realiza decât printr-un dialog larg între autoritățile guvernamentale, reprezentanții mediului de afaceri, ai mediului academic şi societatea civilă, atât la nivel național, regional, cât şi global.

Guvernele şi instituțiile acestora au rolul de a stimula, conduce, controla şi participa activ la acest proces de tranziție către Societatea Informațională prin programe de acțiune concrete şi prin inițierea unui nou cadru de reglementări specifice. Prin noile legi, norme, standarde şi reglementări care vor fi elaborate, se va stimula, pe de o parte, dezvoltarea noilor servicii specifice Societății Informatice (comerț şi tranzacții electronice, informatizarea serviciilor publice, accesul cetățeanului şi agenților economici la informația publică etc.), iar pe de altă parte, se vor asigura regulile etice de a munci şi trăi într-un nou tip de societate (protecția vieții private şi a datelor personale, confidențialitatea tranzacțiilor, protecția consumatorului etc.).

La rândul său, comunitatea de afaceri din domeniul tehnologiilor informației şi comunicațiilor oferă produse şi servicii de înalt nivel tehnologic, accesibile ca prețuri şi tarife. Totodată se formează o nouă cultură a competitivității agenților economici din toate sectoarele în noul tip de economie, economia digitală. Prin complexitatea fenomenelor pe care le implică dezvoltarea societății informaționale, prin necesitatea formării unei noi culturi a cunoaşterii şi a învățării în condițiile utilizării noilor tehnologii a cercetării-dezvoltării şi inovării tehnologice, participarea activă a comunității academice (instituții de cercetare, de educație şi de cultură) devine de asemenea esențială.

Societatea civilă are de asemenea atât un rol proactiv prin formularea de cerințe şi priorități privind modul de utilizare al noilor tehnologii în folosul întregii societăți, cât şi reactiv față de politicile şi reglementările guvernamentale. Aceste roluri pot fi exercitate atât la nivel de grup (organizații non guvernamentale, asociații profesionale etc.), cât şi la nivel individual. Drepturile cetățeanului şi consumatorului în societatea informațională au noi dimensiuni şi se pot manifesta sub noi forme.

Dezvoltarea durabilă a agenților adaptivi la identificarea intruziunilor în rețele informaționale

Etapa actuală de dezvoltare a Republicii Moldova se caracterizează prin dezvoltarea şi răspândirea rapidă a tehnologiilor informaționale, prin rolul avansat al domeniului informațional, ce include totalitatea informației, infrastructurii tehnologiei informației şi comunicațiilor (TIC), instituțiilor care prelucrează informația şi a sistemului ce reglementează relațiile sociale apărute în acest context.

Fiind o parte importantă şi indispensabilă a vieţii societăţii moderne, domeniul informaţional influenţează activ asupra stării componentelor de stat, sociale, militare, economice şi a altor componente ale securităţii naţionale. Totodată, securitatea naţională depinde considerabil de asigurarea securităţii informaţionale a persoanei, societăţii şi statului.

Pe parcursul ultimilor ani a crescut semnificativ necesitatea unei abordări complexe şi eficiente a procesului de asigurare a securităţii spaţiului informaţional naţional, inclusiv al infrastructurii critice naţionale, de asigurare şi protecţie a informaţiei atribuite la secret de stat, de prevenire şi combatere a crimelor informaţionale, extremismului şi terorismului în spaţiul informaţional.

Importanţa problemei a fost conturată în Concepţia securităţii naţionale şi Strategia securităţii naţionale a Republicii Moldova, care, stabilind obiectivele sistemului de securitate naţională, au reflectat atât ameninţările din domeniul tehnologiilor informaţionale, cât şi asigurarea securităţii informaţionale.

Adoptarea Concepţiei este determinată de necesitatea protecţiei intereselor persoanelor, societăţii, statului în domeniul informaţional, importanţa pericolelor securităţii informaţionale în societatea modernă, de necesitatea menţinerii unui echilibru între interesele persoanelor, societăţii, statului pentru asigurarea securităţii informaţionale.

Perfecţionarea bazei normative în domeniul dat este determinată de elaborarea şi consolidarea normativă a anumitor drepturi şi obligaţiuni ale statului, instituţiilor administraţiei publice, persoanelor cu funcţii de răspundere, organizaţiilor care asigură securitatea informaţională, mecanismelor de realizare a drepturilor şi obligaţiunilor date. Consolidarea acestora va permite sistematizarea relaţiilor sociale privind asigurarea securităţii informaţionale, înlăturarea incertitudinilor şi limitelor discreţionare în domeniul dat.

Echipele de răspuns la incidente de securitate există în toată lumea pentru a ajuta utilizatorii să reacţioneze la atacurile îndreptate asupra echipamentelor IT, indiferent de tehnologia utilizată sau din ce organizaţie face parte utilizatorul respectiv. Multe organizaţii au echipe interne de răspuns la incidente al căror scop este tratarea incidentelor din punctul de vedere al instituţiei respective pentru a proteja utilizatorii şi/sau clienţii săi. Guvernele naţionale organizează echipe de răspuns la incidente de securitate la nivel de ţară, pentru a contracara atacuri masive şi specializate asupra cetăţenilor, a companiilor şi a infrastructurilor de importanţă naţională - unele dintre acestea critice pentru o bună existenţă şi funcţionare a societăţii. Două exemple de astfel de atacuri sunt atacurile de tip distribuit asupra serviciilor (Distributed Denial of Service - DDoS) şi atacurile de tip „phishing”.

Serviciul Trusted-Introducer a fost înfiinţat în Europa în anul 2000 pentru a facilita colaborarea între astfel de echipe de răspuns şi, prin urmare, pentru a creşte nivelul de

securitate prin răspunsul mai rapid la atacurile în desfăşurare şi a ameninţărilor de tip nou. TI asigură o bază de încredere, cu servicii adiţionale specializate pentru toate echipele de răspuns la incidente de securitate. De asemenea, TI administrează o bază de date cu informaţii despre astfel de echipe existente şi oferă o imagine de ansamblu actualizată asupra nivelului lor demonstrat de maturitate şi abilitate. Pentru garantarea acestor informaţii a fost conceput un mecanism de acreditare şi certificare bazat pe cele mai bune practici dezvoltate şi testate de-a lungul timpului în cadrul aceleeaşi comunităţi TI.

Pentru îndeplinirea obiectivelor sale, acest serviciu, asigură tuturor utilizatorilor săi accesul gratuit la o bază de date cu echipele de răspuns. Această bază de date conţine informaţii despre toate echipele de răspuns cunoscute şi înregistrate care sunt acceptate de comunitatea Trusted-Introducer. Putem căuta în această bază de date echipa sau echipele adecvate în funcţie de tipul echipei, ţara unde activează şi statutul în cadrul TI.

În Republica Moldova, există două astfel de echipe de răspuns la incidente de securitate: www.cert.gov.md şi www.cert.acad.md (www.cert.md). Denumirea CERT vine de la Echipă de răspuns la incidentele legate de securitatea calculatoarelor (Computer Emergency Response Team) ce reprezintă o echipă de experţi în securitatea informaţională, a cărei sarcină este să răspundă la incidente ce ţin de securitatea sistemelor informaţionale. Acesta asigură serviciile necesare pentru gestionarea incidentelor şi sprijinirea beneficiarilor lor în recuperarea de pe urma încălcărilor de securitate.

În vederea executării prevederilor Hotărârii Guvernului Nr. 746 din 18.08.2010 „Cu privire la aprobarea Planului Individual de Acţiuni al Parteneriatului Republica Moldova – NATO actualizat”, în cadrul Întreprinderii de Stat „Centrul de telecomunicaţii speciale” a fost creat Centrul pentru Securitatea Cibernetică - CERT-GOV-MD [vezi şi 15, 16].

Misiunea Centrului pentru Securitatea Cibernetică este de a susţine societatea moldovenească în protejarea împotriva incidentelor IT. CERT-GOV-MD va fi punctul central de raportare şi coordonare privind incidentele de securitate în sistemele de comunicaţii şi informatice aflate în administrarea Întreprinderii de Stat „Centrul de telecomunicaţii speciale”. CERT-GOV-MD va facilita schimbul de informaţii privind incidentele IT între organizaţiile din societate şi va disemina informaţiile legate de noi probleme, care ar putea împiedica funcţionarea sistemelor IT guvernamentale. Totodată, CERT-GOV-MD asigură informaţii şi consultanţă privind măsuri pro-active, precum compilarea şi completarea statisticilor.

CERT-GOV-MD a fost creat pentru a asista beneficiarii în utilizarea sistemelor informaţionale şi de telecomunicaţii ale autorităţilor administraţiei publice în implementarea măsurilor pro active şi reactive în vederea reducerii riscurilor de incidente a securităţii IT şi acordarea asistenţei în reacţionarea la incidente. Centrul, de asemenea,

examinează incidentele apărute în rețelele Moldoveneşti şi care sunt raportate de către cetățeni şi instituții din Republica Moldova, precum şi celor din străinătate.

Centrul de expertiză şi securitate pe internet MD-CERT - este un centru de expertiză a securității pe internet, situat la RENAM, (Asociația Națională Educație şi Cercetare din Republica Moldova). Centrul dat studiază vulnerabilități web, cercetează schimbările pe termen lung în sistemele de rețea şi contribuie la dezvoltarea, informarea şi instruirea cu scopul îmbunătățirii securității.

MD-CERT este un proiect necomercial fiind înregistrată oficial la CSIRT (Computer Security Incident Response Team) şi este angajată în colectarea şi analizarea faptelor de incidente informatice, în ceea ce privește resursele de rețea situate pe teritoriul Republicii Moldova. MD-CERT garantează confidențialitatea tuturor informațiilor trimise cu privire la incidente.

Sistemele informatice şi rețelele de calculatoare din cadrul organizațiilor tot mai des sunt atacate şi securitatea este minimă, ceea ce duce la mari probleme atât organizațiilor cât şi clienților acestor organizații. În urma acestor atacuri informaționale datele confidențiale sunt deteriorate, modificate sau chiar şterse.

Din această cauză mediul de afaceri are nevoie pentru a proteja resursele sale. Dar din păcate cele mai dese incidente de securitate a informației au loc în interiorul organizației, din cauza nerespectării măsurilor de securitate.

Procesul de integrare a agenților adaptivi de identificare a intruziunilor în rețele informaționale

Conceptele agenților adaptivi sânt totalitatea măsurilor, politicilor şi principiilor luate în ansamblu pentru a spori nivelul de securitate în vederea protejării sistemului sau rețelei din care face parte o structură sau o organizație.

Trei concepte importante referitoare la securitatea în rețea sunt: *confidențialitatea*, *integritatea* şi *disponibilitatea*.

Confidențialitatea se referă la ideea că informația trebuie sa fie accesată doar de persoanele autorizate în a face aceasta, altcineva având interzis accesul la aceste date. Când informația este citită sau copiată de către cineva neautorizat, rezultatul este cunoscut ca *pierdere a confidențialității*. Uneori confidențialitatea este critică, în cazul informațiilor private, date secrete, coduri bancare, etc.

Integritatea constă în faptul că informația este primită identic după cum a fost trimisă, adică datele nu au fost interceptate sau modificate în timpul transferului. Informația poate fi coruptă dacă se află într-o rețea nesecurizată, iar în cazurile când ea este modificată neautorizat, aceasta se numeşte o *pierdere a integrității,* ceea ce înseamnă că informația a fost modificată din cauza erorilor întâmplătoare a personalului sau datele au fost interceptate de persoane neautorizate. Integritatea datelor poate fi foarte importantă în cazul datelor financiare, transferurilor de fonduri, etc.

Informația, de asemenea, poate fi inaccesibilă, chiar dacă se află în rețeaua necesară, făcând persoanele autorizate să rămână fără acces la datele de care au nevoie, acest fapt numindu-se *pierdere a disponibilității.* Un astfel de exemplu este atunci când un utilizator nu poate accesa o rețea sau un anumit serviciu, cel mai probabil suferind în urma unui atac de tipul *Denia of Service.*

Ca concepte distincte care tratează problema securității deosebim:

- securitatea bazată pe mai multe nivele – *security in depth;*
- securitatea implementată încă din faza de proiectare – *security by design.*

Pentru a reduce riscurile de securitate în utilizarea şi administrarea sistemelor IT, cea mai bună strategie este cea pe ansamblu (security in depth). Aceasta presupune evaluarea pe ansamblu a infrastructurii IT şi clasificarea expunerii la riscuri de securitate. Pentru fiecare dintre riscurile identificate trebuie realizate planuri de măsuri, fie pentru reducerea expunerii la acele riscuri (mitigation), fie pentru reducerea impactului odată ce riscul s-a produs (contingency).

La polul opus se află abordarea punctuală (limitată în a oferi protecție doar la un anumit nivel), a implementării unui sistem specific de securitate, de exemplu antivirus sau detectarea accesului neautorizat (Intrusion Detection Systems – IDS). Deşi aceste sisteme sunt foarte utile în cadrul ariei specifice de aplicabilitate, această abordare lasă descoperite alte zone cu posibile breşe de securitate.

Un sistem de detecție al intruziunilor - IDS (Intrusion Detection System) reprezintă un echipament (sau o aplicație) care monitorizează activitățile rețelei și/sau sistemului căutând activități malițioase sau violări ale politicilor.

Detecția intruziunilor este procesul de monitorizare a evenimentelor care au loc intr-un sistem sau o rețea de calculatoare și analiza lor pentru a detecta posibile incidente care sunt violări sau amenințări iminente de violare a politicilor de securitate, a politicilor de utilizare acceptate sau a practicilor standard de securitate. Prevenirea intruziunilor este procesul prin care se desfășoară detecția intruziunilor și încercarea de înlăturare a posibilelor incidente detectate. Sistemele de detecție și prevenire ale intruziunilor - IDPS (Intrusion Detection-Prevention Systems) au ca scop principal identificarea posibilelor incidente, înregistrarea informațiilor despre ele, încercarea de înlăturare a incidentelor si raportarea către administratorii de securitate. În plus, organizațiile pot folosi IDPS-urile si pentru alte scopuri: identificarea problemelor legate de politicile de securitate, documentarea amenințărilor existente si descurajarea indivizilor în a încălca politicile de securitate.

Pentru a avea o abordare de ansamblu, trebuie pornit de la lucrurile elementare: uniformitatea infrastructurii din punct de vedere al sistemelor utilizate, administrarea centralizată, menținerea la zi a sistemelor din punct de vedere al patch-urilor şi fix-urilor (pentru sistemele de operare şi aplicațiile instalate), aplicarea unor configurări standard

de securitate pe toate serverele şi staţiile de lucru, în funcţie de rolul funcţional al acestora precum şi realizarea unor proceduri standard de utilizare şi administrare.

Studiile arată că în medie 90% din breşele de securitate identificate nu sunt datorate problemelor tehnologice ci instalării şi configurării necorespunzătoare sau datorită nerespectării unor proceduri de utilizare şi administrare a sistemului. În multe cazuri, aceste proceduri nici nu există. Trebuie deci să privim problema pe ansamblu, adresând tehnologia, oamenii şi procedurile interne ale organizaţiei.

Conceptul de „*security by design*" este foarte bun atunci când posibilităţile de implementare sunt justificate. De multe ori totuşi acest concept impune unele restricţii care limitează foarte mult utilizarea sa în arii diferite, metoda fiind utilizată în zone speciale, foarte specializate (zone cu statut de importanţă majoră, ca de exemplu, reţelele de calculatoare care controlează traficul aerian, laboratoare de cercetare, etc.), zone în care accesul prin definiţie este foarte restrictiv.

Acest concept aplicat la „nivel software" generează un principiu de funcţionare al aplicaţiei cu restricţii foarte clare – care de multe ori din cauza acestor limitări devine în scurt timp nefezabil.

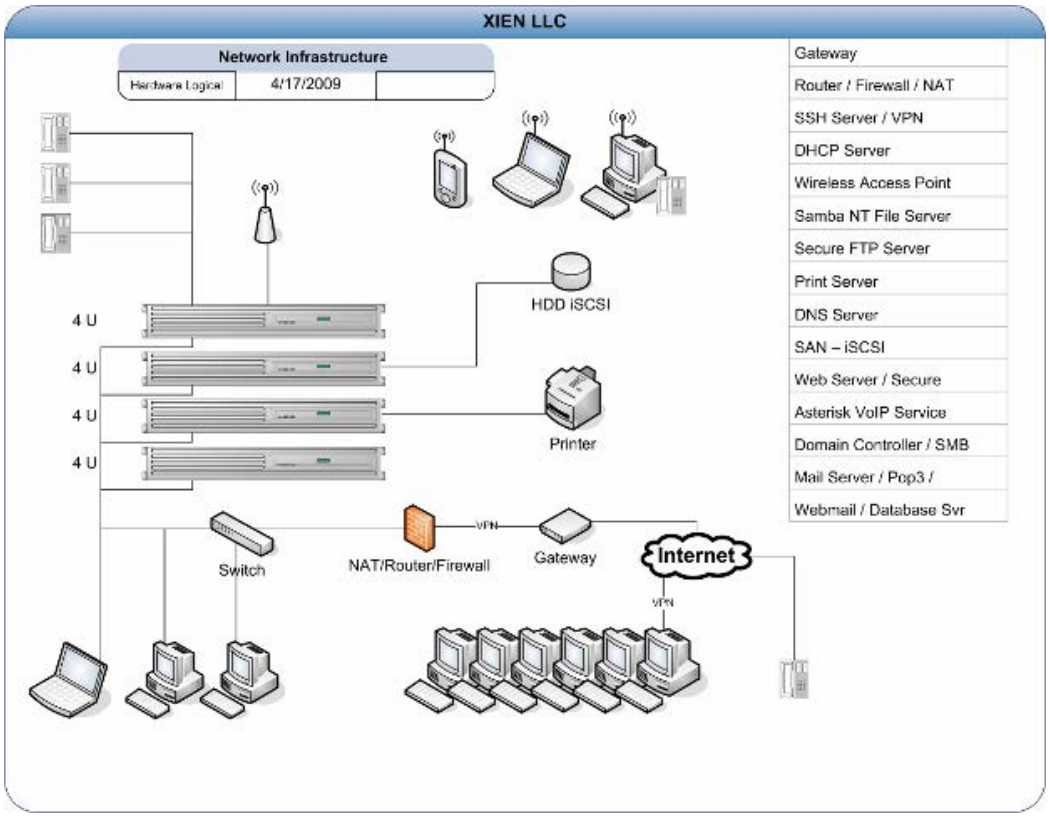

Figura 1. Exemplu de utilizare al conceptului de „security by design" la nivel IT

Pentru a exemplifica acest concept la nivel de aplicaţie (software) să presupunem că se citeşte de către o aplicaţie un şir de caractere care ar trebui să reprezinte un nume. Dacă se limitează prin definiţie ca acel nume să conţină numai caractere alfabetice (litere mici şi/sau mari) vor fi persoane care se vor simţi ofensate că nu pot introduce nume de

tipul „best4you” sau diferite caractere gen /.$%@, etc. în acest caz acel program ajungând să-şi piardă din start unii utilizatori mai pretenţioşi. Totuşi merită semnalat faptul că implementarea unei astfel de metode este foarte binevenită în unele cazuri când netratarea corespunzătoare a unei astfel de secvenţe citite poate genera probleme de tipul „buffer overflow” generând apariţia unor breşe de securitate ce pot fi utilizate în scopuri malefice (cazul când se folosesc caractere speciale ce pot ascunde informaţii tratate distinct, de exemplu, dacă se acceptă introducerea unei secvenţe „%n” se poate interpreta ca „salt la linie nouă” de către o funcţie de afişare generând în acel caz o posibilă eroare, cel puţin la nivel estetic – ca formă de prezentare).

„*In-depth security*” sau „*defence in depth*” este un principiu bazat pe mai multe „straturi” de securitate în vederea protejării sistemului sau reţelei din care face parte.

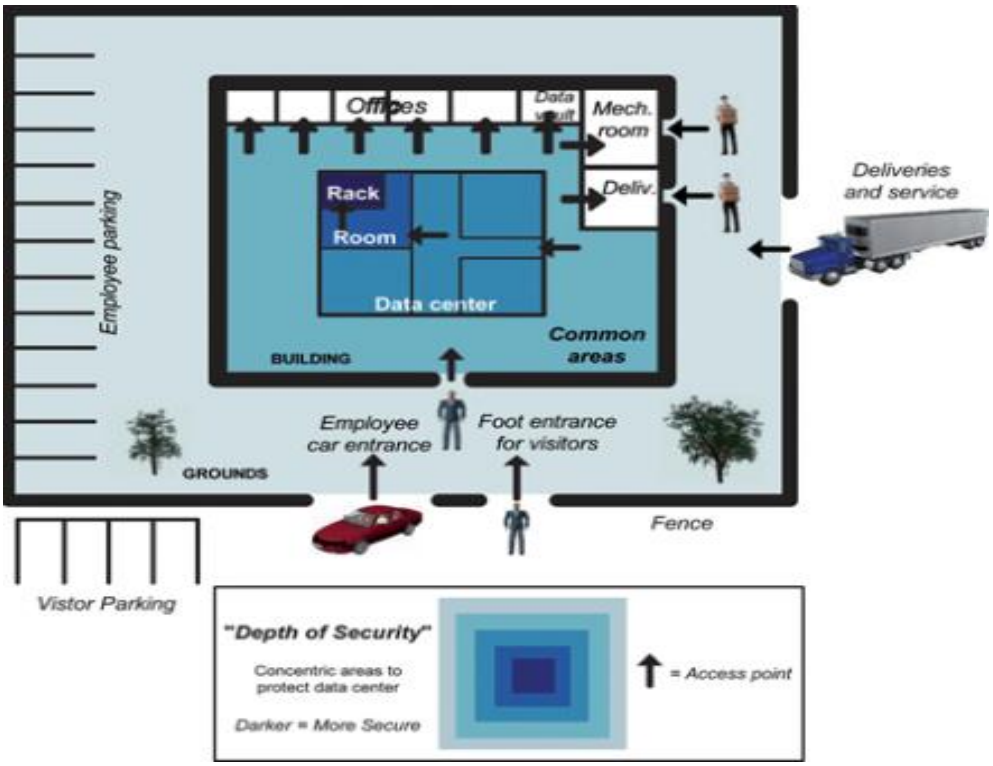

Figura 2. Evidenţierea conceptului de „Security in depth”

Trebuie să se înţeleagă că nu contează cât de bun este fiecare „strat” – privit singular, există cineva mai deştept, cu resurse materiale şi temporale suficiente încât să treacă de „strat”-ul dat. Acesta este motivul pentru care practicile uzuale de securitate sugerează existenţa mai multor nivele de securitate sau pe scurt „in-depth security”.

Ca o regulă de bază (nivele minime de securitate instalate) se sugerează următoarele produse:

- firewall – o barieră protectivă între calculator, reţeaua internă şi lumea din jur. Traficul din interior şi spre exterior este filtrat, restricţionat, blocând eventualele transmisii nenecesare. Folosind reguli stricte de acces la nivel de aplicaţii şi utilizatori, se poate îmbunătăţi substanţial securitatea sistemului şi a reţelei locale;

- antivirus – un software instalat cu scopul clar de a te proteja de viruşi, viermi şi alte coduri malițioase. Majoritatea aplicațiilor antivirus monitorizează traficul în fiecare moment, scanând în timp ce se navighează pe Internet sau scanând mesajele primite pe mail (cu tot cu ataşamente) şi periodic oferind posibilitatea rulării unei scanări la nivelul întregului sistem în căutarea de cod malițios;
- intrusion detection system (IDS) şi Intrusion Prevention System (IPS o varianta mai specială a IDS) – un dispozitiv sau o aplicație folosit(ă) pentru a inspecta întregul trafic dintr-o rețea şi de a trimite mesaje de alertă utilizatorului sau administratorului sistemului cu privire la încercări neautorizate de acces. În funcție de metodele utilizate IDS-ul poate rămîne la stadiul de a alerta utilizatori. Tehnologia VPN oferă asemenea conexiuni private, separând datele în „tuneluri". În acest mod, o rețea privată poate fi creată prin rețele publice cum ar fi Internetul, folosind protocoale ca Generic Routing Incapsulation (GRE) sau Layer 2 Tunneling Protocol, pe scurt L2TP.

Pentru a oferi protecția datelor pe care le transportă, echipamentele hardware şi software VPN susțin tehnologia de criptare. Tot traficul care circulă printr-un tunel între două puncte într-un VPN este criptat.

Uneori, separarea datelor folosind tehnologii de tunneling oferă confidențialitate eficientă, de exemplu în cadrul rețelei locale. Deseori însă, cerințele suplimentare de confidențialitate necesită protecție mai mare, de exemplu prin folosirea unor tehnologii sau protocoale de criptare digitale ca IPSec.

IPSec. IPSec, sau protocolul de securitate IP, este un cadru de standarde deschise pentru asigurarea comunicațiilor private securizate pe Internet. IPSec asigură confidențialitatea, integritatea şi autenticitatea comunicațiilor de date prin rețea publică, fiind o componentă tehnică cheie pentru o soluție de securitate totală.

Acest protocol poate rezolva amenințările de securitate din infrastructura de rețea, fără a cere modificări costisitoare ale gazdei şi aplicațiilor. IPSec oferă criptare şi autentificare la nivelul de rețea IP. Deoarece pachetele criptate arată ca pachete IP obişnuite, ele pot fi redirecționate uşor către o rețea IP, ca Internetul, exact ca pachetele IP obişnuite. Singurele dispozitive care cunosc criptarea sunt punctele finale. IPSec utilizează diferite tehnologii existente, cum sunt criptarea DES şi certificatele digitale.

Criptare şi decriptare. Tehnologia de criptare asigură ca mesajele să nu fie interceptate sau citite de altcineva decât destinatarul autorizat.

Criptarea este utilizată pentru a proteja date care sunt transportate prin rețea publică, şi folosește algoritmi matematici avansați pentru a cifra mesajele şi documentele atașate. Există mai multe tipuri de algoritmi de criptare, dar unii sunt mai siguri decât alții. În cei mai mulți algoritmi, datele originale sunt criptate utilizînd o anumită cheie de criptare, iar computerul destinatar sau utilizatorul pot descifra mesajul folosind o cheie de decriptare specifică.

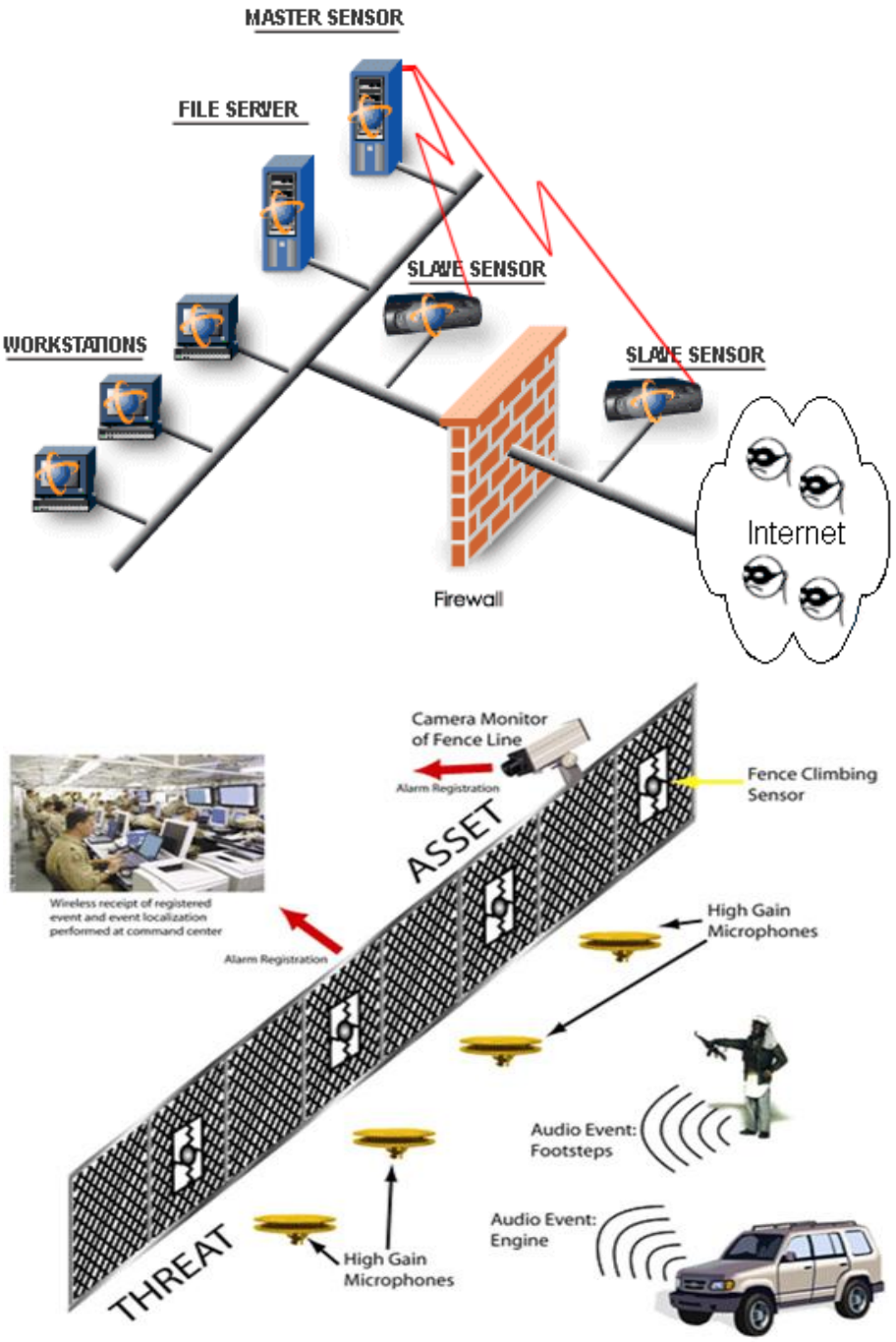

Figura 3. IDS la nivel software şi hardware

Aplicarea conceptelor enumerate mai sus reduce în mare parte ameninţările la care sunt supuse sistemele informaţionale a reţelelor IP şi sporeşte semnificativ nivelul de securitate astfel încât totalitatea informaţiilor de diferite categorii sa fie păstrată în structura de reţea.

Monitorizarea şi analiza activităţii agenţilor adaptivi în reţele informaţionale

Identificarea intruziunilor în sisteme si reţele informaţionale a devenit una din componentele majore ale securităţii informaţionale. Analiştii acestui concept au sesizat o contradicţie între nevoia de comunicaţii şi conectivitate, pe de o parte, şi necesitatea

asigurării confidențialității, integrității şi autenticității informațiilor, pe de altă parte. Domeniul relativ nou al identificării intruziunilor caută soluții tehnice pentru rezolvarea acestei contradicții aparente. Viteza şi eficiența comunicațiilor „instantanee" de documente şi mesaje conferă numeroase atacuri actului decizional într-o societate modernă, bazată pe economie concurențială. Însă utilizarea serviciilor de poştă electronică, web, transfer de fonduri, etc. se bazează pe un sentiment, deseori fals, de securitate a comunicațiilor, care poate transforma potențialele câştiguri generate de accesul rapid la informații, în pierderi majore, cauzate de furtul de date sau de înserarea de date false sau denaturate.

În loc de a ne focaliza numai pe un anumit tip de securizare, este important să înțelegem că o soluție completă de identificare a intruziunilor în rețelele informaționale este necesară instituției pentru a-şi proteja datele şi resursele informaționale. Această soluție trebuie să includă autentificare şi autorizare, confidențialitatea datelor şi securizarea perimetrului.

Studierea materialelor şi practicii de până acum din domeniul identificării intruziunilor în sistemele şi rețelele informaționale arată că metodele tehnice şi programul de aplicare a principiilor securității informaționale sunt bine documentate şi este foarte greu de ales vre-un domeniu unde aceste metode nu sunt subiectul unei cărți sau articol.

Păstrarea datelor a devenit o problemă tot mai importantă atât datorită faptului că se manipulează un volum tot mai mare de date, dar şi modului de accesare al acestor informații care trebuie să fie rapid, eficient, optim din punct de vedere al raportului timp, accesare/valoare a informației. Nu în ultimul rând, datele stocate trebuie să fie protejate astfel încât să se asigure o securitate adecvată în ceea ce priveşte persoanele care au acces la ele, dar şi din punct de vedere al concordanței cu legislația privind securitatea şi protecția informațiilor şi datelor cu caracter clasificat, utilizarea procedurilor de răspuns la incidente de securitate cibernetică şi stabilirea responsabililor pentru astfel de activități.

Există numeroase direcții de cercetare în domeniul identificarii intruziunilor în sisteme si rețele informaționale, şi mai ales în ceea ce priveşte estimarea de stare. Trebuie avute în vedere beneficiile introducerii tehnologiilor avansate de protecție a sistemului informatic: IDS/IPS, soluții antimalware de tip enterprise, criptare fişiere şi conexiuni, acces la distanță prin VPN şi capacitățile acestora de a trata erorile de topologie apărute în sistem.

Concluzii

Modelul societății viitorului - Societatea Informatică a pus în fața Uniunii Europene probleme de maximă prioritate şi urgență: crearea unui nou cadru de reglementări, promovarea unei noi culturi şi a spiritului întreprinzător în afaceri,

obținerea poziției de lider în noile tehnologii, educarea şi instruirea cetățenilor, implementarea unor noi metode de a face afaceri.

În acest context Uniunea Europeană, prin organismele sale politice şi executive a acționat începând din anul 1993 printr-o serie de decizii strategice şi programe, cel mai recent document strategic fiind e-Europe - O Societate Informatică pentru toți. Comisia Europeană a luat această inițiativă prin adoptarea Comunicării „e-Europe an information Society for All" la 8 decembrie 1999, prin care se propune accelerarea implementării tehnologiilor digitale în Europa şi asigurarea competențelor necesare pentru utilizarea acestora pe scară largă. Această inițiativă are un rol central în agenda reînnoirii economico-sociale pe care şi-o propune UE, constituind totodată elementul cheie pentru modernizarea economiei europene, pentru tranziția la noua economie bazată pe cunoaştere în perspectiva anului 2020.

Aplicarea tehnologiilor digitale precum şi implimentarea agenților adaptivi de identificare a intruziunilor în sisitemele şi rețelele informaționale a devenit un factor vital. Deşi Europa este lider tehnologic în multe domenii (de exemplu, comunicații mobile, televiziune digitală, extinderea rețelelor informaționale), în altele - în special în utilizarea Internetului a rămas în urmă comparativ cu S.U.A. şi Canada.

În consecință inițiativa e-Europe îşi propune să aducă Europa în situația de a beneficia din plin de avantajele economiei digitale, de a valorifica la maxim prioritățile sale tehnologice, de a-şi creşte potențialul educațional şi antreprenorial necesar.

Obiectivele cheie sunt:

- ***asigurarea comunicării on-line pentru fiecare locuință, şcoală, întreprindere şi instituție din administrația publică;***
- ***crearea culturii digitale şi antreprenoriale a Europei, de care să beneficieze investitorii dinamici, care vor finanța şi dezvolta aceste idei noi;***
- ***asigurarea principiului conform căruia tranziția la era digitală să fie un proces care să includă întreaga societate, să asigure încrederea consumatorilor şi să întărească coieziunea socială.***

Pentru implementarea acestor obiective a fost adoptat planul de acțiune e-Europe (Feira, 2000), actualizat în 2006, la Sevilia (prin planul de acțiune e-Europe 2005). Planul de acțiuni e-Europe conține o serie de acțiuni pentru asigurarea accesului ieftin, sigur şi rapid la Internet, pentru asigurarea resurselor umane capabile să dezvolte şi să utilizeze noile tehnologii şi pentru stimularea utilizării Internet-ului la nivel european. Progresele importante ale țărilor membre UE au permis definirea unui nou plan de acțiune având ca orizont, care se va baza pe progresele tehnologice din domeniul comunicațiilor în bandă largă şi al multi-platformelor de acces, mizând totodată pe sinergia dintre dezvoltarea infrastructurii de bandă largă şi industria de servicii TI de conținut digital.

Obiectivele e-Europe sunt de maximă importanță nu numai pentru țările membre UE, ci şi pentru țările din Europa Centrală şi de Est candidate la aderare. Ritmurile de

dezvoltare şi utilizare a TIC în toate sectoarele economico-sociale vor influența în mod direct ritmul procesului de integrare europeană şi vor oferi totodată noi oportunități de depăşire a dificultăților întâmpinate de țările în plin proces de reformă. Conferința ministerială a țărilor din Europa Centrală şi de Est, organizată sub patronajul şi cu participarea Comisiei Europene a decis elaborarea unui Plan de acțiune e-Europe pentru țările în curs de aderare, complementar cu cel al țărilor membre UE, dar convergent ca obiective. Față de obiectivele şi acțiunile prevăzute pentru țările UE, planul e-Europe conține un obiectiv suplimentar, care se referă la accelerarea asigurării elementelor fundamentale pentru Societatea Informatică în țările candidate la aderare, prin dezvoltarea şi asigurarea accesibilității serviciilor de comunicație. Realizarea obiectivelor e-Europe necesită o angajare politică susținută din partea țărilor candidate.

Bibliografie

1. Held G. ş.a. Arhitecturi de securitate. Editura Teora, 2003.
2. Hontanon R.J. Securitatea rețelelor. Editura Teora, 2003.
3. Hsiao S.B., Stemp R. Advanced Computer Security. CS 4602. Monterey, California, 2006.
4. Mihai I.C. Securitatea informațiilor. Editura Sitech, 2012. 317 p.
5. Mihai I.C. Securitatea sistemului informatic. Editura Dunărea de Jos, 2007.
6. Oprea D. Protecția şi securitatea informațiilor. Editura Polirom, 2007. 448 p.
7. Sarcinschi A. Vulnerabilitate, risc, amenințare. Securitatea ca reprezentare psihosocială. Editura Militară, 2009.
8. Udroiu M. ş.a. Securitatea informațiilor în societatea informațională Editura Universitară, 2010. 402 p.
9. Institutul de Dezvoltare a Societății Informaționale. https://idsi.md/node/515 (vizitat 01.01.2018)..
10. ISO 27001:2005. Sistemul de management al securității informațiilor – Cerințe.
11. ISO 27002:2005. Codul de practică al managementului securității informațiilor.
12. ISO 27001:2013. Sistem de management al securității informației: specificații şi ghid de utilizare.
13. ISO/IEC 27007:2011. Tehnologia Informației – Tehnici de securitate – Ghid pentru auditarea SMSI.
14. ISO/IEC 27000:2014. Sisteme de management al securității informației.
15. Hotărârea Parlamentului pentru aprobarea Strategiei securității naționale a Republicii Moldova nr. 153 din 15.07.2011. În: Monitorul Oficial nr. 170-175 din 14.10.2011.
16. Hotărârea Guvernului cu privire la Strategia Națională de dezvoltare a societății informaționale „Moldova Digitală 2020” nr. 857 din 31.10.2013. În: Monitorul Oficial nr. 252-257 din 08.11.2013.