

INTERNEWS
RITI dot-Gov



MCTI

Bucure⁰ti,
Mai 2004

Elaborarea acestui ghid a fost posibilă prin asistența asigurată de către Centrul de Servicii Regional Budapesta al Agenției Statelor Unite pentru Dezvoltare Internațională, USAID, în cadrul Acordului nr. CA # 186-A-00-02-00101-00; LA#GDG-A-00-01-00009-00; Internews Network/RITI dot-Gov Project.

Opiniile exprimate în cadrul acestui document aparțin autorilor și nu reprezintă în mod necesar vederile Agenției Statelor Unite pentru Dezvoltare Internațională.

© Internews Network, Inc., 2004. Acest ghid poate fi utilizat și copiat în scop ne-comercial atâta vreme cât "Internews Network, RITI dot-GOV" este creditat ca sursă și "USAID" menționat ca finanțator.

Capitolul IV – Vulnerabilități ale sistemelor informatice

Începuturile

2 noiembrie 1988 este o zi importantă pentru Internet. În acea zi un proaspăt absolvent al Universității Cornell din Statele Unite, Robert Morris Jr., a executat un program de tipul *vierme*, primul program care a afectat într-un mod foarte serios Internet-ul. În câteva secunde, mii de calculatoare de pe întreg teritoriul Statelor Unite au fost scoase din funcțiune de neobișnuitul program. Sute de rețele ale institutelor de cercetare, universităților, dar și ale celor câteva companii care erau conectate în acea vreme la Internet au fost afectate.

În decursul a câteva ore a fost format un grup de voluntari care să rezolve cât mai rapid această situație urgentă. Membrii grupului, denumit „Virus Net”, comunicau cu ajutorul telefonului și al segmentelor neafectate ale rețelei. În urma unui efort deosebit au reușit să identifice cauza problemei, să izoleze programul virus și să găsească o slăbiciune în codul acestuia. Această descoperire a făcut ca răspândirea virusului să fie oprită într-un timp record de 24 de ore de la apariție.

Modalitatea prin care programul, denumit *vierme*, deoarece se propagă prin rețea, a infectat și oprit atât de multe calculatoare este foarte simplă. După ce programul infecta un calculator crea două copii ale sale în memorie, al căror scop era să caute alte calculatoare care să poată fi infectate. Aceste două copii creau fiecare la rândul lor câte două copii ale virusului. Un calcul simplu, arată că la a 16-a „generație” pe calculator existau mai mult de 65 de mii de copii ale programului pe sistemul infectat, și alte 65 de mii de alte calculatoare cercetate pentru a fi infectate.

Cum programul nu se oprea, el ajungea în timp foarte scurt să consume toate resursele calculatorului, acesta nemaifiind capabil să răspundă comenzilor utilizatorilor legitimi. Deși problema se rezolva printr-o simplă repornire a calculatorului, era foarte probabil ca acesta să fie reinfectat în foarte scurt timp, de către celelalte sisteme care rula copii ale virusului.

Deși nu a avut efecte catastrofale, Internet-ul fiind format din foarte puține calculatoare la acea vreme (câteva zeci de mii, față de câteva sute de milioane câte sunt acum), acest incident a tras un serios semnal de alarmă în ceea ce privește securitatea sistemelor informatice în general și a rețelelor în special.

Virusul lui Morris a revelat vulnerabilitatea Internetului și a făcut să fie conștientizată nevoia de securizare a acestuia, având același efect asupra lumii informatice ca și efectul primei deturnări a unui avion de pasageri, în 1960, asupra lumii aviației.

Despre riscuri

În lumea reală există persoane care pătrund în case și pot fura tot ce găsesc valoros. În lumea virtuală există indivizi care pătrund în sistemele informatice și „fură” toate datele valoroase. La fel cum în lumea reală există oaspeți nepoftiți și persoane care simt plăcere atunci când își însușesc sau distrug proprietatea altcuiva, lumea calculatoarelor nu putea fi lipsită de acest fenomen nefericit. Este cu adevărat detestabilă perfidia acestor atacuri. Căci dacă se poate observa imediat lipsa cutiei cu bijuterii, o penetrare a serverului de

contabilitate poate fi depistată după câteva luni, atunci când toți clienții au renunțat la serviciile firmei deoarece datele furate și ajunse la concurență au ajutat-o pe aceasta să le facă oferte mai bune.

Poveștile despre *cracker*-i și viruși periculoși constituie deliciul cărților și articolelor de securitate informatică. Poate tocmai de aceea pericolul cel mai mare în ceea ce privește asigurarea acestei securități este de cele mai multe ori neglijat. Pentru că cele mai multe amenințări nu vin din exterior, ci din interior.

Noțiunea de *persoană din interior* este oarecum greu de definit. Spre exemplu membrii unui departament se consideră reciproc drept fiind din *interior*, cei de la celelalte departamente fiind considerați ca fiind din afară. În ceea ce privește securitatea, o *persoană din interior* este cineva care este familiarizat cu procedurile și operațiunile organizației, are prieteni în interiorul grupului, având totodată acces la resursele și sistemele oferite de această organizație.

Ceea ce face ca persoanele din interior să fie și mai periculoase este că ele sunt greu de detectat. Un străin este ușor observat atunci când încearcă să treacă una din barierele dintre organizație și lumea exterioară, lucru pe care un membru al organizației nu are nevoie să îl facă.

Sistemele de calcul sunt în general protejate la accesul persoanelor neautorizate. Există mai multe mecanisme de autentificare și apoi autorizare a utilizatorilor autorizați, însă cel mai răspândit este cel bazat pe nume de utilizator și parolă (*username* și *password*). Un utilizator primește un nume și o parolă pe care le folosește atunci când vrea să acceseze un serviciu sau un calculator.

Perechea *nume de utilizator / parolă* are pentru sistemele informatice rolul pe încuietoarea ușii îl are în ceea ce privește protejarea unei camere la intrarea străinilor. Încuietoarea este considerată drept un mijloc sigur de protecție, însă în realitate, există persoane capabile, pentru care aceasta nu constituie o problemă atunci când doresc accesul în încăpere. Același lucru este din păcate valabil și pentru lumea calculatoarelor.

Un aspect special referitor la criminalitatea informatică este reprezentat de făptuitorii acestor tipuri de infracțiuni. Problema realizării unui "portret robot" al celor care încalcă legea înfăptuind infracțiuni de natură informatică este foarte actuală în cercetările criminologice la scară mondială. Cu toate acestea realizarea profilului autorilor poate fi subiectul influenței unor clișee existente în mass-media. Unanimitatea autorilor consideră că infracțiunile comise prin sistemelor informatice se încadrează în tipul "criminalității gulerelor albe". Un profil "clasic" al făptuitorilor acestor infracțiuni poate fi rezumat astfel: bărbat cu vârsta cuprinsă între 15 și 45 de ani, având un statut social bun, fără antecedente penale, inteligent și motivat. În multe cazuri, autorul este chiar salariat al întreprinderii atacate, sau cunoaște modul de funcționare a sistemului atacat.

Au fost numeroase încercări de realizare a unei tipologii a făptuitorilor, clasificarea acestora mergând de la două categorii la nu mai puțin de 26. Criteriile de delimitare a acestor tipologii sunt în principal două: motivațiile autorilor, precum și consecințele legale ale acestora. Cel de-al doilea criteriu introduce o distincție între acțiunile care au scop fie producerea de pagube, fie un folos necuvenit, și acțiunile justificate de curiozitate, sau explicate de motive pedagogice. Această distincție ar legitima astfel acțiunile de tip "hacking", fapt inacceptabil.

Revenind la primul criteriu de distincție, autorii au delimitat mai multe tipuri de motivații. Astfel, *Direction de Surveillance de Territoire* din Franța propune distincția între

amenințările ludice (hackeri, etc.), cele averse (câștig financiar, etc.), și cele strategice (spionaj, etc.). Trei autori americani propun o analiză mai complexă, bazată pe determinanțele conduitei criminale, acestea implicând elemente motivaționale (având caracteristici personale – motive economice, ideologice, egocentrice sau psihotice), elemente de oportunitate (reprezentând caracteristici ale mediului – acces în grupări criminale, recompense sociale, etică diferită, încredere în grup), mijloace și metode.

John D. Howard propune următoarele șase categorii de autori:

- *hackeri* - persoane, mai ales tineri, care pătrund în sistemele informatice din motivații legate mai ales de provocare intelectuală, sau de obținerea și menținerea unui anumit statut în comunitatea prietenilor;
- *spioni* - persoane ce pătrund în sistemele informatice pentru a obține informații care să le permită câștiguri de natură politică;
- *teroriști* - persoane ce pătrund în sistemele informatice cu scopul de a produce teamă, în scopuri politice;
- *atacatori cu scop economic* - pătrund în sistemele informatice ale concurenței, cu scopul obținerii de câștiguri financiare;
- *criminali de profesie* - pătrund în sistemele informatice ale întreprinderilor pentru a obține câștig financiar, în interes personal;
- *vandali* - persoane ce pătrund în sistemele informatice cu scopul de a produce pagube.

O altă prezentare identifică 5 categorii de intruși, fiecare cu diferite aptitudini, niveluri de cunoștințe, dar mai ales cu obiective diferite. Toate aceste categorii pot proveni atât din exteriorul cât și din interiorul companiei.

- **Novicele** este de obicei un începător singuratic. Nu are experiență în calculatoare și nici cum să pătrundă în sisteme din afară. Novicele lucrează singur și nu are ajutor din afară, fiind în cele mai multe ori un experimentator care nu comite ilegalități. Este destul de ușor de depistat deoarece nu este capabil să își șteargă urmele; ceea ce este greu este ca el să fie considerat o amenințare. Rezultatele „muncii” acestuia pot fi găsite de regulă în câteva locații:

1. fișiere cu parole;
2. fișiere de configurare pentru utilizatori;
3. fișiere de configurare ale sistemului.

Cea mai bună metodă de a combate novicele este educarea utilizatorilor, deoarece novicele profită de lipsurile în administrarea parolilor. Aproape 80% din totalul intrărilor neautorizate pe sisteme se întâmplă în acest fel.

- **Ucenicul** este acel novice care progresează dincolo de fazele inițiale, în general cu ajutorul IRC, schimbând mesaje cu cei care i se aseamănă. Nu numai că își îmbunătățește foarte mult cunoștințele, dar devine parte a unei rețele. Membri mai avansați sunt bucuroși să își împărtășească experiența, iar novicele devin ucenici. Ei învață să își acopere mai bine urmele și să intre sau să iasă din sisteme fără să atragă atenția. Și, deși nu cunosc încă modalitățile de funcționare ale sistemelor de securitate, au învățat însă cum să procedeze astfel încât să nu lase urme. „Ucenicii” de cele mai multe ori reușesc să treacă de protecția prin parolă a sistemelor și știu câte ceva și despre alte sisteme de securitate, ceea ce îi face ceva mai greu de prins.

- **Vizitatorul** este probabil cel mai „inocent” dintre atacatori. Aceste persoane sunt simpli trecători curioși. Rareori se întâmplă ca ei să compromită sistemele, în afara cazului în care întâlnesc o oportunitate serioasă. Dacă un vizitator va găsi un obstacol, de cele mai multe ori se va retrage, căutând alt sistem unde accesul este mai ușor. O excepție la această regulă, foarte rară, este situația în care vizitatorul observă un lucru interesant și este dispus să își mai petreacă ceva timp pentru a îl putea studia.
- **Amatorul avansat** sau altfel spus, semi-profesionistul, spre deosebire de vizitator, capabil, este greu de detectat și de cele mai multe ori cu o dorință specială de a face rău. Pentru mulți din această categorie scopul principal este să vadă cât de mult pot distruge. În general ei folosesc greșeli de programare a sistemului de operare pentru a ocoli mecanismele de autentificare și a primi acces neautorizat la sistem.
- **Profesionistul** este diferit de toate celelalte categorii de intruși: o persoană bine antrenată, un spion profesionist al calculatoarelor. Aceste persoane se pricep foarte bine să intre într-un sistem de calcul (server, PC, router, etc.) și să îl părăsească fără să fie observați în vreun fel. Ei alterează sau ocolesc aplicațiile de jurnalizare a activităților la fel de ușor cum pot compromite orice parte a sistemului. Cea mai bună apărare față de acești atacatori este evitarea legării în rețea a sistemelor care conțin informații importante și controlul strict al accesului fizic la acestea.

Clasificarea riscurilor și incidentelor

Clasificările se pot face după mai multe criterii. Vom analiza câteva dintre acestea:

Clasificarea ca listă de termeni

O clasificare populară dar simplistă este o listă de termeni definiți. Un exemplu este următorul:

- Interceptarea cablurilor și a semnalelor emise (*Wiretapping, Eavesdropping on Emanations*);
- Căutarea prin fișierele șterse (*Dumpster diving*);
- Refuzarea serviciului (*Denial-of-service*);
- Hărțuire (*Harassment*);
- Mascare (*Masquerading*);
- Pirateria software (*Software piracy*);
- Copierea neautorizată de date (*Unauthorized data copying*);
- Degradarea serviciului (*Degradation of service*);
- Analiza traficului (*Traffic analysis*);
- Uși ascunse (*Trap doors*);
- Canale ascunse (*Covert channels*);
- Viruși și viermi (*Viruses and worms*);
- Deturnarea sesiunii (*Session hijacking*);

- Atacuri temporale (*Timing attacks*);
- Forare (*Tunneling*);
- Cal troian (*Trojan horses*);
- Simulare IP (*IP spoofing*);
- Bombe logice (*Logic bombs*);
- Distrugerea datelor (*Data diddling*);
- Tehnica tăierii salamului (*Salamis*);
- Interceptarea parolelor (*Password sniffing*);
- Privilegii excesive (*Excess privileges*);
- Scanare (*Scanning*).

Listele de termeni în general nu îndeplinesc cele 6 caracteristici ale unei clasificări satisfăcătoare.

În primul rând, termenii tind să nu fie mutual exclusivi. De exemplu, termenii virus și bombă logică sunt în general găsiți în aceste liste, dar un virus poate conține o bombă logică, deci categoriile se suprapun.

Atacatorii adevărați utilizează de asemenea mai multe metode. Ca rezultat, dezvoltarea unei liste complete de metode de atac nu furnizează o schemă bună de clasificare.

Listă de categorii

O variație a unei singure liste de termeni cu definiții este o listă de categorii. Există o împărțire în șapte categorii:

1. Furtul de parole – metode de a obține parolele altor utilizatori;
2. Inginerie socială – convingerea persoanelor să divulge informații confidențiale;
3. Greșeli de programare și porțițe lăsate special în programe – obținerea de avantaje de la sistemele care nu respectă specificațiile sau înlocuire de software cu versiuni compromise;
4. Defecte ale autentificării – înfrângerea mecanismelor utilizate pentru autentificare;
5. Defecte ale protocoalelor – protocoalele sunt impropriu proiectate sau implementate;
6. Scurgere de informații – utilizarea de sisteme ca DNS pentru a obține informații care sunt necesare administratorilor și bunei funcționări a rețelei, dar care pot fi folosite și de atacatori;
7. Refuzul serviciului – încercarea de a opri utilizatorii de a utiliza sistemele lor.

Categorii de rezultate

O altă variație a unei liste de termeni este gruparea tuturor atacurilor în categorii de bază ce descriu rezultatele. Un exemplu este alterarea, scurgerea de informații și refuzul serviciului, unde alterarea este modificarea neautorizată a unor informații, scurgerea este atunci când informația ajunge în locuri nepotrivite, iar refuzul serviciului reprezintă indisponibilitatea de a utiliza rețelele și calculatoarele.

Se mai folosesc categorii similare, dar cu termeni opuși:

1. discreție și confidențialitate;
2. acuratețe, integritate și autenticitate;
3. disponibilitate.

Cu excepția intrușilor care vor doar să crească accesul la un computer sau la o rețea, sau intrușilor care utilizează computerul sau resursele rețelei fără însă a degrada serviciul celorlalți (furt de resurse), multe atacuri individuale pot fi asociate în mod unic cu una dintre aceste categorii. Totuși plasarea tuturor atacurilor și incidentelor în doar câteva categorii este o clasificare care furnizează informații și înțelegere limitate.

Liste empirice

O variație de categorii de rezultate teoretice (*a priori*) este dezvoltarea unei liste de categorii mai lungă bazată pe o clasificare de date empirice.

- Furtul de informații externe (privitul peste umăr la monitorul altei persoane);
- Abuzul extern al resurselor (distrugerea unui *hard disk*);
- Mascarea (înregistrarea și redarea ulterioară a transmisiunilor de pe o rețea);
- Programe dăunătoare (instalarea unui program cu scopuri distructive);
- Evitarea autentificării sau autorizării (spargerea parolilor);
- Abuz de autoritate (falsificări de înregistrări);
- Abuz intenționat (administrare proastă intenționată);
- Abuz indirect (utilizarea unui alt sistem pentru a crea un program rău intenționat).

Clasificări bazate pe acțiuni – modelul este focalizat doar pe informația în tranzit și prezintă 4 categorii de atacuri:

- Întreruperea – un bun al sistemului este distrus sau devine neutilizabil sau nedisponibil;
- Interceptarea – o parte neautorizată obține accesul la un bun al sistemului;
- Modificarea – o parte neautorizată nu numai că obține acces, dar îl și modifică;
- Falsificarea – o parte neautorizată inserează obiecte contrafăcute în sistem.

Evenimente, atacuri și incidente

Trei concepte de bază ale securității, importante în ceea ce privește informațiile de pe Internet, sunt *confidențialitatea*, *integritatea* și *disponibilitatea*. Conceptele legate de oamenii care utilizează aceste informații sunt autentificarea, autorizarea și acceptarea.

Când informația este citită și copiată de cineva neautorizat, rezultatul este cunoscut ca pierderea *confidențialității*. Pentru câteva tipuri de informații, confidențialitatea este un atribut foarte important.

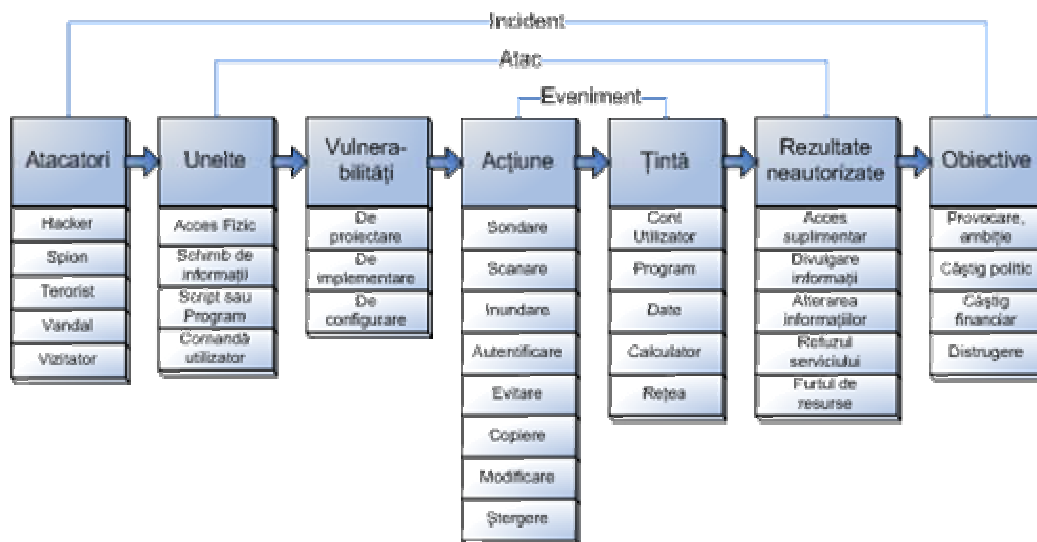
Exemplele includ date obținute din cercetare, înregistrări medicale și de asigurări, specificații ale noilor produse și strategii de investiții corporatiste. În unele locuri, s-ar

putea să existe o obligație legală pentru protecția intimității persoanelor. Aceasta este adevărată pentru bănci și companii de credit, spitale, cabinete medicale, laboratoare de testare medicală, cabinete psihologice și agenții care colectează taxe.

Informația poate fi alterată când este disponibilă pe o rețea nesigură. Când informația este modificată în moduri neașteptate, rezultatul e cunoscut drept pierderea *integrității*. Aceasta înseamnă că datele suferă modificări neautorizate fie ca urmare a unei greșeli umane fie prin modificare intenționată. Integritatea este importantă în mod particular pentru siguranța critică și datele financiare utilizate în activități ca transferuri electronice de fonduri, controlul traficului aerian și contabilitate financiară.

Informația poate fi ștearsă sau poate deveni inaccesibilă, rezultând o *lipsă de disponibilitate*. Aceasta înseamnă că persoanele care sunt autorizate să obțină informații nu pot obține ceea ce doresc.

Disponibilitatea este deseori cel mai important atribut în afacerile orientate pe servicii care depind de informații (programări aeriene și sisteme de inventar on-line). Disponibilitatea rețelei e importantă pentru orice persoană a cărei afacere sau educație depinde de o conectare la rețea. Când un utilizator nu poate accesa rețeaua sau un serviciu specific furnizat pe rețea, el experimentează un refuz al serviciului.



Evenimente

Operarea calculatoarelor și a rețelelor se compune dintr-un șir de *evenimente*. Un eveniment reprezintă schimbarea stării unui sistem sau dispozitiv. Din punctul de vedere al securității informatice, aceste schimbări de stare apar ca urmare a unor *acțiuni* care sunt îndreptate asupra unor *ținte*. Un exemplu de acțiune este de a accesa un sistem de calcul. În acest caz, acțiunea este *autentificarea* de către programul de control a accesului utilizatorului, conform unei identități controlate de nume de utilizator și parolă.

Definim deci:

- **evenimentul**, din punctul de vedere al unui calculator sau al unei rețele de calculatoare ca fiind o acțiune realizată asupra unui sistem țintă prin care se intenționează schimbarea stării sistemului;
- **acțiunea** ca fiind un demers al unui utilizator sau program, cu scopul de a obține un rezultat;

- **ținta** ca fiind o entitate logică a unei rețele sau sistem de calcul (cont de utilizator, program sau date) sau o entitate fizică (PC, rețea).

Acțiuni

- *Sondare (probe)* – accesarea unei ținte cu scopul de a îi determina caracteristicile
- *Scanare (scan)* – accesarea secvențială a unei mulțimi de ținte pentru a determina care dintre ele are o anumită caracteristică
- *Inundare (flood)* – accesarea unei ținte în mod repetat, cu scopul de a o supraîncărca și a produce inaccesibilitatea serviciului pe perioada inundării, serviciul fiind ocupat exclusiv cu răspunsurile la toate cererile venite în avalanșă de la expeditorul inundației
- *Autentificare (authenticate)* – prezentarea identității cuiva unui program și, dacă este nevoie, verificarea acestei identități, cu scopul de a primi acces pe sistemul țintă
- *Evitare (bypass)* – evitarea unui proces sau program folosind o metoda alternativă de a accesa ținta.
- *Simulare (spoof)* – acțiunea de a falsifica caracteristicile unui sistem sau program pentru a imita o altă entitate din rețea.
- *Citire (read)* – obținerea conținutului unui mediu de date
- *Copiere (copy)* – reproducerea ținte fără a o modifica
- *Furt (steal)* – preluarea posesiei unei ținte, fără a păstra o copie în locația originală
- *Modificare (modify)* – schimbarea conținutului sau caracteristicilor ținte
- *Ștergere (delete)* – înlăturarea ținte sau distrugerea capacităților sale

Ținte

- *Cont (account)* – domeniul de acces al utilizatorului pe un calculator sau pe o rețea, care este controlat conform unor înregistrări care conțin numele acestui cont, parola și drepturile în acest domeniu.
- *Proces (process)* – un program în execuție, constând din instrucțiunile programului, datele care sunt prelucrate de acest program
- *Dată (data)* – reprezentarea de fapte, concepte sau instrucțiuni într-o modalitate potrivită pentru comunicare, interpretare sau procesare de către oameni sau mașini automate. Datele pot fi sub formă de fișiere în memoria unui calculator, pe discul acestuia sau pot avea forma de date de tranzit printr-un mediu de transmisie.
- *Componentă (component)* – una din părțile care formează un calculator sau o rețea.
- *Calculator (computer)* – un dispozitiv care constă din una sau mai multe componente asociate, incluzând unități de procesare și periferice și care este controlat de programe stocate intern.
- *Rețea (network)* – un grup interconectat de calculatoare, echipamente de comutare și ramuri de interconectare.
- *Internet (internetwork)* – o rețea de rețele.

Atacuri

Câteodată, un eveniment care are loc pe un computer sau o rețea este parte a unei serii de pași ce intenționează să producă un eveniment neautorizat. Acest eveniment este apoi considerat ca parte a unui *atac*. Un atac are mai multe elemente. În primul rând, e format din mai mulți pași pe care atacatorul îi face. Printre acești pași regăsim o *acțiune* îndreptată către o *țintă*, cât și utilizarea unei *unelte* pentru a *exploata o vulnerabilitate*. În al doilea rând, un atac intenționează să obțină un *rezultat neautorizat*, privit din perspectiva utilizatorului sau administratorului sistemului în cauză. În final, un atac reprezintă o serie de etape voluntare pe care atacatorul le realizează, acest lucru diferențiind un atac de o secvență de acțiuni normale.

Atacurile au 5 părți care reprezintă pașii logici pe care un atacator trebuie să îi facă. Atacatorul utilizează o unealtă pentru a exploata o vulnerabilitate în scopul obținerii unui rezultat neautorizat. Pentru a avea succes, un atacator trebuie să găsească căi care pot fi conectate, simultan sau repetat. Primii doi pași într-un atac, unealta și vulnerabilitatea, sunt folosite pentru a cauza un eveniment pe un computer sau o rețea. Mai specific, în timpul unui atac individual, atacatorul folosește o unealtă pentru a exploata o vulnerabilitate care cauzează o acțiune în atingerea unui scop. Sfârșitul logic al unui atac de succes este un rezultat neautorizat. Dacă sfârșitul logic al pașilor anteriori este un rezultat autorizat, atunci atacul practic nu a avut loc.

Conceptul de *autorizat* contra *neautorizat* este cheia pentru a înțelege ce diferențiază un atac de evenimente normale care au loc.

- *Autorizat* – aprobate de utilizator sau administrator.
- *Neautorizat* – care nu sunt aprobate de utilizator sau administrator.

Unelte

Unealta este o modalitate de a exploata vulnerabilitatea unui computer sau a unei rețele.

Categoriile de unelte folosite sunt următoarele:

- *Atac fizic (physical attack)* – o modalitate de a sustrage sau distruge un calculator, o rețea, componentele acestora sau sistemele de susținere (aer condiționat, electricitate, etc.)
- *Schimbul de informații (information exchange)* – o modalitate de a obține informații fie de la alți atacatori (spre exemplu prin IRC), fie de la oamenii care sunt atacați (inginerie socială)
- *Comandă a utilizatorului (user command)* – modalitate de a exploata o slăbiciune prin introducerea de comenzi într-un program.
- *Script sau program (script or program)* – exploatare a vulnerabilităților prin execuția unui fișier de comenzi (script) sau a unui program.
- *Agent independent (autonomous agent)* – folosirea unui program sau a unui fragment de program care operează independent de utilizator, exemple fiind virușii și viermii de rețea.
 - *Virușii* sunt mici fragmente de programe de calculator care se auto-replică sau înserează copii ale codului propriu în alte programe, atunci când este rulată o aplicație infectată. Un tip diferit de virus este „viermele” (*worm*) care nu infectează fișierele de pe disc, ci se răspândește cu ajutorul rețelei.

- *Troienii* sunt tot fragmente de programe însă nu au capacitatea de auto-replicare, fiind inserați în programe normale. Atunci când utilizatorul execută aceste programe, execută neintenționat și fragmentul de cod de tip „cal troian”, aproape întotdeauna efectele fiind negative.
- *Programe integrate (toolkit)* – un pachet de programe care conține comenzi, programe sau agenți independenți care exploatează slăbiciunile sistemelor.
- *Unelte distribuite (distributed tools)* – unelte care sunt dispersate pe mai multe calculatoare, care pot fi coordonate pentru a conduce atacuri simultane către aceeași țintă.
- *Interceptor de date (data tap)* – mijloc de a monitoriza radiația electromagnetică emanată de un calculator sau o rețea, folosind un echipament extern

Vulnerabilități

Pentru a obține rezultatele pe care le dorește, un atacator trebuie să se folosească de o vulnerabilitate a calculatorului sau a rețelei, care este definită după cum urmează:

Vulnerabilitatea (vulnerability) este o slăbiciune a sistemului care permite o acțiune neautorizată. Acestea sunt erori care apar în diferite faze ale dezvoltării, respectiv folosirii sistemelor. Acestea pot fi deci clasificate în următoarele categorii:

- *Vulnerabilitate de proiectare (design vulnerability)* – o eroare care apare în prima fază a vieții unui produs, aceea de concepție, și pe care chiar o implementare ulterioară perfectă nu o va înlătura
- *Vulnerabilitate de implementare (implementation vulnerability)* – apare ca urmare a fazei de punere în practică a proiectului.
- *Vulnerabilitate de configurare (configuration vulnerability)* – apare ca urmare a erorilor făcute în configurarea sistemelor, cum ar fi folosirea codurilor de acces implicite sau a drepturilor de scriere a fișierelor cu parole

Rezultate neautorizate

Rezultatul neautorizat este o consecință neautorizată a unui eveniment

- *Acces superior (increased access)* – o creștere neautorizată în accesul pe un computer sau pe o rețea
- *Divulgare de informații (disclosure of information)* – propagarea de informații unor persoane care nu sunt autorizate să aibă acces la acestea
- *Alterarea informației (corruption of information)* – alterare neautorizată de date de pe un computer sau o rețea
- *Refuzul serviciului (denial of service)* – degradare intenționată sau blocarea resurselor sistemului
- *Furt de resurse (theft of resources)* – uz neautorizat al unui computer sau a resurselor unei rețele

Soluțiile de protecție la toate aceste tipuri de probleme nu sunt simple, pentru că de cele mai multe ori trebuie tratate cauzele lor. Se poate realiza un progres important tratând cu

cea mai mare atenție aspectele legate de securitate atât în fazele de proiectare și implementare ale produselor, cât și în cea de utilizare.

O clasificare sintetică a tipurilor de incidente, în paralel cu reglementarea legală a criminalității informatice la nivel internațional este prezentată mai jos, după studiul *Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries* realizat în 2002 de Rand Europe pentru Comisia Europeană.

Incidente	Reglementare în Convenția privind criminalitatea informatică
Obținerea de informații cu privire la o posibilă țintă (sondare, scanare)	ARTICOLUL 6 - Abuzurile asupra dispozitivelor
Compromiterea sistemului prin executarea de cod neautorizat	ARTICOLUL 4 - Afectarea integrității datelor ARTICOLUL 5 - Afectarea integrității sistemului
Refuzul serviciului	ARTICOLUL 5 - Afectarea integrității sistemului
Compromiterea sistemului (furt, modificare, ștergere)	ARTICOLUL 2 - Accesarea ilegală
Încercare de intruziune	ARTICOLUL 2 - Accesarea ilegală, coroborat cu ARTICOLUL 11 - Tentativa și complicitatea
Accesul neautorizat la informații	ARTICOLUL 2 - Accesarea ilegală ARTICOLUL 3 - Interceptarea ilegală
Accesul neautorizat la transmiterea datelor	ARTICOLUL 3 - Interceptarea ilegală
Alterarea informațiilor	ARTICOLUL 4 - Afectarea integrității datelor
Accesul ilegal la sisteme de comunicații	ARTICOLUL 2 - Accesarea ilegală