Security in Computer-Related Systems

Prep. Radu CONSTANTINESCU
Catedra de Informatică Economică, ASE Bucureşti

Computers are an integral part of the economic, social, professional and governmental infrastructures. They have become necessities in virtually every area of modern life, but their vulnerabilities is of increasing concern. Computer-based systems are constantly under threats of inadvertent errors and acts of nature, as well as those attributable to unethical, immoral and criminal activities. This paper resumes the most important concepts of security in computer-related systems.
Keywords: *security, vulnerabilities, threats, risk, assets, controls.*

Introducere

Un sistem informatic este determinat de trei componente de bază: echipamente hardware, programe şi date. Fiecare din aceste active este important pentru buna funcţionare a sistemului. Pentru a le putea asigura securitatea trebuie făcută o analiză asupra modalităţilor în care sistemul poate fi afectat de diferite evenimente. O vulnerabilitate este o slăbiciune a sistemului de securitate care poate fi speculată în sensul determinării unor efecte negative. De exemplu, un sistem poate fi vulnerabil la nivelul datelor din cauză că nu verifică identitatea utilizatorului înainte de a-i acorda accesul. O ameninţare reprezintă o serie de circumstanţe care au potenţialul să cauzeze pagube. Pentru sistemele informatice există ameninţări ce au ca factor iniţiator o persoană sau un calculator. De asemenea există ameninţări naturale cum ar fi inundaţiile, incendiile sau cutremurele. Pentru a proteja sistemul de posibilele efecte negative se folosesc o serie de măsuri de control. Acestea pot fi reprezentate de anumite activităţi, dispozitive, proceduri sau metode ce elimină sau reduc vulnerabilităţile. Sintetizând, o ameninţare este blocată prin măsuri de control al vulnerabilităţilor. Ameninţările se pot clasifica în patru categorii:

- *interceptarea:* semnifică faptul că o entitate neautorizată poate accesa o anumită componentă a sistemului. Entitatea poate fi o persoană, un program sau un sistem de calcul. Un exemplu poate fi copierea neautorizată a unui program sau a unor date;
- *întreruperea:* semnifică faptul că un activ din sistem este pierdut, indisponibil sau neutilizabil. Exemple pot fi: distrugerea intenţionată a unui dispozitiv hardware, ştergerea unui program sau a unor date şi funcţionarea greşită a unei componente a sistemului de operare;
- *modificarea:* are loc atunci când un activ nu este numai accesat în mod neautorizat ci sunt făcute şi schimbări la nivelul său. Exemple pot fi: schimbarea unor valori din baza de date, modificarea unui program pentru a executa şi alte operaţii, modificarea datelor în momentul transmiterii electronice sau modificarea componentelor hardware;
- *falsificarea:* contrafacerea sau reproducerea unor obiecte dintr-un sistem informatic. De exemplu, un intrus poate adăuga tranzacţii false în cadrul unui proces de comunicare în reţea sau poate adăuga noi înregistrări în baza de date.

Principiile securităţii informatice

Pentru asigurarea securităţii informaţiei trebuie cunoscute principiile de bază care guvernează domeniul. Acestea sunt principiul penetrării facile, principiul protecţiei adecvate, principiul eficacităţii şi principiul verigii slabe.

Principiul penetrării facile stipulează că un intrus poate folosi orice metodă pentru a pătrunde în sistem. Penetrarea nu va fi făcută neapărat prin metodele cele mai clare şi nici prin cele pentru care s-au luat cele mai semnificative măsuri de protecţie. În aceste condiţii, specialiştii in securitatea informatică trebuie să ia în considerare toate variantele

posibile de penetrare în sistem. Analiza acestora trebuie făcută în mod repetat şi obligatoriu atunci când se schimbă coordonatele sistemului. Întărirea unei anumite părţi a sistemului poate determina simplificarea pătrunderii în sistem prin alte variante.
Principiul protecţiei adecvate specifică faptul că activele informatice trebuie protejate până în momentul în care îşi pierd valoarea, iar protecţia trebuie să fie direct proporţională cu valoarea lor.
Principiul eficacităţii stipulează faptul că măsurile de control trebuie să fie utilizate într-un mod corect pentru a putea avea efecte. Măsurile de control trebuie să fie eficiente, adecvate şi uşor de folosit. Eficienţa poate fi măsurată în timp, spaţiu de memorie, activitate depusă sau efecte asupra celorlalte elemente din sistem.
Principiul verigii slabe specifică faptul că securitatea unui sistem nu poate fi superioară securităţii subsistemului cel mai expus. Funcţionarea defectuoasă a unei componente generează automat expunerea întregului sistem.

Obiectivele securităţii sistemelor informatice

Securitatea sistemelor informatice presupune îndeplinirea a trei deziderate: confidenţialitatea, integritatea şi disponibilitatea.
Asigurarea confidenţialităţii presupune că activele informatice sunt accesate numai de către persoane autorizate. Prin acces se înţelege nu numai citirea ci şi vizualizarea, listarea sau chiar cunoaşterea existenţei unui anume activ. Pentru a putea avea un nivel satisfăcător de confidenţialitate trebuie să existe o entitate sau un responsabil care să stabilească cine are drept de acces la sistem şi în ce măsură este permis accesul fiecăruia.
Asigurarea integrităţii semnifică faptul că activele pot fi modificate numai de către persoane autorizate sau numai prin metode autorizate. Prin modificare putem înţelege operaţiuni precum scrierea, crearea, ştergerea sau schimbarea stării curente. Datorită variatelor înţelesuri ale acestui concept, păstrarea integrităţii unui activ poate însemna faptul că respectivul este: precis, exact, nemodificat, modificat într-o măsură acceptabilă, modificat de către persoane autorizate, modificat de către procese autorizate, consistent sau utilizabil. Au fost identificate trei elemente esenţiale pentru asigurarea integrităţii: derularea de acţiuni autorizate, separarea şi protejarea resurselor precum şi detectarea şi corectarea erorilor. Integritatea poate fi implementată în mod similar cu confidenţialitatea, printr-un control riguros al persoanelor care pot accesa anumite resurse şi asupra modului în care resursele pot fi accesate.
Asigurarea disponibilităţii implică faptul că un activ este disponibil persoanelor autorizate în timpii optimi caracteristici. Cu alte cuvinte, dacă o persoană sau un sistem dispun de acces autorizat la anumite resurse, accesul trebuie să nu fie restricţionat. O stare inversă este cea de "denial of service", adică de incapacitatea de a asigura serviciul. Disponibilitatea poate fi asigurată atât la nivelul datelor cât şi la nivelul serviciilor. Ca şi în cazul confidenţialităţii diferite persoane pot avea abordări distincte. De exemplu un obiect sau un serviciu poate fi considerat disponibil dacă este prezent într-o formă utilizabilă, are o capacitate suficientă pentru a satisface necesităţile sau operaţiunea este încheiată într-o perioadă de timp acceptabilă.

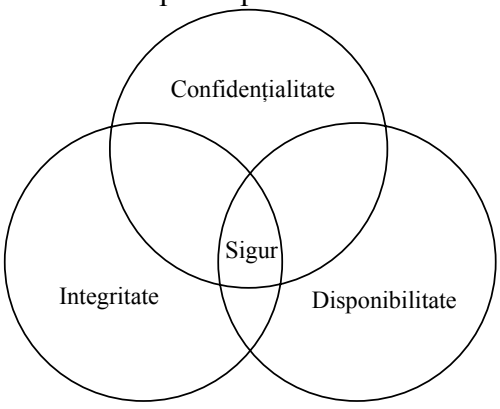

Fig. 1 Relaţia între confidenţialitate, integritate şi disponibilitate

Securitatea informatică presupune îndeplinirea celor trei obiective specificate, aşa cum este prezentat şi în figura 1. O provocare pentru construirea unui sistem securizat este atingerea unei stări de echilibru între cele trei obiective care de multe ori generează situaţii conflictuale la nivelul sistemului. De exemplu, este uşor să se asigure confidenţialitatea

informațiilor din sistem prin simpla blocare totală a accesului la resursele respective. Totuşi, în aceste condiții sistemul nu este securizat deoarece nu îndeplineşte condiția de asigurare a disponibilității. În condițiile descrise trebuie să existe un echilibru între confidențialitate şi disponibilitate.

Vulnerabilități

În momentul în care se doreşte testarea unui sistem se încearcă să se imagineze modalitățile în care acesta eşuează şi care sunt elementele care determină acest lucru. În acelaşi fel, atunci când se defineşte, se descrie, se implementează sau se testează un sistem trebuie identificate vulnerabilitățile care pot împiedica obținerea celor trei deziderate de securitate. Pentru identificarea acestora este indicată varianta abordării pe categorii de active: hardware, software şi date. Elementele din aceste trei categorii şi conexiunile dintre ele reprezintă potențiale puncte slabe de securitate.

Componentele hardware sunt mai uşor de identificat decât cele software şi asta în primul rând datorită tangibilității lor. Identificând dispozitivele ce compun un sistem este relativ simplu să se atace prin adăugarea, modificarea, sau înlocuirea dispozitivelor, interceptarea traficului sau inundarea cu informații redundante.

Pe lângă aceste probleme mai există şi cele determinate de factorii din natură (apă, foc, gaze, rozătoare, praf etc.) sau de curentul electric. De asemenea, fumatul şi consumul de băutură sau mâncare în proximitatea echipamentelor pot determina disfuncționalități. Aceste abuzuri sunt în mare parte neintenționate şi de regulă determină pagube reduse. Atacurile intenționate, cum ar fi cele prin explozibili şi alte mijloace de distrugere, şi furtul constituie probleme mult mai grave din punct de vedere al securității. În această categorie amintim atacurile deliberate cu intenția de a limita disponibilitatea. De multe ori, pentru a asigura o securitate sporită a dispozitivelor hardware pot fi folosite metode standard cum ar fi încuietorile sau personalul de pază.

Echipamentul de calcul este inutil fără instrumentele software adecvate. Dintre acestea amintim: sistemul de operare, programele utilitare şi programele de aplicații. Software-ul poate fi înlocuit, schimbat sau distrus în mod voit sau poate fi modificat, şters sau instalat într-un mod defectuos. Cu sau fără caracterul intențional, aceste atacuri exploatează vulnerabilitățile software-ului.

În unele cazuri atacurile sunt evidente, cum ar fi atunci când programele nu mai rulează. Există şi atacuri mai subtile atunci când programele par că rulează în parametri normali cu toate că sunt modificate. Modificarea este mai greu de observat față de cazul dispozitivelor fizice.

Software-ul este foarte uşor de şters. Majoritatea celor ce au lucrat cu calculatorul au şters la un moment dat în mod accidental un fişier sau au salvat o copie stricată peste varianta bună a unui program. Datorită valorii mari a software-ului, în centrele de calcul accesul este controlat prin procesul de management al configurării pentru a putea preveni accidentele. Astfel, versiunea veche este înlocuită cu una mai nouă doar în momentul în care aceasta a fost testată şi verificată asupra faptului că îmbunătățirile aduse determină efectele corecte fără să degradeze funcționalitatea şi performanțele celorlalte servicii şi funcții.

Software-ul este vulnerabil la modificări care pot determina eşuarea sau efectuarea unor sarcini nedorite. Simpla modificare a unui bit poate determina transformarea unei aplicații funcționale în una nefuncțională. Efectele pot fi instantanee sau pot apărea după un anumit număr de rulări. Există şi situația în care produsul funcționează normal însă în anumite condiții poate genera o serie de efecte negative. Acest tip de program poartă denumirea de bombă logică. De exemplu, un angajat poate modifica o aplicație astfel încât aceasta să nu se mai execute corect începând cu o dată la care acesta va mai lucra în firma respectivă. O altă variantă de modificare este cea care extinde funcționalitatea unui program astfel încât o lucrare inițial inofensivă să determine efecte ascunse. De exemplu, un program care gestionează un sistem de fişiere poate fi configurat să modifice în mod neautorizat drep-

turile de acces la acestea.
Dintre celelalte categorii de modificări software amintim:

- calul troian: este un program care execută la vedere o serie de lucrări acceptate şi în acelaşi timp execută şi o serie de lucrări neautorizate;
- virus: este o aplicaţie ce are efecte negative asupra sistemului şi care se poate răspândi de la o staţie de lucru la alta;
- backdoor: este o aplicaţie ce deschide căi de comunicaţie neautorizate cu exteriorul;
- scurgeri de informaţii în program: reprezintă o secvenţă de cod dintr-un program care determină ca anumite informaţii să fie disponibile altor persoane sau programe neautorizate.

O altă vulnerabilitate a aplicaţiilor software este furtul. Acesta poate fi făcut prin copierea neautorizată a aplicaţiei. Dezvoltatorii şi distribuitorii aplicaţiilor software beneficiază de prevederile dreptului de autor similar cu muzicienii sau scriitorii. Se înregistrează dificultăţi mari în procesul de adaptare a legislaţiei în vigoare pentru datele electronice.
Datorită multiplelor forme de reprezentare, atacurile asupra datelor sunt mult mai răspândite şi determină efecte mai mari decât în cazul atacurilor asupra echipamentelor hardware sau asupra software-ului. Datele au o valoare publică mai mare deoarece majoritatea oamenilor le pot interpreta sau folosi.
Extrase din context, fragmentele de date ca atare nu au o valoare intrinsecă semnificativă. De exemplu numărul "121" nu are nici o relevanţă atâta vreme cât nu se ştie ce reprezintă. Din această cauză este dificil de măsurat valoarea unei date.
Pe de altă parte, datele sunt legate de costuri, măsurabile de exemplu ca şi efort financiar necesar pentru reconstruirea sau redezvoltarea unor date alterate sau pierdute. De exemplu, date confidenţiale ajunse în mâna unei firme concurente pot determina pierderi semnificative. Datele modificate incorect pot genera pierderi de vieţi omeneşti cum ar fi, de exemplu, greşirea coordonatele de zbor pentru un avion. În plus, datele confidenţiale făcute publice pot determina solicitarea de despăgubiri prin răspunderea purtată.
Activele hardware şi software au de obicei o durată de viaţă îndelungată. În mod normal, valoarea acestora descreşte gradual în timp. În contrast cu acest lucru, valoarea datelor pe axa timpului este greu de anticipat. Există categorii de date care au valoare mare pe moment şi apoi se depreciază într-un interval scurt de timp. Un exemplu în acest sens ar fi datele cu fluctuaţiile probabile ale unor valori mobiliare. Acestea pot fi valabile pentru un interval de 24 de ore. Pentru a putea fi asigurată securitatea acestor date trebuie găsit un mecanism de protecţie a cărui spargere să dureze cel puţin 24 de ore. Situaţia descrisă cade sub incidenţa principiului protecţiei adecvate specificat la începutul capitolului.
Datele pot fi colectate printr-o varietate de mijloace, cum ar fi: bandă audio, microfoane, căutatul prin gunoi, monitorizarea emisiilor electromagnetice, interogarea unor angajaţi cheie, deducere sau prin simpla solicitare. Deoarece de multe ori datele se regăsesc într-o formă inteligibilă, asigurarea confidenţialităţii datelor este o problemă majoră în securitatea informatică.
Furtul, achiziţionarea sau interceptarea unor date nu necesită metode foarte sofisticate. Modificarea sau generarea unor noi date necesită un nivel de înţelegere a tehnologiei prin care datele sunt transmise sau stocate precum şi a formatului în care sunt păstrate. Datele sunt vulnerabile la modificări. Modificarea într-un mod discret şi într-o măsură redusă a datelor este greu de identificat prin metode standard. Reprocesarea datelor este un proces şi mai complicat. De exemplu, un falsificator poate intercepta un mesaj constând într-un ordin dat unei bănci pentru creditarea unui cont personal. Falsificatorul poate retransmite mesajul şi să cauzeze astfel o dublă creditare. De asemenea poate fi modificat contul în care să fie viraţi banii sau suma ce va fi transferată.
Dintre celelalte tipuri de active expuse problemelor de securitate ale sistemelor informatice amintim: reţeaua de calculatoare, mecanismele de acces, personalul. Reţelele de calculatoare reprezintă colecţii specializate de hardware, software şi date. Fiecare nod al reţelei este un sistem de calcul care poate în-

registra problemele discutate anterior. În plus, o rețea se confruntă cu probleme de comunicație deoarece are loc interacțiunea dintre componente ale sistemului şi resurse exterioare. O rețea poate multiplica problemele de securitate. Majoritatea problemelor apar datorită lipsei unei delimitări fizice clare, utilizării unor mijloace nesecurizate de acordare a drepturilor de acces la resursele proprii şi imposibilității identificării corecte a utilizatorilor externi.

Accesul la sistemul de calcul poate determina trei tipuri de vulnerabilități. În primul caz, un intrus poate fura timp de calcul pentru lucrări proprii, fără însă a afecta integritatea sistemului ca atare. Această variantă de furt este echivalentă cu furtul de curent electric, apă sau gaz. Accesul neautorizat şi neplătit la resursele de calcul determină costuri suplimentare care vor fi suportate de către utilizatorii autorizați. În cel de-al doilea caz este vorba despre accesul neautorizat la sistem şi în care intrusul distruge componente software sau datele. Cel de-al treilea caz este al unui intrus care prin acțiunile desfăşurate poate bloca serviciile oferite de sistem pentru utilizatorii legitimi.

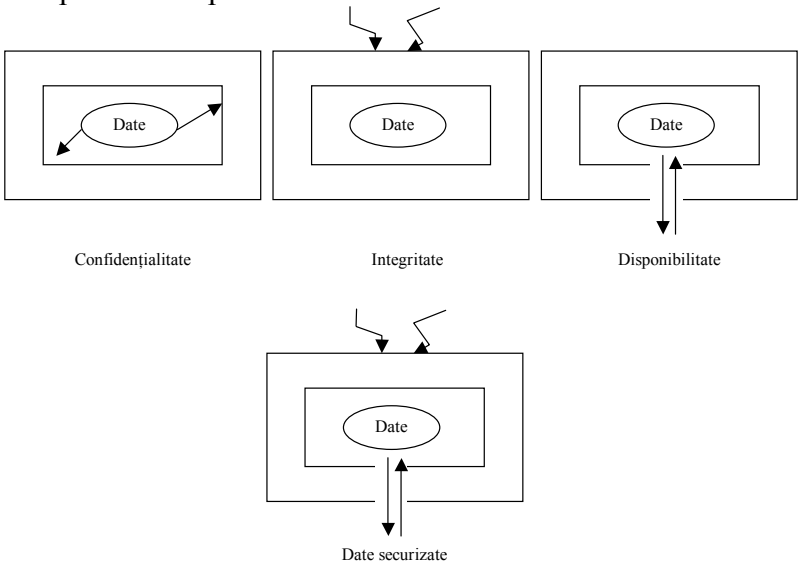

Fig. 2 Modelul securității datelor, Sursa: Charles Pfleeger – *Computer Security*

Oamenii pot fi, de asemenea, puncte slabe pentru securitatea unui sistem. În cazul în care o singură persoană ştie cum să folosească un anume program, pot apărea neplăceri atunci când acea persoană se îmbolnăveşte, suferă un accident sau părăseşte organizația. Un angajat nemulțumit poate cauza pierderi semnificative prin utilizarea cunoştințele sale cu privire la sistem şi la datele folosite. Din aceste motive selectarea angajaților este un proces de mare importanță.

Concluzii

Un atacator este caracterizat prin trei aspecte: metodă, oportunitate şi motiv. Metoda semnifică aptitudinile, cunoştințele, instrumentele şi alte lucruri cu ajutorul cărora poate fi efectuat un atac. Oportunitatea reprezintă timpul şi modalitățile de acces care favorizează atacul. Motivul reprezintă argumentul pentru efectuarea atacului. Eliminarea acestora determină lipsa atacului, însă acest deziderat este de multe ori dificil de atins iar împlinirea lui poate determina apariția altor probleme de securitate. Pentru acest lucru este necesară cunoaşterea vulnerabilităților sistemului precum şi înțelegerea principiilor, obiectivelor şi mecanismelor securității informatice.

Bibliografie

[Bish03] Bishop, M. - *Computer Security Art and Science*, Ed. Addison-Wesley, 2003
[Pfle03] Pfleeger, C. - *Security in Computing,* Ed. Prentice Hall, 2003
[BaKa02] Basworth, S., Kabay, M. - *Computer Security Handbook – 4th Edition*, Ed. John Wiley and Sons, 2002.
[TiKr02] Tipton, H., Krause, M. - *Information Security Management - Handbook 4th edition*, Ed. Auerbach, 2002;
[ISO17799] ISO/IEC 17799 Standard
[BS7799] BS 7799 Standard