Cuprins

Capitolul I

Amenințări și tendințe în ce privește securitatea sistemelor informatice și rețelelor de comunicații

Secțiunea I
Considerații generale

Încă de la apariția sistemelor informatice şi rețelelor de comunicații au fost căutate vulnerabilităților acestora, fie în scopul îmbunătățirii performanțelor şi siguranței în exploatare fie în scopul compromiterii lor.

Secțiunea a II-a
Principalele taxonomii dezvoltate în sfera securității sistemelor informatice și rețelelor de comunicații

***Taxonomia*,** conform definiției[1], este mai mult decât o clasificare, în sensul că aceasta descrie principiile conform cărora clasificarea a fost făcută, dar şi procedura care trebuie urmată pentru clasificarea unui obiect nou[2].

În sfera securității sistemelor informatice şi a rețelelor de comunicații, taxonomiile au apărut din nevoia de a oferi consecvență şi coerență în limbajul utilizat pentru descrierea şi clasificarea vulnerabilităților şi atacurilor asupra acestora şi a se evita astfel (pe cât posibil) confuziile.

De asemenea, aceste taxonomii permit aplicarea cunoştințelor anterioare amenințărilor noi, cât şi un mod organizat de percepere a acestora (amenințărilor).

O ***taxonomie satisfăcătoare*** prezintă următoarele **caracteristici**[3]:

---

[1] Taxonomia este considerată „știința legilor de clasificare" (a se vedea Academia Română Institutul de lingvistică, Iorgu Iordan, *Dicționar explicativ al limbii române*, ed. a II-a, Ed. Univers Enciclopedic, București, 1998, p. 1072) sau „știința care se ocupă cu stabilirea legilor de clasificare și sistematizare a domeniilor din realitate cu o structură complexă" (a se vedea DEX online, la http://dexonline.ro/ search.php?Cuv=taxonomie).

[2] A se vedea şi Berghe C. V., Riordan J. Piessens F., *A Vulnerability Taxonomy Methodology applied to web Services*, L.P. 4, disponibil on-line la http://chris.vandenberghe. org/publicattions/ vulnerability_taxonomy_nerdsec2005.pdf.

[3] Lough D. L., *A Taxonomy of Computer Attack with Application to Wireless Networks*, teză de doctorat susținută la Virginia Polytechnic Institute and State University, Virginia, (apr.), 2001, p. 37-39, disponibil on-line la http://scholar.lib.vt.edu/theses/available/etd-etd-04252001-

– ***acceptată*** (Howard, 1997)/***adecvată*** (Amoroso, 1994), în sensul de a fi structurată de o asemenea manieră astfel încât să fie aprobată în general;

– ***comprehensibilă*** (Lindqvist şi Jonsson, 1997), în sensul de a putea fi înţeleasă atât de către specialişti, cât şi de către cei care manifestă interes în domeniu;

– ***completă*** (Amoroso, 1994)/***exhaustivă*** (Howard, 1997; Lindqvist şi Jonson, 1997), în sensul că ar trebui să ţină cont de toate posibilele ameninţări;

– ***precisă*** (Krsul, 1998; Bishop, 1999)***/clară*** (Howard, 1997; Lindqvist şi Jonsson, 1997), în sensul că trebuie să fie clar precizată astfel încât să evite ambiguitatea;

– ***repetabilă*** (Howard, 1997; Lindqvist şi Jonsson, 1997), în sensul că acele clasificări ar trebui să fie repetabile;

– ***folositoare*** (Howard, 1997; Lindqvist şi Jonsson, 1997), în sensul că trebuie să poată fi utilizată pentru o bună cunoaştere a domeniului;

– ***obiectivă*** (Krsul, 1998), în sensul că acele caracteristici trebuie să fie identificate de la obiectul cunoscut nu de la cunoştinţele subiectului;

– ***să se excludă reciproc*** (Howard, 1997; Lindqvist şi Jonsson, 1997), în sensul că o anumită ameninţare să fie grupată într-o singură categorie.

Faţă de caracteristicile prezentate, ***se poate concluziona***[1]:

– realizarea unei bune taxonomii este dificilă;

– taxonomia depinde nu numai de ameninţările respective ci şi de punctul de vedere a celui care o realizează, punct de vedere care este condiţionat de presupusa utilizare a taxonomiei;

– ameninţările, frecvent, se manifestă grupat şi prezintă proprietăţi comune.

Din motivele prezentate, nu surprinde marea diversitate a taxonomiilor dezvoltate în sfera securităţii sistemelor informatice şi reţelelor de comunicaţii.

Având în vedere că majoritatea acestor taxonomii au un pronunţat caracter tehnic, de specialitate, fiind dezvoltate de specialiştii din domeniul securităţii sistemelor informatice şi reţelelor de comunicaţii şi mai puţin pentru autorităţile de aplicare a legii, am să prezint în continuare acele taxonomii înţelese şi de aceia

234145/unrestricted/lough.dissertation.pdf. Lough compilează proprietăţile unei taxonomii din lucrările a cinci autori Amoroso E. G. (*Fundamentals of Computer Security Technology*, Prentice Hall, Englewood Clifs, N.J., 1994), Bishop M. (*How Attackers Break Programs, and How to Write Programs More Securely*, 8th net, USENIX Security Symposium, aug., 1999), Howard J. D. (*An Analysis of Security Incident on the Internet*, 1989-1995, teză de doctorat susţinută la Purdue University, apr., 1997), Krsul I. V. (*Software Vulnerability Analysis,* teză de doctorat susţinută la Purdue University, mai, 1998) Lindqvist U. şi Johnsson E., (*How to Systematically Classify Computer Security Intrusions*, IEEE Security and Privacy, 1997).

[1] A se vedea şi Berghe C.V., Riordan J., Piessens F., *A Vulnerability …*, *op. cit.*, p. 5.

care nu sunt neapărat specialişti, dar manifestă interes în domeniul securităţii sistemelor informatice şi reţelelor.

§ 1. Palauskas N., Garsva E., Clasificarea atacurilor asupra sistemelor informatice[1]

Această taxonomie (numită de autori, din modestie, clasificare) este bazată atât pe clasificările anterioare cât şi pe experienţa autorilor.

Autorii consideră că fiecare *atac* întruneşte ***14 trăsături***[2] care sunt prezentate schematic şi în legătură[3]:

(1) *în funcţie de obiectivul atacului:*
- (1.1) dobândirea privilegiului administratorului (super-utilizatorului);
- (1.2) dobândirea privilegiului utilizatorului;
- (1.3) refuzarea serviciului;
- (1.4) încălcarea serviciului;
- (1.5) încălcarea confidenţialităţii informaţiilor sau resurselor sistemului;
- (1.6) executarea codurilor maliţioase;
- (1.7) încălcarea politicii de securitate.

(2) *în funcţie de tipul efectului:*
- (2.1) detectarea Codului executabil;
- (2.2) „Cal troian", virus;
- (2.3) detectarea Codului executabil al aplicaţiilor de (web) reţea;
- (2.4) utilizarea neautorizată a unei staţii de lucru intermediare tip „server Proxy";
- (2.5) inundarea memoriei tampon;
- (2.6) sondarea sau scanarea;
- (2.7) folosirea unor protocoale neacceptate;
- (2.8) folosirea unor porturi neacceptate;
- (2.9) deghizarea ca alt sistem „gazdă";
- (2.10) inserarea unor obiecte false.

(3) *în funcţie de nivelul modelului de referinţă ISO/OSI*

---

[1] Palauskas N., Garsva E., *Computer System Attack Classification*, în Electronics and Electrical Engineering, nr. 2 (66), 2006, pp. 84-87, disponibil on-line la http://www.ee.ktu.lt/journal/2006/2/1392-1215-2006-02-66-84.pdf.

[2] *Ibidem*, p. 85.

[3] *Ibidem*, p. 86.

(3.1) fizic;
(3.2) conexiuni de date;
(3.3) rețea;
(3.4) transport;
(3.5) sesiune;
(3.6) prezentare;
(3.7) aplicație.

(4) *în funcție de sistemul de operare OS*
(4.1) Windows;
(4.2) Linux;
(4.3) Solaris;
(4.4) BSD;
(4.5) MacOS;
(4.6) altele.

(5) *în funcție de locația subiectului atacului*
(5.1) în interiorul segmentului local;
(5.2) între segmente;
(5.3) acces fizic;
(5.4) privilegiu de utilizator al sistemului;
(5.5) privilegiu de administrator de sistem.

(6) *în funcție de tipul locației obiectului*
(6.1) sistem local;
(6.2) rețea locală;
(6.3) rețea globală;
(6.4) rețea fără fir;
(6.5) rețea tip P2P.

(7) *în funcție de serviciul atacat*
(7.1) rețeaua (web), (HTTP);
(7.2) transfer de fișiere (FTP,SMB,CIFS);
(7.3) poștă (SMTP, POP 3, IMAP);
(7.4) control de rețea (SNMP);
(7.5) nume de domeniu (DNS);
(7.6) control la distanță (telnet, SSH, RDP);
(7.7) configurarea sistemului tip „Gazdă";
(7.8) rutare dinamică (RIP, OSPF);
(7.9) incriptare (SSL);
(7.10) altele.

(8) *în funcție de concentrarea atacului*
(8.1) atomic;
(8.2) fragmentat.

(9) *în funcție de retroacțiune*
  (9.1) cu retroacțiune;
  (9.2) fără retroacțiune.
(10) *în funcție de condițiile inițiale de executare a atacului*
  (10.1) la solicitarea obiectului de atac;
  (10.2) la un eveniment specific obiectului de atac;
  (10.3) necondiționat.
(11) *în funcție de condițiile inițiale de executare a atacului*
  (11.1) pasiv;
  (11.2) activ.
(12) *în funcție de automatizarea atacului*
  (12.1) automatic;
  12.2 semi-automatic;
  12.3 manual.
(13) *în funcție de sursa atacului*
  (13.1) unu contra unu;
  (13.2) mai mulți contra unu;
  (13.3) unu contra mai mulți.
(14) *în funcție de calitatea legăturilor*
  (14.1) singură;
  (14.2) multiplă.

Autorii consideră[1] (și de aici se conturează caracterul de taxonomie) că „realizarea obiectivului este cea mai importantă pentru atacator (1), prin urmare, evaluarea numerică a severității atacului este fondată pe aceasta. Tipul efectului (2) depinde mai mult de obiectivul intrusului la fel ca și locația subiectului și obiectului. Modelul ISO/OSI poate descrie toate procesele de sistem. Nivelul aplicației (3.7) este cel mai potrivit, din cauza potențialității și complexității sale, pentru a efectua atacuri. Există o varietate de sisteme de operare OS în rețeaua globală, familii specifice de sisteme de operare OS au vulnerabilități comune care atrag atacuri specifice OS (4). Locația subiectului atacului (5) influențează tipul efectului și probabilitatea îndeplinirii obiectului atacului. Tehnologia atacului și posibilele amenințări sunt influențate de tipul locației obiectului (6) și de serviciul atacat (7). Atacul poate fi concentrat într-un singur pachet, și atacul este denumit atomic (8.1.) sau poate fi fragmentat în câteva pachete (8.2.). Retroacțiunea (9) nu este necesară pentru toate atacurile... Pentru a evita detectarea sau pentru o mai bună eficiență, atacatorii pot alege diferite condiții inițiale de exe-

[1] *Ibidem*, p. 85.

cutare (10), tipuri de impact (11) sau nivele de automatizare (12). În conformitate cu obiectivele atacului şi tipul efectului, numărul surselor atacului (13) şi cantitatea legăturilor (14) pot diferi".

§ 2. Howard John D., Longstaff Thomas A., Un limbaj comun pentru incidentele privind securitatea calculatoarelor[1]

Aceasta este una dintre cele mai bune taxonomii dezvoltate, şi are ca bază teza de doctorat a lui John Howard (unul dintre autori), „*O analiză a incidentelor de securitate pe Internet 1989-1995*"[2].

Autorii au dezvoltat un set minim de termeni de „nivel înalt", împreună cu o structură care indică legăturile dintre aceştia (o taxonomie), care poate fi folosită pentru a clasifica şi înţelege informaţiile incidentelor de securitate a calculatoarelor.

Unii autori susţin[3] „Howard încearcă să concentreze atenţia pe procesul care conduce taxonomia, mai degrabă, decât pe o schemă de clasificare... Aceasta însemnă că întregul proces al atacului este luat în considerare, ceea ce este, cu siguranţă, valoros... Howard nu reuşeşte să îndeplinească una dintre cerinţele taxonomiei sale: să se excludă reciproc. Unele dintre categorii se pot suprapune... pentru organele de informare cum ar fi CERT, o astfel de taxonomie nu poate fi practică. Organele de informare sunt mai preocupate de atacul în sine decât de motivaţiile şi obiectivele din spatele lui... problemele menţionate mai sus există încă chiar cu taxonomia perfecţionată".

Nu sunt de acord cu aceste consideraţii şi chiar dacă unele dintre subcategoriile descrise nu s-ar exclude reciproc, aşa cum susţin autorii mai sus citaţi[4] dar şi alţii[5], totuşi, *consider mai valoroasă descrierea procesului prin care atacatorul reuşeşte să îşi îndeplinească obiectivul, decât o simplă clasificare a atacurilor*.

---

[1] Howard J.D., Longstaff T.A., *A Common Language for Computer Security Incidents*, Sandia Report (SAND98-8667), (oct.) 1998, disponibil on-line la http://www. cert.org/research/ taxonomy_988667.pdf.

[2] Howard J.D., *An Analysis of Security Incidents on the Internet 1989-1995*, teză de doctorat susţinută la Carnegie University, Pittsburg, Pensylvania, (apr.) 1997, disponibil on-line la http://www.dtic.mil/mil/cgi-bin/GetTRDoc?AD=ADA389085& Location=U2&doc=GetTRDOC.pdf.

[3] Hansman S., Hunt R., *A taxonomy of network and computer attacks*, în Computers &Security, (iun) 2004, p. 4, disponibil on-line la http://ce.sharif.edu/courses/83-84/1/ce534/ resorces/root/Papers/attacks; Steichen P., Advanced Security Methodologies – Computer and Network attacks, pp. 15-16, disponibil on-line la http://pst.libre.eu/m2ssic-metz/02_attacks.pdf.

[4] *Ibidem*.

[5] Lough D. L., *A taxonomy …*, *op. cit*., p. 50.

Revenind la taxonomia dezvoltată, și la procesul care conduce această taxonomie, trebuie precizat că, față de taxonomia inițială (Howard, 1997), aceasta este structurată în 7 categorii (față de 5 categorii) și fiecare categorie este mai bine structurată și dezvoltată.

În prezentarea și explicarea taxonomiei dezvoltate, autorii identifică trei grupuri generale:

– *eveniment* – „o acțiune îndreptată către o țintă, intenționându-se a avea drept rezultat o schimbare a statusului țintei respective"[1] –, care include categoriile „acțiuni" și „ținte", și este inclus grupul general „atac(uri)";

– *atac(uri)* – „o serie de măsuri luate de un atacator pentru a obține un rezultat neautorizat"[2] –, care include, alături de grupul general „eveniment" și categoriile „unelte", „vulnerabilitate" și „rezultate neautorizate" și este inclus în grupul general „incident";

– *incident* – „un grup de atacuri care se pot distinge de alte atacuri datorită deosebirii atacatorilor, atacurilor, obiectivelor, localizării și sincronizării"[3] – care include alături de grupul general „atac(uri)" și categoriile „atacatori" și „obiective".

Alături de aceste grupuri generale identifică alți termeni mai generali care pot fi necesari pentru a putea descrie complet un incident[4]:

– locația (numele, numărul, cele care au raportat);
– data (raportării, începerii, încheierii);
– numărul incidentului;
– acțiunile corective.

Categoriile și subcategoriile incluse în taxonomia dezvoltată sunt următoarele:

a) ***atacatorul*** – „un individ care încearcă unul sau mai multe atacuri pentru a atinge un obiectiv" –; din această categorie fac parte:

– ***hackeri*** – „atacatori care atacă calculatorul pentru provocare, statut sau emoția obținerii accesului";

– ***spioni*** – „atacatori care atacă calculatoarele pentru informații care să fie folosite pentru avantaje politice";

– ***teroriști*** – „atacatori care atacă calculatoarele pentru a provoca teamă pentru avantaje politice";

– ***invadatori corporativi*** – „angajați (atacatori) care atacă calculatoarele concurenților pentru câștig financiar";

---

[1] Howard J. D., Longstaff T.A., *A Common Language …, op. cit.*, p. 7.
[2] *Ibidem*, p. 12.
[3] *Ibidem*, p. 15.
[4] *Ibidem*, pp. 17-18.

– ***criminali profesionişti*** – „atacatori care atacă calculatoarele pentru câştig financiar";

– ***vandali*** – „atacatori care atacă calculatoarele pentru a provoca daune".

b) ***instrumentul*** – „mijloc de exploatare a vulnerabilităţii unui calculator sau reţele"; din această categorie fac parte:

– ***atac fizic*** – „mijloc de a fura fizic sau a strica calculatorul, reţeaua, componentele sale sau sistemele de suport ale sale (cum ar fi aerul condiţionat, energia electrică etc.)";

– ***schimb de informaţii*** – „un mijloc de a obţine informaţii de la alţi „atacatori" (cum ar fi buletine electronice), sau de la persoane care au fost atacate (aşa numita inginerie socială)";

– ***comandă a utilizatorului*** – „un mijloc de a exploata o vulnerabilitate prin introducerea de comenzi într-un proces prin intermediul introducerii de date direct de utilizator în interfaţa procesului. Un exemplu este introducerea comenzilor Unix prin intermediul unei conexiuni telnet sau de la un port SMPT";

– ***script sau program*** – „un mijloc de a exploata o vulnerabilitate prin introducerea de comenzi într-un proces prin executarea unui fişier de comenzi (script) sau a unui program în interfaţa procesului. Exemple sunt o sesiune Shell script pentru a exploata o eroare a programului, un program de conectare tip cal troian sau un program de spargere a parolei";

– ***agent autonom*** – „un mijloc de exploatare a unei vulnerabilităţi prin utilizarea unui program sau a unui fragment dintr-un program care operează independent de utilizator. Exemple sunt viruşii şi viermii";

– ***kit de instrumente*** – „un pachet de programe care conţine scripturi, programe sau agenţii autonome care exploatează vulnerabilităţile. Un exemplu este larg răspânditul kit de instrumente numit kit de acces la rădăcină";

– ***instrument distribuit*** – „un instrument care poate fi distribuit la mai multe sisteme tip gazdă care pot fi apoi coordonate pentru a efectua în mod anonim un atac „după un anumit timp simultan asupra unor sisteme tip gazdă";

– ***interceptor de date*** – „un mijloc de monitorizare a radiaţiilor electromagnetice provenite de la un calculator sau reţea folosind un dispozitiv extern".

c) ***vulnerabilitate*** – „un punct slab într-un sistem care să permită o acţiune neautorizată" –; din această categorie fac parte:

– ***vulnerabilitate de proiectare*** – „o vulnerabilitate în proiectarea sau specificaţiile echipamentului sau programului care chiar şi după o implementare perfectă va avea ca rezultat o vulnerabilitate";

– ***vulnerabilitate de implementare*** – „o vulnerabilitate care rezultă dintr-o eroare în implementarea programului sau echipamentului care au fost proiectate corespunzător" –;

– *vulnerabilitate de configurare* – „o vulnerabilitate care rezultă dintr-o eroare în configurarea unui sistem, cum ar fi să ai un cont cu parole implicite, să ai permisiune de scriere... pentru fișiere noi sau să ai active servicii vulnerabile".

d) ***acțiune*** – „o măsură luată de către un utilizator sau proces în vederea obținerii unui rezultat"; din această categorie fac parte:

– *sondare* – „accesarea unei ținte în vederea determinării caracteristicilor sale";

– *scanare* – „accesarea secvențială a unui set de ținte în scopul de a identifica care țintă are o caracteristică specifică" –;

– *inundare* – „accesarea repetată a unei ținte în scopul de a supraîncărca capacitatea țintei" –;

– *autentificare* – „prezentarea identității cuiva unui proces și, dacă este necesar, verificarea acelei identități în vederea accesării unei ținte" –;

– *ocolire* – „evitarea unui proces prin utilizarea unei metode alternative de accesare a țintei" –;

– *păcălire* – „deghizare prin „asumarea apariției unei alte entități în rețea";

– *citire* – „obținerea conținutului datelor din dispozitivele de stocare sau alte medii de date" –;

– *copiere* – „reproducerea unei ținte lăsând neschimbată ținta originală";

– *furt* – „luarea în posesie a unei ținte fără a lăsa o copie în locația originală";

– *modificare* – „schimbarea conținutului sau caracteristicilor unei ținte";

– *ștergere* – „îndepărtarea unei ținte sau transformarea în irecuperabilă".

e) ***țintă*** – „o entitate logică sau fizică a unui calculator sau rețele":

– *cont* – „un domeniu pentru accesul utilizatorului pe un calculator sau rețea care este controlat ținându-se seama de o înregistrare de informații care conține numele contului utilizatorului, parola și restricții de utilizare";

– *proces* – „un program în executare, constând în programul executabil, datele și stiva programului, controlul programului, indicatorul de stivă SP și alți regiștrii și toate celelalte informații necesare pentru executarea unui program";

– *dată* – „reprezentarea de date, concepte sau instrucțiuni într-o manieră adecvată pentru comunicare, interpretare sau prelucrare de către om sau prin mijloace automate. Datele pot fi sub forma fișierelor, în memoria volatilă sau permanență a calculatorului sau într-un dispozitiv de stocare, sau într-o formă de date în tranzit printr-un mediu de transmitere";

– *componentă* – „una dintre părțile din care este făcut calculatorul sau rețeaua;

– *calculator* – „un dispozitiv care este alcătuit din unul sau mai multe componente asociate, inclusiv unitatea de procesare și unitățile periferice, care este controlată de programe stocate intern și care poate efectua calcule substanțiale,

incluzând numeroase operațiuni matematice sau operațiuni logice, fără intervenţie umană în timpul execuției";

– *rețea* – „un grup de calculatoare gazdă interconectate şi interdependente, elemente de comutare şi ramificații interconectate";

– *inter-rețele* – „o rețea de rețele".

f) ***rezultat neautorizat*** – „o consecinţă neautorizată a unui eveniment"; din această categorie fac parte:

– ***acces crescut* –** „o creştere neautorizată în domeniul de acces de pe un calculator sau rețea";

– ***divulgare de informații* –** „diseminarea de informaţii către orice persoană care nu este autorizată să acceseze acele informații";

– ***falsificare de informații* –** „modificarea neautorizată a datelor de pe un calculator sau rețea";

– ***refuzare a serviciului* –** „deteriorarea sau blocarea intenţionată a resurselor calculatorului sau rețelei";

– ***furt de resurse* –** „utilizarea neautorizată a resurselor calculatorului sau rețelei";

g) ***obiective*** – „scopul sau obiectivul final al unui incident"; din această categorie fac parte:

– *provocare, status, emoție;*

– *câștiguri politice;*

– *câștiguri financiare;*

– *pagubă*.

Taxonomia completă este prezentată de autori sub formă grafică[1] fiind evidenţiată relaţia dintre evenimente, de la atacuri la incidente, şi sugerează că prevenirea îndeplinirii obiectivelor atacatorilor ar putea fi realizată prin asigurarea faptului că un atacator nu ar reuşi parcurgerea celor şapte paşi descrişi mai sus.

§ 3. Weber Daniel James, O taxonomie a intruziunilor în calculatoare[2]

Taxonomia dezvoltată de acest autor, a fost creată special pentru testarea şi evaluarea sistemelor de detectare a intruziunilor (IDS).

---

[1] *Ibidem*, p. 16.

[2] Weber D.J., *A Taxonomy of Computer Intrusions*, lucrare de dizertație susținută la Massachuetts Institute of Technology, (iun.) 1998, disponibil on-line la http://dspace.mit.edu/bitstream/handle/1721.1/9861/41473759.pdf.

Autorul consideră[1] „taxonomia necesită un mod de descriere a nivelurilor privilegiului, un mod de descriere a tranzițiilor și un mod de clasificare a acțiunilor". Astfel:

(1) ***niveluri ale privilegiului utilizatorului***:

a) ***fără acces (O)***, când nu are practic acces la un sistem;

b) ***rețea la distanță (R)***, când are un minim acces de rețea la un sistem prin intermediul altor rețele;

c) ***rețea locală (L)***, când are abilitatea să citească și să scrie în rețeaua locală ceea ce dispozitivul țintă folosește;

d) ***acces modem (M)***, când are abilitatea să se conecteze direct la un calculator țintă;

e) ***acces utilizator (U)***, când are abilitatea să ruleze comenzi normale de utilizator;

f) ***acces la rădăcină/status de administrator (S)***, când are acces total la sistem.

(2) ***acțiuni***:

a) ***sondare***, în situația în care sunt colectate datele despre sistem:

– *sondare (Utilizator)*, când privesc utilizatorul dispozitivului;

– *sondare (Serviciu)*, când privesc serviciile dispozitivului;

– *sondare (Dispozitiv)*, când privesc dispozitivele în rețea.

b) ***refuz al serviciului***, în situația în care este împiedicat accesul legitim la sistem (include deteriorarea serviciului):

– *Refuz (Temporar)*, când refuzul este temporar, cu recuperare automată;

– *Refuz (Administrativ)*, când refuzul necesită acțiunea administratorului pentru recuperare;

– *Refuz (Permanent)*, când refuzul este permanent.

c) ***interceptare/citire a datelor***, în situația în care sunt interceptate/citite datele:

– *interceptare (Fișiere)*, când sunt vizate fișierele unui sistem;

– *interceptare (Rețea)*, când este vizat traficul de rețea.

d) ***alterare/creare a datelor***, în situația în care sunt alterate/create datele:

– *Alterare (Date)*, când vizează alterarea datelor stocate;

– *Alterare (Urmărire, intruziune)*, când vizează înlăturarea urmelor intruziunii.

e) ***utilizare a sistemului de către atacatori***, în situația în care sistemul țintă este utilizat de atacator:

– *Utilizare (Recreațională)*, când vizează utilizarea sistemului pentru distracție;

---

[1] *Ibidem*, p. 40.