Considerații asupra politicii de securitate informatică într-o firmă

Prof.dr.Victor-Valeriu PATRICIU, ing. Silviu PETRESCU
Academia Tehnică Militară, Bucureşti

Securitatea informatică a devenit una din componentele majore în preocuparea conducerii unei firme. Analiştii acestui concept au sesizat o contradicție aparentă între nevoia de comunicații şi conectivitate, pe de o parte şi necesitatea asigurării confidențialității şi autenticității datelor, pe de altă parte. Domeniul relativ nou al securității informatice caută soluții tehnice pentru rezolvarea acestei contradicții. Viteza şi eficiența comunicațiilor "instantanee" de documente şi mesaje conferă numeroase atuuri actului decizional în firme, într-o economie concurențială. Dar, utilizarea serviciilor de poştă electronică, transfer electronic de fonduri etc., se bazează pe un sentiment, adeseori fals, de securitate a comunicațiilor, care poate transforma potențialele câştiguri generate de accesul rapid la informații în pierderi majore, cauzate de furtul de date sau de inserarea de date false ori denaturate.

Cuvinte cheie: *rețele, securitate, informații, comunicație*

Internet este o structură deschisă, la care se poate conecta un număr mare de calculatoare, fiind, deci, greu de controlat. De aceea, putem vorbi de *vulnerabilitatea* rețelelor, manifestată pe variate planuri. Un aspect crucial al rețelelor de calculatoare, în special al comunicațiilor prin Internet, îl constituie *securitatea informațiilor*. Utilizatorii situați la mari distanțe trebuie *identificați* cu precizie, uzual prin parole. Din nefericire, sistemele de parole au devenit vulnerabile, atât datorită "spărgătorilor" de rețea (hackers) care şi-au perfecționat metodele, cât şi datorită alegerii necorespunzătoare a parolelor de către utilizatori. În cazul firmelor, *nevoia de securitate şi de autenticitate apare la toate nivelurile arhitecturale ale rețelelor lor*. De exemplu, utilizatorii vor să se asigure că poşta electronică soseşte chiar de la persoana care pretinde a fi expeditorul. Uneori utilizatorii, mai ales când acționează în numele unor firme, doresc *asigurarea caracterului confidențial* al mesajelor transmise. În tranzacțiile financiare, alături de autenticitate şi confidențialitate, un loc important îl are şi *integritatea mesajelor*, ceea ce înseamnă că mesajul recepționat nu a fost alterat în timpul transmisiei prin rețea. În tranzacțiile de afaceri este foarte important ca, odată recepționată, o comandă să fie nu numai autentică, cu conținut nemodificat, dar să nu existe posibilitatea ca expeditorul să nu o mai recunoască, adică să se respecte *proprietatea de nerepudiere*. Pe de altă parte, la nivel scăzut, porțile (gateways) şi ruterele trebuie să discearnă între calculatoarele autorizate şi cele intruse.

Pentru majoritatea firmelor, interesul în ceea ce priveşte securitatea calculatoarelor este proporțional cu modul în care sunt percepute riscurile şi pericolele. Lumea calculatoarelor s-a modificat dramatic în ultimii ani. Cu aproximativ 25 de ani în urmă, majoritatea calculatoarelor erau centralizate şi administrate în centrele de calcul; ele erau ținute în camere închise şi o echipă întreagă de specialişti avea grijă de securitatea fizică şi de administrarea lor. Legăturile în exterior erau foarte rar întâlnite. Pericolele în ceea ce priveşte securitatea erau rare şi se datorau în majoritate utilizatorilor interni: utilizatori privilegiați care foloseau conturile în mod eronat, furturi, distrugeri de date sau echipamente şi aşa mai departe. Lumea informatică din anii '90 este total diferită. Multe sisteme se află localizate în birouri private sau laboratoare, adesea administrate de către persoane din afara centrului de calcul. Multe dintre sisteme sunt conectate la Internet, şi de aici în toată lumea: Statele Unite, Europa, Asia şi Australia sunt conectate împreună. Din acest motiv, pericolele privind securitatea informatică trebuie privite diferit. Printr-o conexiune Internet, cineva din cealaltă parte a lumii vă poate apela sistemul şi poate

fura fişierul de parole pe timpul nopţii, atunci când întreaga clădire este încuiată. Viruşii, viermii sau caii troieni pot fi transferaţi de la o maşină la alta. Internetul permite acum echivalentul electronic al unui spărgător care caută uşi sau ferestre lăsate deschise: în câteva ore, o persoană rău intenţionată poate căuta vulnerabilităţi în mai multe sute de maşini.
Administratorii de sistem şi factorii de decizie din firme trebuie să înţeleagă pericolele existente în securitatea informatică, care ar fi riscul şi costul unei probleme apărute în acest domeniu precum şi tipul acţiunii pe care ar trebui să o întreprindă.

Moduri de abordare

Configurarea politicilor şi procedurilor de securitate într-o firmă presupune conceperea unui plan. Iată o modalitate de abordare a acestei probleme:
- Identificaţi ceea ce doriţi să protejaţi;
- Identificaţi ceea ce reprezintă pericolele potenţiale;
- Determinaţi cât de probabile sunt pericolele;
- Implementaţi măsuri care să vă protejeze resursele proprii;
- Revedeţi periodic etapele de mai sus, luând măsuri de fiecare dată când este întâlnită o slăbiciune.

Probleme organizatorice

Scopul dezvoltării unei politici oficiale a firmei privind securitatea informatică îl reprezintă definirea procedurilor de utilizare corespunzătoare a calculatoarelor şi a reţelei, precum şi a unor proceduri care să prevină şi să acţioneze în cazul unor incidente de securitate. Pentru aceasta, trebuie luate în considerare mai multe aspecte:
1. Scopul şi tipul de activitate al organizaţiei. O firmă şi o universitate pot să acorde securităţii atenţii diferite.
2. Politica de securitate dezvoltată trebuie să se conformeze cu politicile, legile şi regulamentele de ordine interioară proprii. Din acest motiv este nevoie de identificarea acestora şi luarea lor în considerare pentru dezvoltarea politicii de securitate.
3. Dacă reţeaua locală nu este izolată şi independentă, este necesar să se ia în considerare problema securităţii într-un cadru mai larg. Politica de securitate trebuie să stipuleze proceduri atât pentru cazurile în care în reţeaua internă apar probleme de securitate datorate acţiunii unui sistem extern, cât şi pentru problemele de securitate apărute în cadrul altor sisteme din cauza acţiunii unui utilizator al propriului sistem.
Crearea politicii de securitate trebuie să rezulte din eforturile comune ale personalului tehnic, care înţelege implicaţiile implementării politicii propuse, cât şi a factorilor de decizie, care au puterea de a o aplica şi impune. O politică ce se dovedeşte a nu fi implementabilă sau care nu poate fi impusă nu este de nici un folos. Stabilirea unei politici de securitate informatică într-o firmă implică aproape fiecare utilizator de calculator. Utilizatorii obişnuiţi sunt responsabili pentru administrarea parolelor personale, pe când administratorii de sistem sunt obligaţi să rezolve erorile de securitate şi să supravegheze întregul sistem.
Un alt element cheie în cadrul unei politici de securitate îl constituie asigurarea că fiecare îşi cunoaşte propriul rol în menţinerea securităţii. O politică de securitate nu poate anticipa toate posibilităţile; totuşi, poate prevede ca pentru fiecare tip de problemă apărută să existe cineva responsabil cu rezolvarea aceasteia. Pe primul nivel se află fiecare utilizator, care are responsabilitatea de a-şi proteja propriul cont; un utilizator care permite compromiterea propriului cont poate mări şansele de a pune în pericol şi alte conturi sau resurse din sistem. Administratorii de sistem formează un alt nivel de responsabilitate; aceştia trebuie să asigure securitatea întregului sistem de calcul. Pe un alt nivel, mai important, se pot afla administratorii de reţea.

Analiza riscurilor

Analiza riscurilor reprezintă o etapă importantă, care implică determinarea entităţilor ce se doreşte a fi protejate, de cine anu-

me vor fi protejate şi cum anume va fi realizat acest lucru. Procesul prin care se examinează toate prezumtivele riscuri se catalogheză pe nivele de importanţă. Tot în această etapă se iau deciziile referitoare la costurile aferente protecţiei; o regulă de bază spune că niciodată nu trebuie făcute cheltuieli mai mari decât valoarea bunurilor protejate.

Principalele etape din analiza riscurilor sunt:

1. Identificarea resurselor ce trebuie protejate;
2. Identificarea pericolelor.

În continuare este prezentată o listă cu câteva *categorii de resurse* care ar trebui să intre în atenţia colectivului care elaborează politica de securitate a unei firme:

- **Hardware**: unităţi centrale, tastaturi, terminale, staţii de lucru, PC-uri, imprimante, discuri, linii de comunicaţie, servere de terminale, routere.
- **Software**: programe sursă, utilitare, programe de diagnoză, sisteme de operare, programe de comunicaţie.
- **Date**: date folosite pe timpul execuţiei programelor, arhive, baze de date, jurnale de auditare, date în tranzit pe mediile de comunicaţie.
- **Personal**: utilizatori, operatori, administratori de sistem şi de reţea.
- **Documentaţie**: documentaţie de programe, documentaţie tehnică a echipamentelor sau a sistemelor, proceduri administrative şi organizatorice locale.
- **Consumabile**: hârtie, formulare, riboane, medii optice şi magnetice.

Odată identificate resursele care necesită protecţie, este necesară identificarea posibilelor pericole care le ameninţă. Pericolele trebuie evaluate pentru a determina ce pierderi potenţiale pot implica. Cele mai importante tipuri sunt următoarele:

- **Accesul neautorizat** poate lua mai multe forme. Un exemplu de acces neautorizat îl reprezintă folosirea contului unei alte persoane pentru a obţine acces în sistem. Un alt exemplu este folosirea resurselor unui calculator fără permisiune prealabilă. Riscul unui acces neautorizat variază de la un sistem la altul; unele sisteme reprezintă ţinte preferate altora. Din studiile efectuate de echipa *CERT (Computer Emergency Response Team)* a rezultat că ţinta predilectă a intruşilor o formează universităţile de renume şi sistemele guvernamentale, bancare sau militare.
- **Divulgarea informaţiilor** reprezintă un alt posibilă pericol. El este determinat de valoarea sau gradul de secret al informaţiilor stocate pe calculatoare. De exemplu, cunoaşterea conţinutului unui fişier de parole poate conduce ulterior la o serie de accese neautorizate; citirea unei oferte comerciale poate oferi unui concurent un avantaj necinstit; o documentaţie tehnică a unui produs poate avea o valoare imensă datorată anilor de cercetare din care a rezultat.
- **Blocarea serviciilor** reprezintă un alt posibil pericol. Atunci când erviciile folositoare oferite de calculatoarele nu pot fi utilizate, rezultă inevitabil şi o pierdere de productivitate. Blocarea serviciilor poate avea multe forme şi poate afecta utilizatorii în mai multe moduri. O reţea poate deveni inutilizabiă datorită unui pachet de date nestandard, datorită unei blocări răuvoitoare a traficului sau datorită dezactivării sau configurării greşite a unei componente de reţea. Un virus poate încetini foarte mult viteza de operare sau poate chiar distruge complet datele dintr-un calculator. Fiecare organizaţie ar trebui să determine ce servicii îi sunt esenţiale şi pentru fiecare dintre ele să determine modul în care este afectată în cazul în care serviciile respective ar fi dezactivate.

Probleme de politică a securităţii

Există un număr de factori care trebuie luaţi în calcul la dezvoltarea unei politici de securitate a unei firme:

1. Cui i se permite accesul la resurse? Un prim pas în ceea ce priveşte dezvoltarea politicii de securitate este definirea exactă a celor cărora li se permite accesul la sistem şi la servicii. Politica trebuie să specifice explicit *cine* este autorizat şi *ce* resurse poate accesa.

2. Care este utilizarea corespunzătoare a resurselor? Politica de securitate trebuie să

specifice clar că utilizatorii sunt răspunzători pentru acţiunile pe care le iau. Această responsabilitate există indiferent de măsurile de securitate care sunt luate. Trebuie subliniat clar faptul că nu este permisă folosirea altor conturi în afara celui acordat, la fel ca şi încercarea de a ocoli măsurile de securitate. Iată câteva întrebări la care ar trebui răspuns în cadrul politicii de securitate adoptate:

- Este permisă folosirea altor conturi decât cel propriu?
- Este permisă încercarea de „spargere" a parolelor?
- Este permisă întreruperea unor servicii?
- Dacă utilizatorul găseşte un fişier cu drepturi de citire pentru „world" (toţi), înseamnă că are automat permisiunea de a-l citi?
- Dacă utilizatorul găseşte un fişier care nu îi aparţine, dar care are drepturi de modificare pentru „world" (toţi), înseamnă că are permisiunea de a-l modifica?
- Este permisă partajarea conturilor?

Răspunsul la majoritatea acestor întrebări ar trebui să fie *nu*.

Alte informaţii care ar trebui incluse în politica de securitate sunt cele referitoare la drepturile de autor (copyright):

- Programele software cu licenţă sau copyright nu pot fi copiate, decât dacă este explicit indicat;
- Modalităţile în care se poate face transferul licenţei;
- Dacă există dubii sau omisiuni referitoare la statutul programelor, copierea acestora este interzisă.

3. Cine este autorizat să acorde acces şi să aprobe folosirea resurselor? Politica de securitate ar trebui să specifice cine este autorizat să acorde acces utilizatorilor la serviciile sistemului. Mai mult, trebuie determinat ce tip de acces este permis a fi acordat. Dacă nu aveţi control asupra celor care acordă permisiunea de a accesa sistemul, înseamnă că nu veţi avea control nici asupra celor care utilizează sistemul. Există mai multe modalităţi ce pot fi folosite pentru a controla distribuţia accesului la serviciile sistemului. Factorii care trebuie luaţi în considerare sunt următorii:

- *Distribuirea accesului se face centralizat, dintr-un singur punct, sau descentralizat, din mai multe locuri?* Puteţi avea un punct de distribuire centralizată într-un sistem distribuit, în care mai multe departamente autorizează independent accesul. Compromisul care se face este între securitate şi confort; cu cât distribuirea accesului se face centralizat, cu atât este mai uşor de asigurat securitatea.
- *Ce metode veţi folosi pentru crearea conturilor şi întreruperea accesului?* În cel mai restrictiv caz, persoanele care sunt autorizate să acorde acces trebui să fie în măsură să intre direct în sistem şi să creeze conturi manual sau prin intermediul mecanismelor oferite de către producător. În general, acest mecanism presupune acordarea unei încrederi destul de mari persoanelor care fac acest lucru, deoarece acestea beneficiază de privilegii mari în cadrul sistemului. Altă soluţie este de a crea un mecanism (program) automat pe care îl pot folosi persoanele autorizate sau chiar utilizatorii înşişi pentru crearea conturilor. Selectarea sau proiectarea mecanismului trebuie făcută cu grijă, deoarece poate conţine puncte slabe care odată descoperite pot fi exploatate. De asemena, trebuie specificată clar procedura de utilizare a mecanismului respectiv precum şi interzicerea folosirii abuzive a acestuia. Nu trebuie uitate restricţiile de stabilire a parolelor: stabilirea unei lungimi minime, stabilirea intervalului după de expirare, interzicerea folosirii unei parole care a mai fost utilizată, o eventuală căutare în dicţionare pentru a elimina folosirea de parole uşor de ghicit etc.

4. Cine poate avea privilegii de administrare a sistemului? O decizie referitoare la securitate se referă la alegerea persoanei (persoanelor) care au acces la privilegiile administratorului de sistem şi la parolele serviciilor. Persoanele care deţin privilegii speciale pot fi controlate de o autoritate destinată acestui scop; în absenţa acestui control, există riscul pierderii controlului asupra sistemului.

5. Care sunt drepturile şi obligaţiile utilizatorului? Politica de securitate trebuie să conţină un enunţ referitor la drepurile şi

responsabilitățile utilizatorilor în ceea ce privește folosirea serviciilor sistemului de calcul. Trebuie subliniat clar că utilizatorii sunt responsabili de înțelegerea și respectarea regulilor de securitate în sistemele pe care le folosesc. Iată o listă cu elementele care trebuie acoperite de această parte a politicii:

- Există restricții (și dacă da, care) impuse referitor la consumul de resurse?
- Ce fapte ar constitui abuz, relativ la performanțele sistemului?
- Utilizatorii folosesc conturi proprii sau le partajează între ei?
- Cât de „secrete" ar trebui să își păstreze utilizatorii parolele?
- Cât de des ar trebui utilizatorii să își schimbe parolele și care sunt alte restricții referitoare la parole?
- Sistemul păstrează copii de siguranță (backups) ale datelor, sau utilizatorii trebuie să efectueze singuri acest lucru?
- Ce se întâmplă în cazul în care se fac publice informații private?
- Care este statutul poștei electronice private?
- Care este poziția față de participarea în liste de poștă sau grupuri de discuție controversate (referitoare la obscenitate, hărțuire etc.)?
- Care este poziția referitoare la comunicațiile electronice (interceptarea și falsificarea poștei etc.)?

6. Care sunt drepturile și responsabilitățile administratorului, raportat la cele ale utilizatorului? Trebuie făcut un compromis între dreptul utilizatorului la intimitate (activitate privată în cadrul sisteului) și necesitatea ca administratorul de sistem să aibă acces la cât mai multe informații pentru a diagnostica o problemă. Politica de securitate trebuie să specifice în ce măsură administratorul de sistem poate examina fișierele utilizatorilor în scopul diagnosticării sistemului; de asemenea, nu ar fi lipsită de importanță introducerea unui enunț prin care administratorii de sistem sunt obligați să păstreze confidențialitatea asupra informațiilor observate în aceste circumstanțe.

Iată câteva întrebări la care ar trebui să dați un răspuns:

- Poate un administrator să monitorizeze sau să citească fișierele unui utilizator, indiferent de motiv?
- Au dreptul administratorii de rețea să examineze traficul prin rețea sau pe calculatoarele gazdă?

7. Cum se procedează în ceea ce privește informațiile confidențiale? Înainte de a permite accesul utilizatorilor la serviciile sistemului, trebuie să determinați până la ce nivel asigurați securitatea datelor din sistem. Prin aceasta, veți determina nivelul de secret al datelor pe care utilizatorii au dreptul să le păstreze în sistemul dumneavoastră, și veți evita situațiile în care utilizatorii păstrează date cu înalt grad de confidențialitate pe un sistem insuficient asigurat din punct de vedere al securității. Trebuie specificat în mod clar utilizatorilor care folosesc informații confidențiale ce anume suporturi să folosească pentru păstrarea acestora (discuri, benzi, servere de fișiere etc.). Politica în acest domeniu trebuie coroborată cu cea referitoare la drepturile administratorilor de sistem raportate la drepturile utilizatorilor.

Proceduri de prevenire a incidentelor de securitate

Pentru a determina riscurile, trebuie identificate punctele vulnerabile. Lista redată în continuare nu este completă, dar poate prezenta un punct de plecare în stabilirea vulnerabilităților unui sistem:

- *Puncte de acces.* Într-o rețea, punctele de acces în sistem trebuie menținute în număr minim. Liniile telefonice conectate prin modem la un port al unei mașini oferă de obicei acces la calculatorul respectiv, însă dacă modemul este conectat la un server de terminale, linia telefonică poate permite accesul în întreaga rețea.
- *Sisteme configurate greșit.* Aceste sisteme sunt ideale pentru a fi atacate, prezentând de obicei vulnerabilități. Sistemele de operare de azi sunt atât de complexe încât administrarea lor este foarte complexă. De multe ori, administratorii de sistem sunt nespecialiști, aleși din cadrul personalului organizației. Și vânzătorii de sisteme sunt

parțial responsabili pentru sisteme incorect configurate; pentru a simplifica procedura de instalare, aceştia aleg pentru instalare configurația cea mai redusă din punct de vedere al securității.

• *Erorile de programare.* Programele complexe vor conține întotdeauna erori. Erorile cunoscute ale unor programe pot fi exploatate de către atacatori; din acest motiv, este indicat ca administratorii de sistem să fie la curent cu ultimile versiuni de produse anunțate de către producători şi să instaleze completările (patch-urile) care rezolvă problema existentă. De asemenea, trebuie raportate producătorului toate erorile semnalate în programe, aşa încât acesta să găsească soluția şi să distribuie un nou patch.

• *Amenințări din interior.* Un risc considerabil îl reprezintă persoanele din interiorul organizației care au acces la componente ale sistemului sau ale rețelei. O persoană din interior poate avea acces fizic la mai multe stații de lucru de rețea, stații de unde poate urmări cu ajutorul anumitor programe tot traficul de pe rețea.

Există metode hardware, software sau procedurale care pot fi folosite în sprijinul asigurării securității sistemului:

• Majoritatea rețelelor sunt deschise în zilele noastre spre diferite rețele publice (Internet). Conectarea într-o rețea WAN este indicat să se realizeze prin intermediul unui sistem de protecție de tip *pasarelă de securitate* (*firewall*) care să izoleze rețeaua internă de „lumea" din exterior, sau printr-un router configurat pentru a filtra anumite pachetele de date adresate anumitor porturi.

• Confidențialitatea reprezintă unul dintre scopurile primare ale administratorilor de sistem. Există mai multe mecanisme care asigură acest lucru, cum ar fi criptarea hardware şi software (folosind mecanismul DES care este standardizat, sau alte mecanisme de criptare simetrică), sau folosirea programelor de poştă securizată (PGP sau PEM).

• Autentificarea autorului unui mesaj reprezintă un mijloc de protecție în cazul rețelelor nesigure, deoarece este relativ simplu de imitat adresa sursei unui mesaj de poştă. În aceste cazuri sunt folositoare semnăturile digitale obținute prin criptosisteme cu chei publice, sau certificatele digitale elaborate de o autoritate de încredere.

• Integritatea informației reprezintă o altă problemă care trebuie să se afle în atenția administratorilor de sistem. Testarea integrității confirmă sau infirmă faptul că documentul sau mesajul vehiculat prin rețea a fost modificat de persoane neautorizate. Problema integrității este rezolvată de obicei prin folosirea unor sume de control (checksums) ataşate documentului, sau prin folosirea unor funcții hash (MD5, Snefru etc.), care prin proprietatea de a fi neinversabile determină cu exactitate dacă informația a fost sau nu alterată.

• Sistemele de autentificare presupun de obicei ca utilizatorul să confirme că este autorizat să acceseze sistemul furnizând o parolă personală. Pentru a îmbunătăți acest mecanism de autentificare s-au proiectat mecanisme complexe (de tip provocare/ răspuns, Kerberos sau prin cartele inteligente - smartcard) care reduc la minim riscul ca un utilizator neautorizat să folosească o parolă care nu îi aparține pentru a accesa sistemul.

• Monitorizarea sistemului şi a traficului prin rețea reprezintă o activitate specifică administratorului de sistem, care foloseşte în acest scop diverse metode. Nu trebuie uitată şi căutarea continuă a eventualelor „porți" vulnerabile ale sistemului, prin care se pot „strecura" intruşii; în acest scop există utilitare specializate (SATAN, COPS) care sunt special proiectate pentru a căuta vulnerabilitățile unui sistem.

Tratarea incidentelor de securitate

Ori de câte ori un sistem suferă un incident care poate duce la compromiterea securității informatice a firmei, strategiile de abordare pot fi influențate de două interese opuse.

Dacă factorii de decizie (conducerea) se tem că sistemul este vulnerabil, poate alege strategia denumită „Protejează şi continuă" *(Protect and Proceed)*. Acest mod de abordare are ca scop protecția şi păstrarea

funcţiilor sistemului, precum şi revenirea rapidă la condiţiile normale de lucru pentru utilizatori. Trebuie făcute încercări de a interveni în procesul de intruziune, în scopul de a-l stopa şi de a preveni repetarea incidentului; măsurile pot implica oprirea serviciilor, închiderea accesului la reţea sau alte măsuri drastice. După stoparea intrusului, trebuie luate măsuri imediate de identificare şi inventariere a pagubelor, precum şi măsuri de refacere a pierderilor. Dezavantajul metodei este că dacă instrusul nu poate fi identificat direct, el poate reveni în sistem pe o altă cale, sau poate încerca să atace o altă gazdă din sistem. Această modalitate de abordare poate fi aleasă dacă resursele nu sunt foarte bine protejate, dacă penetrarea repetată a sistemului conduce la riscuri din punct de vedere financiar, sau dacă utilizatorii sistemului nu deţin cunoştinţe în domeniul securităţii şi din aceată cauză lucrările lor devin vulnerabile.

Cealaltă modalitate de abordare a incidentelor de securitate, „Urmăreşte şi acuză" *(Pursue and Prosecute)* adoptă o strategie total diferită ca scopuri. Principalul scop este acela de a permite intruşilor să-şi continue activităţile în sistem până când se pot identifica persoanele responsabile. Această strategie este agreată în special de instituţiile sau organizaţiile guvernamentale. Metoda poate fi aplicată în cazurile în care sistemul şi resursele sale sunt bine protejate, dacă sunt disponibile copii de siguranţă (back-ups), dacă sistemul atrage prin natura sa intruşii (firme internaţionale, organizaţii guvernamentale, financiar-bancare etc.), dacă accesul intrusului poate fi controlat cu uşurinţă şi dacă există mijloace (echipamente, personal de specialitate, programe etc.) care să permită monitorizarea şi investigarea activităţilor instrusului.

În cazul apariţiei unui incident, trebuie să existe un plan de urmat (tot aşa cum există şi planuri în cazul apariţiei a unui incendiu sau a unui accident de muncă). Răspunsul eficient la apariţia unui incident de securitate este important din mai multe motive. Iată câteva dintre avantaje:

- Cel mai important beneficiu este legat de prevenirea pierderilor de vieţi omeneşti; anumite sisteme de calcul sunt sisteme de care pot depinde vieţi omeneşti - cum ar fi sistemele din spitale sau cele pentru asistarea controlului traficului aerian.
- Un alt avantaj major este referitor la protejarea informaţiilor secrete, confidenţiale sau personale. Unul dintre pericolele majore în cazul apariţiei unui incident de securitate este acela că datele pot fi distruse iremediabil; o rezolvare eficientă a cazului minimizează aceste pierderi.
- Un al beneficiu este legat de publicitatea negativă; ştirile referitoare la incidente de securitate se răsfrâng negativ asupra imaginii organizaţiei, de exemplu asupra unei bănci; o abordare rapidă şi eficientă a cazului minimizează pericolul răspândirii unor astfel de veşti neplăcute.

Principalele puncte care trebuie atinse într-o politică de rezolvare a incidentelor sunt:

- *Trecerea în revistă* (care sunt scopurile şi obiectivele ce trebuiesc urmărite pentru a rezolva incidentul). Scopurile urmărite pentru rezolvarea unui incident de securitate pot fi asigurarea integrităţii sistemelor critice, menţinerea şi restaurarea datelor şi serviciilor, cunoaşterea situaţiei (ce s-a întâmplat), evitarea amplificării pierderilor sau a viitoarelor incidente, evitarea publicităţii negative, găsirea şi pedepsirea atacatorului.
- *Evaluarea* (cât de serios este incidentul). Există anumite indicaţii sau „simptome" care atrag atenţia asupra unui incident şi care trebuie luate serios în considerare: blocări ale sistemului, apariţia unor conturi noi de utilizator, apariţia unor fişiere noi, unele cu denumiri neobişnuite, modificări în fişierele jurnal, modificări în dimensiunea sau data unor fişiere, încercări de a scrie în fişiere de sistem, scăderi ale performanţei sistemului etc. Totuşi, nici una dintre aceste indicaţii nu determină 100% că este vorba de un incident; pe de altă parte, se poate petrece un incident fără ca nici una dintre simptomele de mai sus să se manifeste. Aceste indicaţii trag totuşi un semnal de alarmă; administratorul de sistem trebuie să caute cauza apariţiei simptomelor pentru a lua decizia de anunţare a unui incident de securitate.

• *Anunțarea* (cine trebuie anunțat în cazul apariției unui incident). După ce incidentul a fost confirmat cu precizie, trebuie anunțat personalul responsabil cu rezolvarea incidentului și factorii de decizie.
• *Răspunsul* (care este reacția la incident). Trebuie definite măsurile care se iau ca răspuns la atac: recâștigarea controlului asupra sistemului, respectarea politicii de securitate, monitorizarea activității, limitarea accesului sau oprirea sistemului.
• *Implicațiile legale* (care sunt aspectele legale ale producerii incidentului). Există mai multe implicații legale, referitoare printre altele la colaborarea cu agențiile de investigare, responsabilitatea organizației în cazul în care sistemul propriu atacat conduce ulterior și la atacarea unui sistemu al altei organizații, responsabilitatea organizației în legătură cu distribuirea de informații referitoare la vulnerabilitatea altei organizații, sau posibilitatea de a fi dat în judecată dacă traficul utilizatorilor din rețea este monitorizat fără ca aceștia să fie avertizați de aceasta.
• *Documentația* (ce documente și înregistrări trebuie păstrate înainte, în timpul și după incident). Principalele documente ce trebuie păstrate în cazul unui incident sunt jurnalele de activități din sistem (care conțin înregistrări de investigare sau audit), jurnalele cu comenzile date (împreună cu ora la care au fost executate), precum și înregistrarea eventualelor convorbiri telefonice (cu cine s-a vorbit, când și care a fost conținutul conversației).

Procedurile post-incident

După un incident de securitate ar trebui luate mai multe măsuri. Acestea pot fi rezumate după cum urmează:
• Trebuie făcută o inventariere a resurselor sistemului, din care să rezulte cât de afectat a fost acesta în urma atacului.
• Trebuie înlăturate vulnerabilitățile care au cauzat incidentul.
• Politica de securitate trebuie revizuită pe baza cunoștințelor dobândite pe urma incidentului, pentru a evita reapariția aceluiași tip de incident.
• Trebuie dezvoltată o nouă analiză de risc, pe baza pierderilor suferite datorită incidentului;
Dacă se dorește și este posibil, trebuie începută acționarea în justiție a persoanelor responsabile de producerea incidentului.

Unde mai puteți apela în caz de incident

După spectaculoasa invazie a Viermelui în Internet, **Echipa de intervenție specializată în caz de incidente de calculatoare-*CERT*-** s-a stabilit la Carnegie Mellon University Pennsylvania. Rolul CERT este de a asigura punctul de distribuție și colecție a informațiilor de securitate legate de Internet. Adresa Internet a lor este **www.cert.org** iar persoanele care sunt pregătite să vă ajute sunt specialiști de marcă. Țineți minte că ei sunt plătiți ca să asigure protecția membrilor Internet-ului. Dacă nu sunteți un expert al sistemelor de operare și al rețelelor, puteți să găsiți un consultant cu mai multă experiență care să vă ajute în timpul și după perioada cu probleme. Există un număr mare de specialiști, iar un bun expert în securitate informatică vă poate fi de ajutor.

Bibliografie

1. Securitatea informatică în UNIX și INTERNET - Victor Patriciu, Monica Pietroșanu, Ion Bica, Costel Cristea, Editura Tehnică, 1998
2. Internet Security Professional Reference Derek Atkins, Paul Buis, Chris Hare, Robert Kelley, ș.a, New Riders Publishing 1996
3. RFC 1244 - The Site Security Handbook Grupul de lucru pentru elaborarea politicilor de securitate (Site Security Policy Handbook Working Group) de la Internet Engineering Task Force, 1991