Security Planning in IT Systems

Prep. Radu CONSTANTINESCU
Catedra de Informatică Economică, A.S.E. Bucureşti

Security planning is a necessity nowadays. Planning involves policies, controls, timetable and a continuing attention. Policies are the foundation of effective information security. Security policies challenge users to change the way they think about their own responsibility for protecting corporate information. The paper presents the compulsive elements of security planning.
Keywords: *security planning, policy, business continuity, timetable*

Introducere

Cu ceva ani în urmă, majoritatea activităților de calcul se efectuau pe stații mainframe. Acestea se găseau în centre de calcul specializate şi erau supravegheate de experți ce asigurau securitatea informatică. Începând cu introducerea calculatoarelor personale în anii 1980, o mare parte a responsabilităților de securitate au fost transferate la nivelul utilizatorilor. Responsabilitatea nu este conştientizată la nivel real de către mulți utilizatori. Din nefericire sunt multe exemple în acest sens. Tendința este accentuată de natura aparent ascunsă a unor date importante. Oamenii au înclinația să protejeze cu atenție documentele în format tipărit însă neglijează gradul de securitate pe care trebuie sa-l asigure documentelor în format electronic. Modul facil de stocare a unor cantități imense de informație pe dispozitive de dimensiuni reduse accentuează riscul la care acestea sunt expuse. Pentru a evita neplăcerile şi nu numai, companiile trebuie să dezvolte planuri de securitate. Un plan de securitate este un document care descrie modul în care organizația va aborda problemele de securitate. Planul trebuie reanalizat şi îmbunătățit periodic deoarece nevoile de securitate ale organizației se schimbă în permanență.

Un plan de securitate identifică şi organizează activitățile pentru asigurarea securității informației. Orice plan de securitate trebuie să se refere la următoarele aspecte: politica de securitate, starea curentă, cerințele de securitate, mecanismele de control, înregistrarea evenimentelor, planificarea operațiilor şi îmbunătățirea permanentă.

Politica

Un plan de securitate trebuie să specifice politica de securitate a firmei. O politică de securitate conține precizarea scopurilor şi a intențiilor. La o primă vedere toate politicile de securitate sunt similare având ca obiectiv prevenirea breşelor de securitate. În realitatea elaborarea unei politici de securitate este un proces dificil care presupune adaptarea la specificul organizației.

O politică de securitate trebuie să răspundă fără echivoc la următoarele întrebări:

- Cine poate avea acces?
- La ce resurse de sistem şi organizaționale va fi permis accesul?
- Ce tip de acces va primi fiecare utilizator pentru fiecare resursă?

O politică de securitate trebuie să specifice în mod clar următoarele aspecte:

- *obiectivele organizației privind securitatea:* asigurarea protecției datelor împotriva scurgerilor de informații către entități externe, protejarea datelor față de calamitățile naturale, asigurarea integrității datelor sau asigurarea continuității afacerii;
- *personalul răspunzător pentru asigurarea securității, care poate fi:* un grup restrâns de lucru, un grup de conducere sau fiecare angajat;
- *implicarea organizației în ansamblu la asigurarea securității:* cine va asigura instruirea în domeniul securității, cum va fi integrată partea de securitate în structura organizației.

Starea curentă

Pentru a putea planifica securitatea, o organizație trebuie să înțeleagă vulnerabilitățile la care este expusă. Organizația poate determina vulnerabilitățile pe baza unei analize a riscului. Aceasta reprezintă o investigare atentă a sistemului, a mediului şi a lucrurilor care ar putea funcționa necorespunzător. Analiza riscului este fundamentală pentru descrierea stării curente a securității informatice. Descrierea poate conține lista activelor organizaționale, amenințările de securitate la adresa lor şi mecanismele de control care protejează aceste active.

În descrierea stării curente trebuie specificați responsabilii pentru securitatea fiecărui activ. De asemenea este stabilită limita de responsabilitate, cu precădere atunci când organizația lucrează în rețea.

Cu toate că un plan de securitate trebuie să aibă caracter atotcuprinzător, cu siguranță vor exista vulnerabilități neluate în considerare. Acestea pot fi rezultatul ignoranței şi naivității dar şi a introducerii de noi echipamente sau tipuri de date pe măsură ce sistemul evoluează. De asemenea pot apărea situații noi, neanticipate de către proiectanții sistemului de securitate. Din aceste motive trebuie să existe o detaliere a procesului de urmat în momentul identificării unor noi vulnerabilități şi a modului de integrare a metodelor de control aferente.

Cerințele de securitate

Cerințele de securitate constituie nucleul unui plan de securitate. Acestea reprezintă necesități funcționale sau de performanță din cadrul unui sistem care determină un nivel dorit de securitate. În unele cazuri cerințele pot fi impuse de către organisme externe, cum ar fi agențiile guvernamentale sau organismele de standardizare. Figura 1 ilustrează modul de construire a unui plan de securitate ținând cont de cerințe şi de restricții.

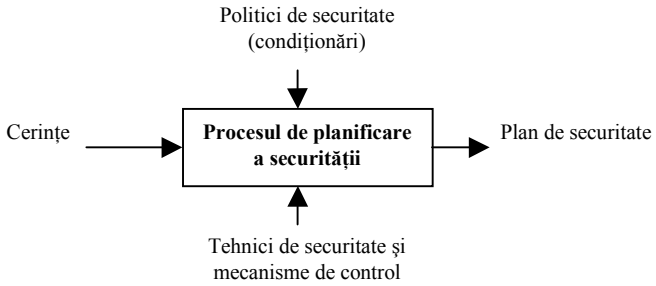

Fig.1. *Elaborarea planului de securitate*

Un exemplu de pachet de cerințe este varianta TCSEC (Trusted Computer System Evaluation Criteria):

- *politica de securitate:* este obligatorie existența unei politici de securitate explicită şi bine definită impusă la nivelul sistemului;
- *identificarea:* fiecare subiect trebuie să fie unic şi bine definit. Identificarea este necesară pentru a putea verifica modul de accesare a resurselor de către subiecții sau obiectele din sistem;
- *marcarea:* fiecare obiect trebuie asociat cu o etichetă care să indice nivelul de securitate specific. Asocierea trebuie să permită specificarea rapidă a parametrilor de securitate în momentul solicitării accesului la obiectul respectiv;
- *înregistrarea:* sistemul trebuie să țină o evidență completă şi sigură a acțiunilor care pot afecta securitatea. Astfel de acțiuni includ adăugarea unor noi utilizatori în sistem, modificarea nivelului de securitate aferent unui subiect sau obiect şi interzicerea unei încercări de acces la resursele sistemului;
- *asigurarea*: sistemul trebuie să poată impune mecanismele de securitate şi trebuie să poată evalua corect eficiența acestora;
- *protecție continuă:* mecanismele ce implementează securitatea trebuie să fie protejate față de modificări neautorizate.

Procesul de planificare a securității trebuie să permită clienților sau utilizatorilor să specifice funcțiile dorite, independent de implementare. Cerințele trebuie să se refere la toate aspectele securității: confidențialitate, integritate şi disponibilitate. Acestea trebuie să aibă următoarele caracteristici: corectitudine, consistență, completitudine, realism, necesitate, verificabilitate, trasabilitate. Cerințele mai pot fi condiționate şi de buget, planuri, performanță, politici sau reglementări guvernamentale.

Mecanismele de control recomandate

Cerințele de securitate specifică necesitățile sistemului în ceea ce priveşte componentele ce trebuie protejate. Un plan de securitate trebuie să recomande şi ce mecanisme de control să fie cuprinse în sistem pentru a realiza aceste cerințe. Prin analiza riscului se poate crea o schemă a corelării vulnerabilităților cu mecanismele de control. Mecanismele de control determină modul în care va fi proiectat şi dezvoltat sistemul pentru a îndeplini cerințele de securitate.

Responsabilitatea implementării

Un plan de securitate trebuie să conțină şi o secțiune care să identifice persoanele responsabile cu implementarea cerințelor de securitate. În acelaşi timp, planul specifică în mod exact răspunzătorii în cazul în care o cerință nu este îndeplinită sau dacă anumite vulnerabilități nu sunt documentate. Planul specifică, de asemenea, cine este responsabil pentru implementarea măsurilor de control atunci când o nouă vulnerabilitate este descoperită sau un nou tip de activ este introdus în folosință. Putem specifica rolurile diferitelor persoane care interacționează cu sistemul:

- *utilizatorii PC:* pot fi responsabili pentru securitatea propriilor calculatoare. În mod alternativ poate fi delegată o persoană sau un grup care să coordoneze această activitate;
- *şefii de proiect:* pot fi responsabili pentru securitatea datelor;
- *managerii:* pot fi responsabili cu urmărirea modului în care personalul implementează măsurile de securitate;
- *administratorii de baze de date:* pot fi responsabili cu reglementarea accesului şi integritatea datelor;
- *membrii departamentului resurse umane:* pot fi responsabili cu verificarea bonității morale a angajaților şi cu organizarea de activități de pregătire a personalului în domeniul securității informației.

Planificarea operațiilor

Un plan de securitate la nivel de organizație nu poate fi implementat în mod instantaneu. Planul de securitate conține un planificator care specifică cum şi când vor fi efectuate activitățile prevăzute. Sunt planificate şi etapele intermediare pentru ca echipa de conducere să poată urmări progresul implementării.

În cazul în care implementarea are o dezvoltare fazică, în sensul că sistemul va fi implementat parțial într-o primă fază ca apoi în fazele ulterioare să se adauge noi funcționalități, planul trebuie să descrie şi modul în care cerințele de securitate vor fi implementate în timp. De exemplu, în cazul în care mecanismele de control sunt costisitoare sau complicate, acestea pot fi introduse gradual. De asemenea, mecanismele de control procedurale pot necesita pregătirea personalului pentru ca toată lumea să le înțeleagă şi să le accepte. Planul trebuie să specifice şi ordinea de implementarea a mecanismelor de control, astfel încât cele mai mari expuneri să fie acoperite pe cât de repede posibil.

Planul trebuie să fie extensibil, deoarece condițiile se pot schimba. Pot apărea noi echipamente, pot fi solicitate noi modalități de conectare sau pot fi identificate alte amenințări. Planul trebuie să includă o procedură pentru modificare şi dezvoltare, astfel încât aspectele de securitate aferente să fie luate în considerare la momentul pregătirii schimbării şi nu după ce schimbarea a fost deja făcută.

Atenție continuă

Securitatea informatică necesită mai mult decât bune intenții. Este important să existe o metodă de evaluare a nivelului de securitate. Odată cu schimbările la nivelul utilizatorilor, datelor sau echipamentelor pot apărea noi expuneri. Măsurile curente pot deveni depă-

şite sau ineficiente. Inventarul activelor şi lista mecanismelor de control necesită îmbunătăţirea permanentă şi reefectuarea analizei de risc.

Acceptarea planului de securitate

După scrierea planului de securitate, acesta trebuie să fie aprobat iar recomandările sale sunt duse la îndeplinire. Acceptarea de către organizaţie este cheia succesului unui plan de securitate. Angajamentul faţă de plan presupune că funcţiile de securitate vor fi implementate iar activităţile vor fi duse la îndeplinire. Succesul planului depinde de trei categorii de persoane:

- echipa de planificare trebuie să fie sensibilă la nevoile fiecărui grup ce este afectat de plan;
- persoanele asupra cărora planul de securitate produce efecte directe trebuie să înţeleagă ce înseamnă acesta şi ce presupune pentru modul în care utilizează sistemul şi îşi desfăşoară activitatea;
- echipa de management trebuie să supervizeze implementarea politicii de securitate şi să-i dea greutate acesteia.

Prin promovarea importanţei securităţii informaţionale se pot accepta şi înţelege mai uşor planurile de securitate şi importanţa lor. Este relevant pentru acest lucru cazul unui angajat care a modificat de 24 de ori succesiv parola pentru a putea reveni la varianta favorită iniţială în condiţiile în care sistemul solicita modificarea parolei la un interval de timp stabilit şi restricţiona parola în sensul nerepetării acesteia în istoricul ultimelor 23 de variante. În mod evident angajatul nu a înţeles sau nu a fost de acord cu planul de securitate sau cel puţin cu partea ce specifică restricţiile la nivelul parolelor de acces.

Sprijinul conducerii este condiţionat de înţelegerea rolului politicii de securitate şi a funcţiunilor acesteia. Înţelegerea presupune şi cunoaşterea efectelor potenţiale ale lipsei de securitate. Planul de securitate trebuie să prezinte o analiză comparativă a costurilor mecanismelor de securitate şi a pierderilor potenţiale în lipsa lor. Personalul de conducere nu este reprezentat în majoritatea cazurilor de specialişti IT. Din acest motiv, riscurile de securitate informatică trebuie prezentate în termeni uşor de înţeles de către nespecialişti. Trebuie evitată terminologia tehnică. De asemenea, conducerea este reticentă în a aloca fonduri pentru mecanisme de control fără o justificare clară. Echipa de dezvoltare pentru politica de securitate poate ajuta eliminarea acestor probleme prin descrierea vulnerabilităţilor în termeni financiari şi în contextul activităţilor curente.

Planuri pentru continuitatea afacerii

Companiile cu putere financiară redusă pot fi scoase de pe piaţă în urma unui incident de securitate. Lipsa sistemului informatic poate determina oprirea temporară a afacerii ceea ce implică sistarea vânzărilor şi automat înregistrarea de pierderi.

Un plan pentru continuitatea afacerii documentează modul în care o afacere se va derula în condiţiile unui incident de securitate. Un plan de securitate standard presupune abordarea problemelor de securitate informatică în condiţii normale şi presupune protejarea afacerii în prisma unui număr de vulnerabilităţi din surse uzuale. Un plan pentru continuitatea afacerii se referă la situaţii catastrofale, în care o mare parte a capacităţii de calcul este în mod brusc indisponibilă. Efectele sunt pe termen lung, ceea ce afectează în mod direct afacerea.

În continuare vom prezenta o serie de evenimente care necesită existenţa unui plan de continuitate a afacerii:

- incendiu care distruge întreaga reţea de calculatoare a unei companii;
- eroare software persistentă care determină neutilizarea sistemului informatic;
- lipsa curentului electric, a echipamentelor de comunicaţie, a accesului la reţea sau a altor servicii critice;
- inundaţie ce împiedică personalul specializat să ajungă la un punct de lucru important.

Pentru elaborarea unui plan de continuitate a afacerii trebuie urmate o serie de etape. Acestea sunt:

- evaluarea impactului situaţiilor de criză asupra afacerii;
- dezvoltarea unei strategii de control a impactului;

• dezvoltarea şi implementarea unui plan pe baza strategiei.

Pentru evaluarea impactului unor situaţii de criză asupra afacerii trebuie răspuns la următoarele întrebări:

• Care sunt activele esenţiale?
• Care sunt evenimentele care pot bloca afacerea?
• Ce vulnerabilităţi ar putea influenţa negativ folosirea activelor?

În determinarea activelor cheie nu trebuie să se treacă cu vederea personalul şi materialele folosite, cum ar fi documentaţiile sau echipamentele de comunicaţie. O altă modalitate de abordare este să se determine care este numărul minim de activităţi necesare pentru a menţine caracterul operaţional al afacerii, la un acceptabil.

Strategia de control specifică modul în care pot fi protejate activele cheie. În unele cazuri o copie de rezervă sau un echipament hardware redundant pot fi de ajuns. Ideal este ca afacerea să poată continua fără nici o pierdere, însă în situaţii catastrofale numai o anumită parte a afacerii poate fi funcţională. În acest caz, trebuie dezvoltată o strategie optimă pentru afacere şi clienţi. De exemplu se poate decide să se menţină jumătate din funcţiunea X şi jumătate din funcţiunea Y sau o mare parte din funcţiunea X şi puţin din funcţiunea Y. Durata evenimentului catastrofal este un alt factor important. De exemplu, reconstrucţia după un incendiu poate fi un proces lung şi implică funcţionarea îndelungată în stare de avarie. Modalităţile de răspuns trebuie să fie alcătuite astfel încât să existe variante de răspuns şi pentru incidente de durată mică şi pentru cele pe termen lung.

Un plan pentru continuitatea afacerii specifică o serie de aspecte importante: cine este coordonatorul în momentul declanşării unui eveniment catastrofal, ce trebuie făcut şi cine trebuie să fie implicat în activităţile respective. Planul justifică activităţile de prevenire cum ar fi: achiziţionarea de hardware redundant, alcătuirea de copii de rezervă pentru date sau depozitarea de provizii pentru calamităţi. Planul specifică necesitatea pregătirii personalului pentru a ştii cum trebuie să reacţioneze şi pentru a evita confuzia generalizată. Responsabilul cu coordonarea în caz de calamitate va declara starea de urgenţă şi va instrui colaboratorii asupra modului de urmare a procedurilor specificate în plan. Tot acesta va instaura starea de urgenţă care se va încheia atunci când lucrurile vor reveni la normal.

Scopul planului pentru continuitatea afacerii este să ţină afacerea în derulare cât timp personalul specializat rezolvă problema. Un plan de continuitate a afacerii nu include aspecte conexe cum ar fi chemarea pompierilor sau prezentarea modului de evacuare a clădirii ci este axat pe menţinerea în funcţiune a afacerii.

Concluzii

Planificarea securităţii informaţiei determină crearea unui cadru de lucru coerent aducând siguranţă şi calitate demersului economic. Nivelul de bunăstare al unei naţiuni, mai exact nivelul calităţii vieţii de care au parte cetăţenii acelei ţări, depinde în mod decisiv de calitatea produselor şi serviciilor pe care acea ţară le produce. În a doua jumătate a secolului trecut, una dintre cele mai importante înnoiri survenite în planul calităţii a fost transformarea încrederii în calitate într-o marfă în sine, într-un element care adaugă valoare la valoarea intrinsecă a produsului sau serviciului.

Informaţiile trebuiesc să fie protejate, indiferent de forma în care se regăsesc. Implementarea politicilor şi standardelor de securitate asigură o mai bună înţelegere a responsabilităţilor tuturor celor implicaţi în activitatea economică. De asemenea activitatea va beneficia de un plus de credibilitate.

Bibliografie

[Ghos01] Ghosh, A. - *Security and Privacy for E-Business,* Ed. John Wiley & Sons, 2001

[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.

[ISO17799] ISO/IEC 17799 Standard

[BS7799] BS 7799 Standard