Sistem de detecție și prevenirea intruziunilor în rețele informaționale

Andrei ȘESTACOV
Academia Militară a Forţelor Armate „Alexandru cel Bun"
mun. Chișinău, Republica Moldova
andrei.sestacov@academy.army.md

The intrusion detection and prevention systems are security solutions consisting in software components that are designed to suport the protection for vulnerable information systems and networks. The capabilities of this system are very often associated with firewall. Alerting information will generally include information about the source address of the intrusion, the target/victim address, and type of attack that is suspected.

It is important for organizations to be aware of the risks associated with the use of technology and information management and to address positively this issue through employee awareness of the importance of information security, understanding the typology of threats, risks and vulnerabilities specific to computerized environments, and applying adaptive agents to identify intrusions in information networks.

***Termeni cheie* — intrusion detection, security, firewall, risks and vulnerabilities.**

I.INTRODUCERE

Securitatea1 sistemelor și rețelelor informaționale a devenit în prezent o problemă extrem de importantă, de care trebuie să ţină cont atât producătorii de echipamente, cât şi dezvoltatorii de softuri şi sisteme de operare, precum şi administratorii de reţea. Desigur, integritatea sistemelor și rețelelor informaționale, precum şi cerinţele de protejare a confidenţialităţii datelor, pot fi abordate printr-o multitudine de tehnici şi metode. Soluţiile actuale de securitate se bazează pe utilizarea de componente hardware şi pe dezvoltarea de soluţii software capabile să detecteze fişierele, scripturi şi loguri suspecte de a fi considerate intruziuni, acţiuni nepermise şi consecinţe ale acestora [1]. Foarte des, însă, detecţia evenimentelor cu caracter intruziv în cadrul unui sistem informatic conectat în reţea nu este suficientă. În principiu, după cum se va arăta în continuare, detecţia intruziunilor se bazează pe tipuri de comportament. Foarte importantă s-ar dovedi şi capabilitatea de prevenire a intruziunilor. Aceasta ar asigura un nivel de securitate mai înalt, deoarece ar bloca orice acţiune maliţioasă şi sistemul informațional care se dorește a fi protejat. Desigur, în cazul sistemelor IDS (Intrusion Detection Systems) care implementează şi funcţii de prevenire a intruziunilor, problema care se pune este în ce măsură o astfel de capabilitate nu poate conduce la o blocare a funcţionării serviciilor utile ale sistemului informațional, afectând aplicaţiile practice ale utilizatorilor finali. De aceea, problema implementării unor mecanisme eficiente de detecţie/prevenire a intruziunilor este foarte importantă. Pentru abordarea eficientă a acesteia, se impune cunoaşterea potenţialului pe care soluţiile tipice de detecţie şi prevenire a intruziunilor îl prezintă.

II.DETECŢIA INTRUZIUNILOR ÎN SISTEME ŞI REŢELE INFORMAŢIONALE

Sistemul de detectare a intruziunilor într-un mod similar completează securitatea firewall-ului. Firewall protejează o organizație de atacurile rău intenționate din exteriorul rețelei informaționale. Sistemul de detectare a intruziunilor detectează dacă cineva încearcă să treacă prin firewall sau reușește să spargă securitatea firewall-ului și încearcă să aibă acces în orice sistem și avertizează administratorul de sistem în cazul în care există o încălcare a politicilor de securitate. În plus, firewall-urile filtrează traficul din internet, cu toate acestea, există modalități de a ocoli firewall-ul. De exemplu, utilizatorii externi pot fi conectați la Intranet prin apelarea printr-un modem instalat în rețeaua privată de organizația. Acest tip de acces nu ar fi văzut de către firewall. Prin urmare, un sistem de detectare a intruziunilor (IDS) reprezintă procesul de monitorizare a evenimentelor ce au loc într-un sistem informatic sau într-o rețea informațională, precum și analizarea acestora pentru semne ce indică incidente posibile ce sunt încălcări sau amenințări iminente de încălcare a politicilor de securitate ale calculatorului, a politicilor acceptate de utilizare sau practicile de securitate standard. Incidentele pot avea multe cauze, ca malware-urile (ex: worms, spyware), atacatori externi ce încearcă să obțină accesul neautorizat la sistem precum şi utilizatori autorizaţi ce întrebuinţează greşit privilegiile oferite sau încearcă să obţină unele adiţionale ce nu sunt autorizate [2]. Cu toate că majoritatea incidentelor sunt de natură maliţioasă, multe altele nu sunt: de exemplu, o persoană poate introduce greșit adresa unui calculator, și astfel, neintenţionat să acceseze un alt sistem fără autorizaţie.

III.PRINCIPIILE DETECŢIEI INTRUZIUNILOR

Detectare intruziunilor reprezintă procesul de monitorizare a evenimentelor ce au loc într-un sistem informatic sau într-o reţea, precum şi analizarea acestora pentru semne ce indică incidente posibile ce sunt încălcări sau ameninţări iminente de încălcare a politicilor de securitate ale calculatorului, a politicilor acceptate de utilizare sau practicile de securitate standard. Incidentele pot avea multe cauze, ca malware-urile

(ex: worms, spyware), atacator externi ce încearcă să obţină accesul neautorizat la sistem precum şi utilizatori autorizaţi ce întrebuinţează greşit privilegiile oferite sau încearcă să obţină unele adiţionale ce nu sunt autorizate. Cu toate că majoritatea incidentelor sunt de natură maliţioasă, multe altele nu sunt: de exemplu, o persoană poate introduce greşit adresa unui calculator, şi astfel, neintenţionat să acceseze un alt sistem fără autorizaţie [3].

Detectarea intruziunilor presupune detectare şi încercarea de a opri eventualele incidente.

Sistemele de detectare se concentrează în principal pe :

- identificarea posibilelor incidente;
- logare de informaţii despre acţiunile întreprinse;
- încercarea de stopare a incidentelor şi raportarea acestora la administratorii de securitate.

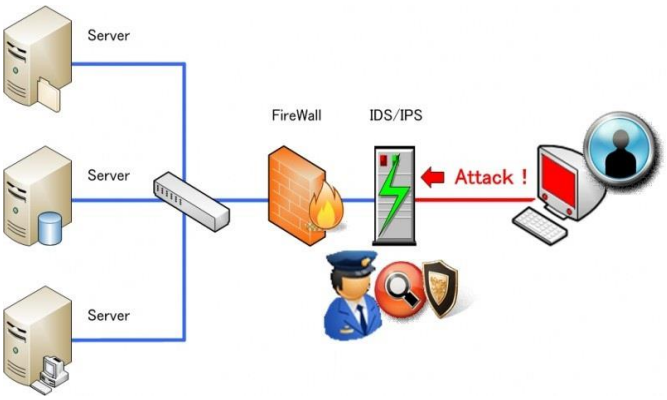

Fig. 1 Sistem de detecţie intruziunilor

IV. TIPURI DE TEHNOLOGII IDS

Există mai multe tipuri de tehnologii IDS, în funcţie de tipul de evenimente pe care le monitorizează şi de modul în care acestea sunt implementate, acestea sunt împărţite în următoarele patru grupe:

- la nivel de reţea: monitorizează traficul de reţea pentru anumite segmente de reţea sau dispozitive, analizând activităţile protocoalelor de reţea şi aplicaţie pentru a identifica activităţi suspecte. Se pot identifica diferite evenimente de interes. Este amplasat de cele mai multe ori la o graniţă între reţele, cum ar fi în apropierea firewall-urilor sau routerelor, serverelor de reţea virtuală privată (VPN), serverelor de acces de la distanţă şi reţelelor fără fir;
- fără fir: monitorizează traficul de reţea fără fir şi analizează protocoalele sale de reţea pentru a identifica activităţi suspecte care implică protocoalele însuși. Nu poate identifica activităţi suspecte ce implică protocoale de nivel aplicaţie sau de transport (TCP, UDP), în traficul de reţea fără fir ce este transferat. Îşi desfăşoară activitatea de monitorizare, cel mai frecvent, în raza de acţiune a reţelei fără fir a unei organizaţii;
- analiza comportamentului de reţea (Network Behavior Analysis - NBA): examinează traficul de reţea pentru a identifica ameninţările care generează fluxuri de trafic neobişnuit, cum ar fi blocarea distribuită a unui serviciu (DDoS), anumite forme de malware(viermi, backdoors) şi încălcări ale politicii (ex: un sistem client ce furnizează servicii de reţea pentru alte sisteme). Sistemele NBA sunt cel mai adesea utilizate pentru a monitoriza fluxurile de pe reţelele interne ale unei organizaţii, şi sunt, de asemenea, uneori, utilizate pentru a monitoriza fluxurile între reţelele unei organizaţii şi reţelele externe;
- La nivel de host**:** monitorizează caracteristicile unei singur host şi evenimentele care au loc în acel host pentru activităţi suspecte. Tipurile de caracteristici urmărite sunt: traficul de reţea(numai pentru gazda respectivă), logurile de sistem, procesele active, activităţile aplicaţiilor, accesul la fişiere precum şi modificarea acestora, schimbarea configuraţiei sistemului sau a unor aplicaţii. Sunt cel mai frecvent utilizate pe gazed critice, cum ar fi servere accesibile în exterior sau servere care conţin informaţii sensibile.

Unele forme de IDS sunt mai mature decât altele pentru că au fost folosite mult mai mult timp. Cele la nivel reţea şi unele forme la nivel de host sunt disponibile pe piaţă de peste zece ani. Cele bazate pe analiza comportamentală a reţelei sunt o formă oarecum mai nouă ce a evoluat din produsele create special pentru a detecta atacuri de tip DDoS şi din produse dezvoltate pentru a monitoriza fluxurile de trafic în reţelele interne. Tehnologiile fără fir sunt un tip relativ nou, dezvoltat ca răspuns la popularitatea reţelelor locale wireless (WLAN) şi a ameninţărilor în creştere la adresa reţele WLAN şi clienţilor WLAN.

V. INTRUZIUNILE

Intruziunile sunt unele dintre cele mai mari ameninţări la adresa reţelelor de calculatoare şi a sistemelor de calcul. Acestea exploatează slăbiciuni ale software-ului sau ale configuraţiei sistemului pentru a-l deteriora. Printre aceştia regăsim: viruşii propriu-zişi, viruşi de macro şi de email, cai troieni şi viermi. De numele acestor tipuri de ameninţări se leagă principalele unelte folosite de persoanele rău intenţionate în demersul lor de a obţine date sensibile care pot fi valorificate în vreun fel.

Viruşii sunt programe – cod executabil numit uneori malware – care se inserează în alt program executabil. Astfel, virusul se propagă atunci când este executat programul infectat. Virusul este pasiv deoarece are nevoie ca un utilizator sau un alt program să-l lanseze şi să execute programul infectat. Înainte de acest eveniment, virusul rămâne în stare adormită. La 10 activare codul este plasat în memoria centrală a calculatorului şi îşi începe execuţia exact ca orice alt program. De obicei, atunci când este activat, virusul îşi inserează copii ale sale în cele mai comune executabile pe care le poate găsi pe discul rigid al calculatorului victimă, proces numit auto-replicare [4]. Programele infectate se răspândesc de obicei de la un calculator la altul prin copii pe medii de stocare sau prin descărcarea de pe Internet.

Cel mai adesea utilizatorii schimbă între ei documente, nu programe. Acestea pot fi ţinta virușilor de macro şi de e-mail.

Macro definiţiile executate de aplicaţii cum sunt Microsoft Word, Excel sau Outlook pot fi şi ele infectate de viruşi. La deschiderea unui document infectat virusul se execută în background, fără ca utilizatorul să observe.
În mod asemănător, există viruşi care se pot ataşa la e-mail. De îndată ce destinatarul deschide conţinutul unui mesaj infectat, virusul este executat. De cele mai multe ori, încep să trimită email-uri care conţin copii ale lor fiecărui contact găsit în cartea de contacte a victimei.

Viruşii de email pot cauza pagube mari infrastructurii de email a Internet prin traficul enorm pe care îl generează ca urmare a replicării multiple. În unele cazuri au provocat căderea serverelor de email care nu au rezistat volumului imens de trafic.

Caii troieni constituie un tip aparte de malware care deschide porţi în sisteme pentru
intruşi. Termenul de cal troian este utilizat pentru a descrie software care permite atacatorilor aflaţi la distanţă să ia controlul sistemului de calcul, să descarce fişiere, să instaleze aplicaţii, să modifice fişiere şi chiar să oprească de tot sistemul.

Caii troieni sunt programe instalate fără cunoştinţa încărcăturii ostile de către utilizatori în urma unei infectări a unui fişier sau a unei aplicaţii descărcate de pe Internet.
Unul dintre cei mai faimoşi cai troieni, Back Orifice, este atât de puternic încât a ajuns să fie considerat program de gestiune de la distanţa a sistemelor de calcul.

Viermii se pot replica fără intervenţia utilizatorului. În timp ce viruşii sunt pasivi şi au nevoie de intervenţia utilizatorului pentru a se rula, viermii sunt activi. Din cauza faptului că nu au nevoie de intervenţia utilizatorului şi se pot replica şi activa autonom, ei sunt mult mai periculoşi. Aceştia sunt programe care folosesc erorile de programare (bug-uri) ale resurselor din reţea pentru a se replica. Ei se pot inocula în sistemele de calcul datorită erorilor din server, loc în care încep să scaneze reţeaua în căutarea altor calculatoare pe care să le infecteze. Proliferarea unui vierme este uimitoare. De exemplu, Code Red a avut nevoie de 15 minute pentru a infecta mii de calculatoare şi a atacat chiar site-ul oficial al Casei Albe a SUA. Pe lângă căutarea altor calculatoare pe care să le infecteze, viermii pot cauza pagube prin atacarea reţelei şi a componentelor sale. Un sondaj la nivel naţional în SUA, sponsorizat de către CA Incorporated şi de National Cyber Security Alliance (NCSA) a arătat că 83% dintre adulţii care se implică în legături sociale prin reţele de calculatoare au descărcat fişiere necunoscute, care le puteau expune PC-urile la atacuri.

Spyware-ul poate fi definit ca orice software care foloseşte conexiunea la Internet a unui utilizator în fundal. Termenul de spyware este, în majoritatea cazurilor, sinonim cu adware, şi poate fi un program de genul cailor troieni. Programele spyware pot colecta date sensibile (cum sunt: versiunea de sistem de operare rulată, tipul de răsfoitor de Web, dacă limbajul de scenarii poate fi executat, dimensiunea ecranului, plug-in-urile disponibile, informaţii de DNS din domeniu, pot trasa ruta spre sursă pentru a stabili unde se află calculatorul ţintă pe reţea) pe două căi: prin cookies şi instalându-se şi apoi executându-se.

Programele care prezintă risc, în legătură cu codul ostil sunt numite generic "riskware" şi constituie orice program legal care poate fi folosit de atacatori pentru a penetra calculatoarele. Un rootkit poate fi considerat ca un cal troian introdus într-un sistem de operare. Pentru ca un atacator să poată instala un rootkit el trebuie să aibă acces la nivelul de administrator la sistem înainte de a putea instala kit-ul respectiv. Rootkit-urile nu permit obţinerea accesului la sistem, ci dau posibilitatea de a pătrunde în sistem cu permisiuni de nivel maxim (root). O dată obţinut accesul la nivel de administrator, poate fi folosit un cal troian care să se deghizeze într-o funcţie sistem existentă pe sistemul compromis. Un atac cibernetic de tip **DoS** (**Denial of Service**) sau **DDoS** (***Distributed Denial of Service)*** este o încercare frauduloasă de a indisponibiliza sau bloca resursele unui calculator [5].

Deşi mijloacele şi obiectivele de a efectua acest atac sunt foarte diverse, în general acest atac este efectul eforturilor intense ale unei (sau a mai multor) atacatori de a împiedica un site web sau servicii din Internet de a funcţiona eficient, temporar sau nelimitat. Autorii acestor atacuri au de obicei drept ţintă site-uri sau servicii găzduite pe servere cu cerinţe înalte, cum ar fi băncile, gateway-uri pentru plăţi prin carduri de credit şi chiar servere în întregime. O metodă tradiţională de atac provoacă „saturarea" calculatorului ţintă (victimei) cu cereri de comunicare externe, astfel încât să nu mai poată reacţiona eficient la traficul Internet legitim, sau chiar să devină indisponibil.

În termeni generali, atacurile de tip DoS se realizează pe mai multe căi:

- provocarea unui restart forţat al calculatorului sau al mai multor calculatoare;
- consumarea intensă a resurselor disponibile ale unui server, astfel încât acesta să nu mai poată furniza servicii;
- blocarea comunicaţiilor dintre utilizatorii bine intenţionaţi şi calculatorul victimă, astfel încât acesta să nu mai poată comunica adecvat;

Atacurile de tip Denial of Service sunt considerate încălcări ale politicii de utilizare
corectă a Internetului elaborate de Internet Architecture Board. De asemenea aceste atacuri constituie deseori încălcări ale legislaţiei din ţara respectivă.

Câteva scopuri pentru care sunt folosite intruziunile sunt:

- obţinerea accesului de la distanţă;
- furtul de resurse;
- sabotajul;
- colectarea de date;
- ocolirea sistemului de control al accesului;
- eludarea detectării.

VI. CONCLUZII ŞI PROPUNERI

Problemele de securitate informațională care afectează sistemele şi reţelele informatice impun utilizarea unor soluţii care să aibă în vedere diferitele tipuri de incidente şi ameninţări care pot duce la pierderea unor informaţii sensibile, precum şi obiectivele propuse până în 2020, aria securităţii şi apărării sistemelor informaţionale din perspectiva implementări „Strategiei de securitatea naţională a Republicii Moldova" trebuie să devină o soluţie completă de securitate a informaţiilor care aşi proteja datele şi resursele informatice [6].

Sistemele de detecţie intruziunilor au devenit obligatorii pentru protejarea împotriva diferitelor tipuri de malware, împotriva interceptării datelor confidenţiale transmise prin reţelele informatice, precum şi pentru protejarea reţelelor interne organizaţionale împotriva unor acţiuni externe ostile, mai ales în cazul instituţiilor militare, care sunt predispuse zilnic la astfel de acte datorită importanţei lor strategice în securitatea naţională şi mondială. Această lucrare am analizat aceste echipamentele din toate punctele de vedere, de la clasificare, metode de detecţie, tehnici de analiză a traficului până la criterii relevante ce pot influenta alegerea unui astfel de echipament şi cerinţele recomandate pentru blocarea eficientă a intruziunilor.

Fiecare IDS şi gen de detecție are avantajele şi dezavantajele sale, iar pentru a detecta şi preveni cu succes atacurile informatice nu este de ajuns un singur tip de echipament, ci o combinaţie de mai multe echipamente şi tehnici de detecţie.

Sistemele de detecție intruziunilor alertează când va depista trafic de pe oricare sursa de IP pe oricare port în ambele direcții și sa afișează mesajul "IP Packet detected".

Sistem monitorizează caracteristicile şi evenimentele din cadrul unui singur host pentru activităţi suspecte.

În procesul detecție intruziunilor au fost obținute următoarele date:

- traficul de reţea cu sau fără fir (numai pentru acel host),
- logurile de sistem;
- Procesarea rapidă a pachetelor de intrare pe senzor astfel încât să se evite pierderea de date;
- accesul şi modificarea fişierelor sau modificările aduse configuraţiei sistemului de operare sau aplicaţiilor [7].

Sistemele de detecție a intruziunilor, reprezintă o variabilă foarte importantă în ecuația unui sistem bine protejat, pentru că una din cele mai importante resurse, poate chiar mai importantă decât cele materiale, este dată de informaţie şi obţinerea ei. Într-o lume în care echilibrul mondial este dictat de puterea informaţiei, menţinerea confidenţialităţi acesteia este foarte importantă, deoarece aceasta dă valoarea unei informaţii.

BIBLIOGRAFIE

[1] Victoria Stanciu, Andrei Tinca, „Securitatea informației. Principii si bune practici." Ediția a doua, 2015 p. 159–186;

[2] Udroiu, M, „Securitatea informaţiilor în societatea informaţională", Editura Universitară, 2010, p. 402;

[3] SANS Institute, InfoSec Reading Room, „Intrusion Detection Systems", 2001.

[4] Sarcinschi A., Vulnerabilitate, risc, amenințare. Securitatea ca reprezentare psihosocială, Editura Militară, 2009;

[5] Mihai I.C., Securitatea informațiilor, Editura Sitech, 2012, p. 317;

[6] Hotărârea Parlamentului pentru aprobarea Strategiei securității naționale a Republicii Moldova nr. 153 din 15.07.2011 // Monitorul Oficial nr. 170-175 din 14.10.2011;

[7] Informaţii multiple, http://support.microsoft.com