Analiza modelelor de detecție a intruziunilor moderne

Lachi Arina
Departamentul Telecomunicații
UTM
Chișinău, Republica Moldova
arinalachi@gmail.com

Sorochin Serafima
Departamentul Telecomunicații
UTM
Chișinău, Republica Moldova
simona55@mail.md

The techniques of intrusion detection could be potentially useful in identifying unexpected behavior in contemporary application systems. It provides a general overview of the key types and properties of intrusion detection systems. As our focus is on detecting anomalous behavior without a priori knowledge of specific misbehavior patterns, we examine existing techniques focusing on those that support some degree of automation in learning the behavior of the system.

***Termeni cheie – sistem de detecatre a intruziunilor, IDS,* cunoștințe, comportament, model, sistem informațional.**

I. INTRODUCERE

Securitatea sistemelor informaționale este unul din cele mai dinamice compartimente ale domeniului de tehnologii informaționale moderne. Asigurarea securității este acum prioritatea numărul 1 a tutror companiilor specializate în dezvoltarea produselor IT dar și a altor organizații pentru care protecția datelor cu care operează este prioritară.

Evoluția tehnologiei și utilizarea de către angajați a propriilor dispozitive în cadrul companiei creste dificultatea înlăturării amenințărilor interne și externe de către companii. Astfel conform unui studio recent s-a stabilit că securitatea în anul 2018 este mai greu de întreținut ca în 2017, conform opiniei a 51% respondenți [1].

Soluțiile actuale de Securitate se bazează în general pe componente software și hardware capabile să detecteze evenimentele suspicioase încă de la marginea rețelei. Cele mai utilizate sisteme de detecție a intruziunilor implementate în prezent se bazează pe tipuri de comportamente (semnături) dar și pe cunoștințele sistemului, ceea ce și va reprezenta subiectele articolului prezent.

Prevenirea intruziunilor este deci una din prerogativele de bază care ar asigura un nivel mai mare de securitate, deoarece ar limita sau bloca chiar interacțiunea dintre un sistem informațional și tentativele de corupere ale atacatorilor.

II. SISTEMELE DE DETECȚIE A INTRUZIUNILOR

Un sistem de detecție a intruziunilor (IDS) este o soluție de securitate ad-hoc, care urmărește protejarea sistemelor informaționale vulnerabile, dar vulnerabile se consideră absolut toate sistemele conectate la o rețea. Sarcina principală a IDS este de a colecta și analiza datele pentru a identifica evenimentele și procesele suspicioase din sistem în baza cunoștințelor și comportamentului.

Între timp, s-au dezvoltat o serie de tehnici care se concentrează pe diferite tipuri de intruziuni, folosind o varietate de mecanisme. Astfel încât este destul de dificil de a face o clasificare unică a sistemelor de detectare a intruziunilor. De exemplu, taxonomia descrisă în Figura 1 [2] clasifică IDS prin patru caracteristici: metoda de detectare, comportamentul la detectare, locația sursei de audit și frecvența de utilizare și oferă clase-cheie pentru fiecare caracteristică.

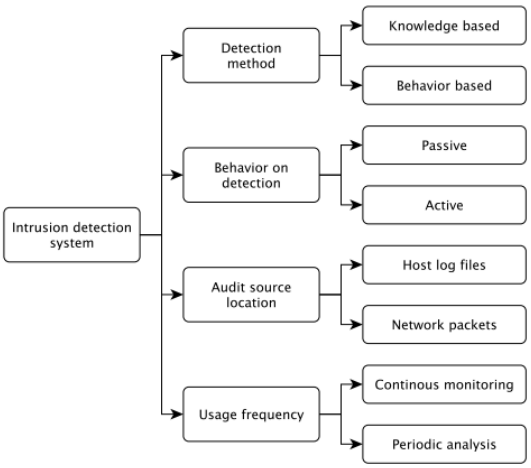

Fig.1 Taxonomia IDS

Fiecare dintre clase conține și alte subclase care nu sunt prezentate în Figura 1. De exemplu, clasa de detectare bazată pe cunoștințe include sisteme expert, analiza semnăturii, rețelele Petri și analiza tranziției în rețea. Această clasificare a fost ulterior extinsă pentru a include mai multe caracteristici și clase [3].

Caracteristicile pot descrie mijloacele tehnice de detectare a unei intruziuni precum și aspectele operaționale ale

sistemelor IDS existente. De exemplu, urmând categoriile în Figura 1, comportamentul la detectare poate fi activ, adică, oferă contramăsuri pentru atac activ sau pasiv, de exemplu, emiterea unei alerte.

În mod similar, având în vedere locația sursei de audit gazdă sau de rețea nu este neapărat importantă. În timp ce majoritatea tehnicilor de detectare a anomaliilor aplicate software-ului sunt bazate pe gazdă [3], observând că activitatea de rețea a unui sistem poate permite identificarea sistematică a comportamentului neașteptat. Astăzi, o rețea nu este folosită numai pentru comunicarea dintre sistem și mediul său, cum ar fi utilizatorii sau infrastructura, dar și pentru funcționarea sa internă. Aplicațiile sunt construite folosind o arhitectură de micro-servicii, în cazul în care un număr de componente independente comunică printr-o rețea utilizând protocoale bine definite.

De asemenea, multe sisteme utilizează servicii de cloud pentru stocare și procesare și comportamentul software-ului ce ar putea fi analizate prin interfețele pe care le comunică [4]. O altă caracteristică din Figura 1 este frecvența de utilizare. Unele tehnici de detectare nu sunt capabile să funcționeze complet on-line și pot numai identifica anomalii atunci când analizează porțiuni complete de activitate.

Aceste trei caracteristici: comportamentul privind detectarea, localizarea sursei de audit și frecvența utilizării, sunt, într-o oarecare măsură, relevante, deoarece acestea reflectă în cea mai mare parte implementarea și detaliile operaționale ale produselor reale de detectare a intruziunilor.

III. Modele de detecție a intruziunilor

În practică, sistemele tipice de detectare a intruziunilor folosesc tehnici bazate pe cunoaștere dar și metode de detecție bazate pe comportament. În continuare vor fi examinate tehnicile comune care stau la baza acestora și va fi evaluat gradul de aplicabilitate pentru detectarea vulnerabilităților în software.

IV. Sisteme de detecție bazate pe cunoștințe

Sistemele bazate pe reguli [5] sunt cele mai populare tehnici folosite de sistemele de detectare a intruziunilor bazate pe cunoaștere. Un sistem conține un set de reguli predefinite pentru atacuri cunoscute sau alte comportamente care sunt nedorite. Funcționarea sistemului, ca de exemplu, modalitățile de execuție sau traficul de rețea, sunt monitorizate pentru a corespunde regulilor preconfigurate ale sistemului. De exemplu, este o practică obișnuită, de a a limita accesul utilizatorilor la contul lor utilizând protocolul FTP. O încercare de a accesa un cont în acest mod poate indica o configurare greșită a sistemului sau un atac de recunoașterea inițiat de un atacator. Sistemele de detectare a intruziunilor, cum ar fi Snort [5], poate fi configurat pentru a detecta o astfel de activitate suspectă prin prescrierea unei reguli, ca de exemplu:

```
alert tcp any any -> any any 21 (content:"user root";)
```

Această regulă setată în Snort face ca sistemul să genereze o alertă în cazul în care detectează un pachet destinat portului 21 (FTP), care conține șirul "user root". Însă acest scenariu este unul foarte simplu și această regulă poate fi compromisă. Comenzile protocolului FTP sunt case-insensitive, astfel încât șirul "user root" și șirul "user(TAB)root", sunt analizate ca fiind diferite, astfel încât activitatea suspicioasă nu va fi analizată ca fiind una suspectă deoarece nu este setată ca regulă. Pentru a seta aceeași regulă dar ca fiind una mai complex și avansată este necesar de a scrie următoarea regulă:

```
alert tcp any any -> any 21 (flow:to_server,established;\
content:"root"; pcre:"/user\s+root/i";)
```

Acest exemplu simplu arată că, chiar și pentru un scenariu simplu stabilirea regulilor este netrivială. Utilizatorul sau sistemul de detectare a intruziunilor trebuie să cunoască că accesarea unui server FTP ca root, este o activitate periculoasă și ar trebui monitorizată. Administratorul de sistem nu specifică absolut toate regulile de unul singur, de exemplu în distribuția standard a lui Snort se includ aproape 3500 de reguli create de comunitate, cu peste 800 de activități prestabilite în mod implicit.
Setul de reguli este revizuit în permanență, iar regulile sunt actualizate ulterior aproape zilnic [6].

O altă tehnică populară bazată pe cunoaștere este folosirea semnăturilor de atac [5]. În loc să folosească regulile generale pentru a defini comportamentul necorespunzător, se bazează pe semnăturile unui atac specific. Astfel, sistemul caută un model specific de semnătură, care indică un anumit atac. O semnătură poate descrie o secvență de acțiuni pe care sistemul o efectuează sau datele pe care le primește în timpul atacului. Adesea, pentru detectarea intruziunilor, sistemele oferă atât potrivirea bazată pe reguli, cât și pe semnătură [5]. Regula sau semnătura bazată pe IDS pot fi, de asemenea, aplicate software-ului, ca unealtă de detecție a malware-ului.

Avantajul cheie al utilizării sistemelor bazate pe cunoștințe este rata scăzută de false-positive și performanța ridicată [5]. Acest lucru se datorează faptului că, de obicei, se execută o verificare simplă dar după criterii precise ceea ce duce la identificarea atacurilor. Principala provocare este incapacitatea de a detecta scenarii necunoscute și neașteptate. Pe măsură ce sunt descoperite noi tehnici de atac sau modificări ale celor existente, setul de semnături devine nefolositor și protecția scade. Atacurile noi trebuie să fie înregistrate în permanență, iar seturile de reguli trebuie să fie actualizate. De asemenea, o problemă majoră este și că malware-ul complex folosește polimorfismul pentru a-și modifica comportamentul, făcând detectarea mai dificilă .

Detectarea anomaliilor se bazează pe ipoteza că o abatere de la comportamentul normal al sistemului, poate reprezenta o intruziune. Principalul beneficiu al acestei abordări este o capacitate de a detecta atacuri necunoscute sau neașteptate. În practică, totuși, mecanismele bazate pe comportament includ o componentă bazată pe cunoștințe, care specifică

caracteristicile de monitorizare, dar și devierea care ar trebui clasificată ca o anomalie.

V. MODELE STATISTICE

Modelele statistice [7] sunt printre cele mai simple și cele mai populare modalități de definire a comportamentului normal. Funcționarea cheie a acestor sisteme este de a sonda diverse sisteme, caracteristici periodice și să compare rezultatele cu valorile de bază. De exemplu, un anumit număr de încercări de conectare nereușite este normal, însă un număr neobișnuit de mare poate indica un atac brutal. Astfel sistemul poate fi configurat cu o valoare care stabilește un prag pentru numărul de încercări de conectare nereușite care reprezintă un comportament normal. Dacă se atinge pragul, sistemul poate genera o alertă. O anumită cantitate de cunoștințe este necesară, de exemplu: faptul că o anumită caracteristică (numărul de intrări nereușite) este interesant, unde pot fi obținute datele și valoarea pragului, dificultatea de a implementa această abordare crește odată cu dimensiunea sistemului. O abordare mai utilă este de a deduce automat caracteristicile normale ale sistemului din operația trecută. De exemplu, numărul de conectări nereușite poate să fie stabilit prin analizarea jurnalelor de sistem. Funcționarea normală a sistemului poate să fie modelat într-un mod mai granulat, sistemul poate învăța orele de lucru tipice și locația de la care se conectează utilizatorii, pe baza activității înregistrate anterior. De asemenea, poate învăța separat modelele normale pentru persoane fizice și grupuri de utilizatori [7]. Deși este posibil să se stabilească limitele în mod automat, semnificația caracteristicilor monitorizate de sistem trebuie să fie înțelese mai întâi. În plus, modelele bazate pe statistici captează doar scenarii de intruziune relativ simple, definite ca cantitate sau frecvență de acțiuni discrete. O altă problemă care trebuie luată în considerare sunt fluctuațiile naturale ale cantităților de evenimente datorate volumului de muncă, partea zilei, zilele săptămânii sau lunii [7]. Indiferent de cât de bine sistemul poate stabili valorile de bază, acesta încă mai necesită cunoștințele de specialitate pentru a specifica ce proprietăți ale comportamentului sistemului, cum ar fi numărul de încercări de conectare eșuate, ar trebui monitorizate.

VI. SISTEME EXPERT

Sistemele expert de detectare a anomaliilor utilizează reguli generate automat pe baza comportamentului din trecut înregistrat. Sistemul analizează jurnalul de audit și construiește un sistem de reguli pentru a identifica modelele repetate de corelații între diferite atribute.

Astfel de modele pot varia de la generice, cum ar fi "terminalele valide sunt T1,. . . .Tn ", până la foarte specific:" marți, între orele 6:00 și 7:00, când utilizatorul

are un privilegii de operator de sistem și utilizează terminalul T3, doar comenzi care utilizează foarte puțină activitate directă pe disc ". Un pas mai departe este generarea de reguli

bazată pe corelarea mai multor evenimente ulterioare. Avantajul cheie al acestui sistem, comparativ cu modelele statistice, este că detectează automat caracteristicile sistemului care sunt importante și trebuie incluse în model. Aceste reguli pot reflecta politicile de securitate intenționate, precum și caracteristicile care nu sunt așteptate sau considerate importante, dar este util să se ia în considerare când afirmând funcționarea corectă a sistemului.

Astfel de reguli rezultă din configurația sistemului, modelele de utilizare sau mediul în care operează. Performanța sistemului poate fi îmbunătățită prin reglarea regulilor bazate pe feedback-ul operatorului, de exemplu atunci când se detectează un fals pozitiv [8]. Analizând această abordare este posibilă construirea unui model de comportament al sistemului cu o cantitate limitată de cunoștințe de specialitate. Cu toate acestea, este nevoie de informații detaliate, de expert, despre structura jurnalului și tipurile de date ale elementelor sale, cum ar fi utilizarea timpului sau a procesorului, în clustere discrete. Mai recent, similar au fost aplicate tehnici de generare automată a politicilor de securitate pentru Java.

VII. CONCLUZII

Tehnicile de detectare a intruziunilor bazate pe comportament necesită adesea un anumit grad cunoștințe de specialitate pentru a ghida funcționarea acestora. Secvența de operațiuni bazate pe tehnici oferă un echilibru corect între comportament și cunoaștere, abordări și au fost aplicate la detectarea atacurilor împotriva software-ului în ultimii 20 de ani.

Dovezile experimentale pentru eficacitatea acestor tehnici sunt limitate. Singura încercare de a evalua mai multe tehnici de detecție se concentrează, de asemenea, pe aceleași câteva aplicații și pe vulnerabilitățile corespunzătoare acestor aplicații.

Aplicabilitatea tehnicilor de detectare a anomaliilor la sistemele stratificate de mari dimensiuni care rulează pe platformele software moderne rămâne în mare parte neexplorată.

BIBLIOGRAFIE

[1] https://www.sourcesecurity.com/news/co-11895-ga.13674.html

[2] H. Debar, M. Dacier, and A. Wespi. Towards a taxonomy of intrusion detection systems. *Comput. Netw.*, 31(9):805–822, April 1999.

[3] C. Warrender, S. Forrest, and B. A. Pearlmutter. Detecting intrusions using system calls: Alternative data models. In *IEEE Symposium on Security and Privacy*, pages 133–145, 1999.

[4] O. Pieczul and S. N. Foley. Collaborating as normal: Detecting systemic anomalies in your partner. In *Security Protocols XXII: 22nd International Workshop, Cambridge, UK, March 19-21, 2014, Revised Selected Papers*, pages 18–27. Springer International Publishing, 2014.

[5] M. A. Jamshed, J. Lee, S. Moon, I. Yun, D. Kim, S. Lee, Y. Yi, and K. Park. Kargus: A highly-scalable software-based intrusion detection system. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 317–328, New York, NY, USA, 2012. ACM.

[6] Snort. Snort subscriber rule set categories. Online https://www.snort.org/rules_explanation, retrieved 10 Nov 2016.

[7] C. Wang, K. Viswanathan, L. Choudur. Statistical techniques for online anomaly detection in data centers. In *12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011) and Workshops*, pages 385–392, May 2011.