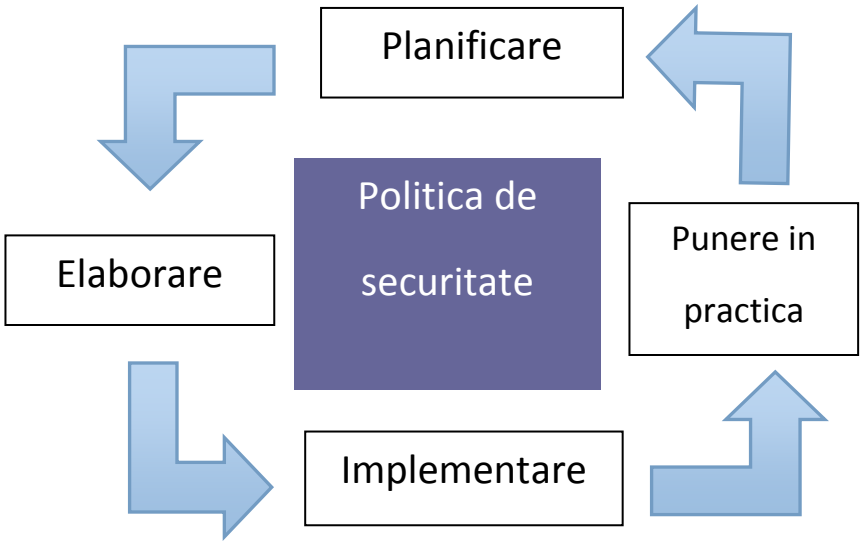
INTRODUCERE

Un plan de securitate impreuna cu politica de securitate din care a rezultat el sunt proiectate pentru a proteja atat informatiile cat si resursele materiale critice de la o gama larga de amenintari in scopul de a asigura continuitatea activitatii acelei institutii (a afacerii in cazul unei companii), de a reduce riscul in afaceri, de a maximiza randamentul investitiilor si a oportunitatilor de afaceri.

Securitatea IT se realizeaza prin implementarea unui set adecvat de politici, de proceduri, si de controale atat la nivel software cat si la nivel hardware pentru toate structurile organizatorice. Toate acestea trebuiesc stabilite, implementate, monitorizate, revizuite si imbunatatite pentru a se asigura securitatea la acest nivel precum si pentru ca obiectivele economice sa poata fi atinse.

Elaborarea unei bune politici de securitate trebuie vazuta ca un proces si nu ca o actiune.



Planul de securitate asigura securitatea si confidentialitatea datelor institutiei, informatiile de interes privat, responsabilitatile atat la nivelul departamentelor cat si la nivelul fiecarei persoane fizice pentru astfel de date.

SCOP

Masurile de securitate in domeniul IT sunt menite sa protejeze informatiile (vazute ca “bunuri”) si sa conserve intimitatea tuturor angajatilor, furnizorilor, sponsorilor, partenerilor, elevilor / studentilor, precum si a oricaror alte entitati asociate cu institutia in cauza.

Politicile de securitate servesc drept linii directoare generale pentru utilizarea, prelucrarea si managementul informatiilor.

Scopul planului de securitate este sa asigure confidentialitatea, integritatea si disponibilitatea datelor, sa defineasca, sa dezvolte, si sa documenteze politicile si procedurile de informare ce vin in sprijinul scopului si obiectivelor institutiei precum si sa permita institutiei sa indeplineasca din punct de vedere legal si etic responsabilitatile cu privire la resursele IT.

Controalele interne ofera un sistem de control si echilibrare in scopul de a identifica nereguli, de a previni acumularea de “deseuri de date”, fraude si abuzuri aparute sau alte discrepante introduse accidental in operatiunile IT curente.

Prin aplicarea in mod consecvent, fara exceptii a politicilor si procedurilor de securitate se asigura protejarea si/sau disponibilitatea informatiilor, se asigura si se contribuie la continuitatea si dezvoltarea afacerii, la cresterea profitabilitatii.

Utilizarea necorespunzătoare a politicii sau planului de securitate expune institutia la riscuri al caror cost este foarte greu de calculat (atacuri ale virusilor, compromiterea sistemelor de calcul, a serverelor, a retelei de comunicatii, a altor servicii IT). DIn pacate, astfel de incidente, pe langa latura financiara si de incredere mai pot avea o latura legala.

DOMENIUL DE APLICABILITATE

Politicile si planul de securitate se pun in aplicare de catre toti membrii acelei comunitati, fara “discriminari pozitive”, inclusiv presedintele / directorul general, rectorul, decanii, directorii / sefii de departament, angajatii, angajatii temporar, profesorii,

studentii, elevii, absolventii, partenerii de afaceri, voluntarii, oaspetii sau, in general, oricine are acces la bunurile informationale ale institutiei respective. Aceste bunuri informationale includ date, imagini, text sau bucati software utilizate pe hardware-ul din institutie, pe hartie sau orice alt mediu de stocare.

DEFINITII

- Confidentialitate = conservarea restrictiilor privind accesul autorizat si folosirea anumitor tipuri de informatii (ex: date personale, medicale, bancare)
- Integritate = reprezinta masurile impotriva modificarilor necorespunzatoare sau neautorizate sau a distrugeri informatiilor
- Disponibilitate = asigura accesul rapid si fiabil la informatii; o pierdere de disponibilitate reprezinta este o perturbare a accesului la informatii sau la un sistem informational
- Evaluarea riscurilor = un proces care determina resursele de informare existente, nevoile de protectie, intelege si documenteaza potentialele riscuri ce apar ca urmare a unor insuccese in securitatea IT ce pot duce la pierderea confidentialitatii, a integritatii sau a disponibilitatii datelor; evaluarea riscurilor sta la baza elaborarii politicilor de securitate
- Controlul activitatilor = sunt politicile, procedurile, tehnicile si mecanismele care ajuta conducerile institutiilor sa se asigure ca reduc riscurile identificate in cadrul evaluarii riscurilor
- Controlul accesului = se refera la procesul de control al accesului la sisteme, retele si informatii pe baza cerintelor de securitate
- Bunuri informationale = definesc bucati de informatii in orice forma, inregistrate sau stocate pe orice mediu si care sunt recunoscute ca fiind “valoroase” pentru institutie

- Politica de securitate = reprezinta o directie propusa si adoptata destinata sa influenteze si sa determine deciziile si actiunile dintr-o institutie tinand cont de amenintarile de securitate

- Planul de securitate = reprezinta setul de actiuni si proceduri necesare implementarii politicii de securitate adoptate.

ANGAJAMENTE SI RESPONSABILITATI

Persoanele interesate de realizarea si implementarea politicilor de securitate ar trebui sa fie managerii executivi si managerii IT.

Toti angajatii dar si celelalte tipuri de utilizatori ai informatiilor institutiilor sunt obligati sa ia la cunostinta politicile si planul de securitate si sa-si asume respectarea intocmai a celor prevazute pentru departamentul sau categoria de personal din care fac parte.

ANALIZA RISCURILOR

O analiza a riscurilor este un proces de identificare a resurselor informatice ce au nevoie de protectie, de intelegere si documentare a riscurilor potentiale la nivelul IT sau la alte niveluri si care pot duce la pierdere confidentialitatii, a integritatii sau a disponibilitatii informatiilor.

Scopul evaluarii riscurilor este de a ajuta managementul sa creeze strategii si controale adecvate pentru o buna gestionare a bunurilor informationale. Pentru ca exista unii factori in continua schimbare trebuie sa gaseasca mecanisme de identificare si rezolvare a acestor riscuri asociate schimbarilor.

CLASIFICAREA INFORMATIILOR

- **Confidentiala** - se refera la informatiile care daca ar ajunge la dispozitia

persoanelor neautorizate, ar provoca pierderi imense institutiei, angajatilor sau partenerilor acelei institutii. Exemplu: date personale - CNP, IBAN, data nasterii, date medicale, unele informatii din unele contracte, etc. Datele din aceasta categorie trebuiesc utilizate exclusiv in interiorul institutiei si numai de catre persoanele care au nevoie de ele in interes de serviciu.

- **Interna / privata** - informatia de uz intern trebuie "**imprejmuita**" luand in considerare autorii, proprietarii, etica si datele private continute. Desi de obicei acest tip de informatie nu este protejata de statut, regulamente sau alte obligatii legale, utilizarea, accesul, difuzarea, achizitia, modificarea, pierderea sau stergerea neautorizata a informatiei de acest tip poate cauza pierderi financiare importante, o pierdere importanta la nivelul increderii / reputatiei, sau violarea drepturilor individuale ale angajatilor, partenerilor, studentilor, etc. Informatia de uz intern este informatia ce trebuie utilizata de angajati, furnizori si parteneri respectand un acord de "**ne-difuzare**" a acesteia.

- **Publica** - in aceasta categorie intra:

  i. in primul rand informatiile prin care acea institutie isi face publicitate;

  ii. informatia care desi nu este diseminata public, este destinata publicului larg (Ex.: statutul de student / angajat al unor persoane sau de partener al acelei institutii)

  iii. orice informatie care nu a fost clasificata drept confidentiala, interna / privata;

Acest tip de informatie (publica) poate fi accesata atat din interiorul institutiei cat si din afara ei, indiferent de suportul pe care ea este prezentata. Accesul la acest tip de informatii nu provoaca pierderi financiare sau de reputatie si nici nu pune in pericol activele institutiei.

Datele din categoria celor publice pot fi supuse procedurilor de revizuire pentru reducerea riscului pentru ca ele sa fie diseminate sau divulgate intr-un mod inadecvat.

PRINCIPII GENERALE IN ELABORAREA POLITICII DE SECURITATE

- Ar trebuie sa plecam de la ipoteza ca oricat de prevazatori si procedurali am fi, un incident de securitate IT tot vom avea (macar o data). Ar trebui deci, sa cautam cai prin care sa scadem probabilitatea de aparitie, sa minimizam dimensiunile unui astfel de incident precum si sa impingem aparitia acelui incident cat mai departe in timp;

- Fiind vorba de colectii de reguli coercitive, trebuie sa luam in calcul gradul ridicat de insatisfactie ce poate aparea la unii din cei vizati de planul si politica de securitate. Daca este prea grea (complexa), multi vor incerca sa o ocoleasca;

- Rata de evolutie a riscurilor are o dinamica ridicata si ele trebuiesc reanalizate periodic, independent de rata de evolutie a firmei / institutiei;

- Daca va afecta in mod negativ productivitatea, ea va esua;

- Trebuie sa exprime clar ce se poate si ceea ce este interzis pe echipamentele institutiei; Trebuie evitat jargonul sau descrierile complexe dar, totodata, trebuie sa fie cat mai cumprinzatoare posibil;

- Trebuie sa contina o fraza de tipul: “Angajatii nu au voie sa descarce jocuri, wallpaper-e, screen-saver-e, imagini, clipuri video, sau ***orice alt fel de aplicatii sau fisiere multimedia***. Ceea ce este scris cu caractere italice trebuie sa acopere tot ce nu a fost explicit specificat in enumerarea anterioara.

- Trebuie sa acopere toate departamentele si toata ierarhia administrativa; Ea trebuie sa fie asumata, respectata si sprijinita pornind de la cel mai inalt nivel (nu se accepta standarde duble)

- Trebuie sa contina clauze ce sa specifice clar consecintele cu care se vor confrunta in cazul nerespectarii politicii de securitate;

- Trebuie actualiazata in concordanta cu noile tehnologii (Ex.: medii de stocare USB, dispozitive mobile de tip smart;
- Se recomanda avizul unui avocat prin care sa se ofere garantia ca politica respectiva respecta legislatia in vigoare si nu incalca nici unul din drepturile celor vizati de ea.

PRINCIPII DE CARE SE TINE CONT IN ELABORAREA PLANULUI DE SECURITATE

- politica de securitate
- utilizarea acceptabila a resurselor IT
- se face un inventar pentru a putea raspunde la urmatoarele intrebari:
    - ce tipuri de informatii exista si unde ?
    - cum sunt folosite si protejate informatiile ?
    - cine are acces la informatii si in ce circumstante ?
- se creeaza mai multe niveluri de securitate
    - accesul fizic
    - securizarea retelei la nivelul 2 + 3
    - securizarea serverelor / website-urilor
    - securizarea statiilor de lucru
    - securizarea la nivelul utilizatorilor
- se creaza proceduri de detectie a incidentelor
- proceduri de backup al datelor si, uneori,chiar al echipamentelor
- se creeaza planuri de recuperare in caz de pierderi / furt de date, de dezastre
- se antreneaza angajatii pentru recunoasterea, raportarea si (non)actiunea in cazuri de:
    - social engineering

    - phishing
    - fraude online
    - falsi antivirusi
    - spyware, adware, malware in general
    - software malitios
    - cererea de date de identitate prin telefon
- securitatea la nivel internet (set de reguli pentru o navigare sigura) si a serviciilor de tip cloud
- politica parolelor puternice si atimpului de expirare a lor
- securizarea si criptarea retelei wireless; izolarea vizitatorilor de angajati
- politica de update-uri ale OS-urilor dar si a plicatiilor
- daca accesul de la distanta este permis, asigurati-va ca este sigur (Ex. VPN + autentificare in doi pasi)
- utilizarea doar a mediiilor de stocare USB inventariate si verificate ca fiind “sigure”
- utilizarea email-urilor (dezvoltarea unei politici specifice)
    - asigurarea unui filtru anti-spam
    - instruirea angajatilor in vederea utilizarii responsabile a email-ului
    - protejarea informatiilor sensibile trimise prin email
- dispozitive mobile
    - utilizarea programelor de securitate
    - actualizari la zi
    - criptarea datelor
    - utilizarea unor parole de acces puternice
    - proceduri in cazul pierderii / furtului
    - asigurati-va ca toate dispozitivele sunt curate (wiped) inainte de a fi eliminate din uz

- angajatii
    - asigurarea trierii la angajare
    - controale de fond si de acces
    - relatiile cu tertii
    - instruiri periodice
    - checklist-uri
- securitatea facilitatilor
    - protejarea materialelor tiparite cu informatii sensibile
    - securitatea corespondentei clasice (posta, firme de curierat)
    - distrugerea deseurile ce contin date sensibile (hartie, alte medii de stocare, echipamente electronice, etc.)
- proceduri operationale
    - identificarea informatiilor critice
    - analiza si evaluarea riscurilor
    - analiza vulnerabilitatilor
- raspunsul la incidente
    - notificarea autoritatilor daca este necesara
    - coerenta intre echipele tehnice si de conducere
    - inceperea procedurilor de recuperare
    - tinerea unei sedinte pentru a se invata din greseli

CONCLUZII

Daca persoanele incluse in politica de securitate vor constientiza de ce politica de securitate a institutiei respective este atat de importanta, ele o vor accepta si o vor pune in aplicare cu o mult mai mare usurinta.

- **DE CE ?**

i. Informatia este un bun - astazi, informatiile se afla in centrul afacerii

Care este cel mai greu lucru cu care se confrunta managerii zilnic ?

“luarea deciziilor”

Care este cel mai de pret ajutor pe care il pot obtine managerii in luarea deciziilor ? **“Informatii potrivite (la momentul potrivit)”**

Este nevoie ca mai intai informatiile sa fie **“colectate”** iar mai apoi **“protejate”**.

ii. Implicatiile lipsei de securitate in privinta informatiilor includ:

a) Pierderi **financiare** (pierderi in tranzactiile curente)

b) Pierderi in **justitie** (ne-respectarea acordurilor contractuale, a drepturilor intelectuale, a confidentialitatii datelor)

c) Pierderi **intangibile** - cum putem masura costul ne-increderii (intern + extern); dar costul pierderii intimitatii ?

……..

n) Pierderea **avantajului competitional** (in afaceri, educatie, cercetare, etc)

iii. Politica de securitate - defineste cerinte specifice ce trebuiesc indeplinite pentru a proteja bunurile informationale.

- confidentialitate = cine poate accesa informatia

- integritate = cum / cand poate fi alterata informatia

- disponibilitate = cum / cand poate fi accesata informatia

Raspunsul la intrebarea **“De ce avem nevoie de o politica de securitate ?”** defineste ceea ce este **“sigur”** pentru un sistem / set de sisteme si sta la baza securitatii informatiei.

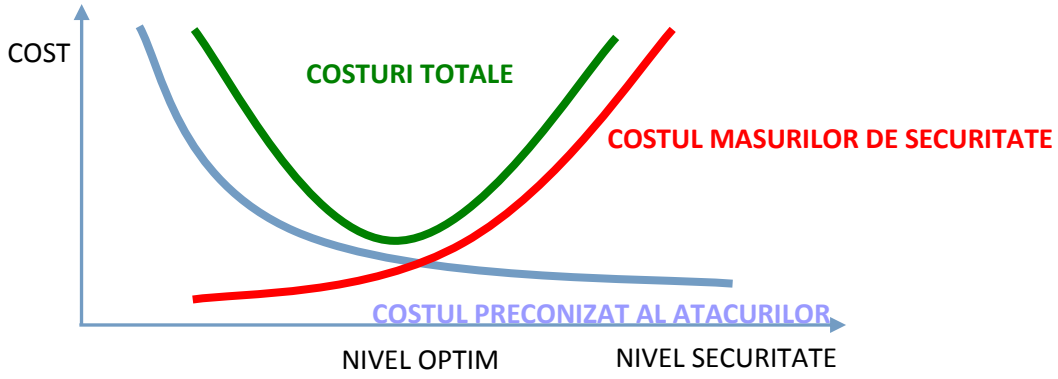
Dar ce facem cu **“afacerea”** ?

Balanta corecta:

- pentru oamenii de securitate: securitatea este o “necesitate” ! Indiferent de ce !

- pentru oamenii de afaceri: securitatea este un “cost” ! Si nimic altceva !

Ca de obicei, balanta este pe undeva pe la mijloc.



Sursa: A Structured Approach to Computer Security, T. Olovsson,

Cuantificarea costurilor

Cum masuram costurile masurilor de securitate ?

- ce trebuie protejat ?
- cum trebuie protejat ? (nu doar prin tehnologie!)

Cum masuram costurile eventualelor atacuri ?

- cunoasterea amenintarilor
- valoarea bunurilor informationale

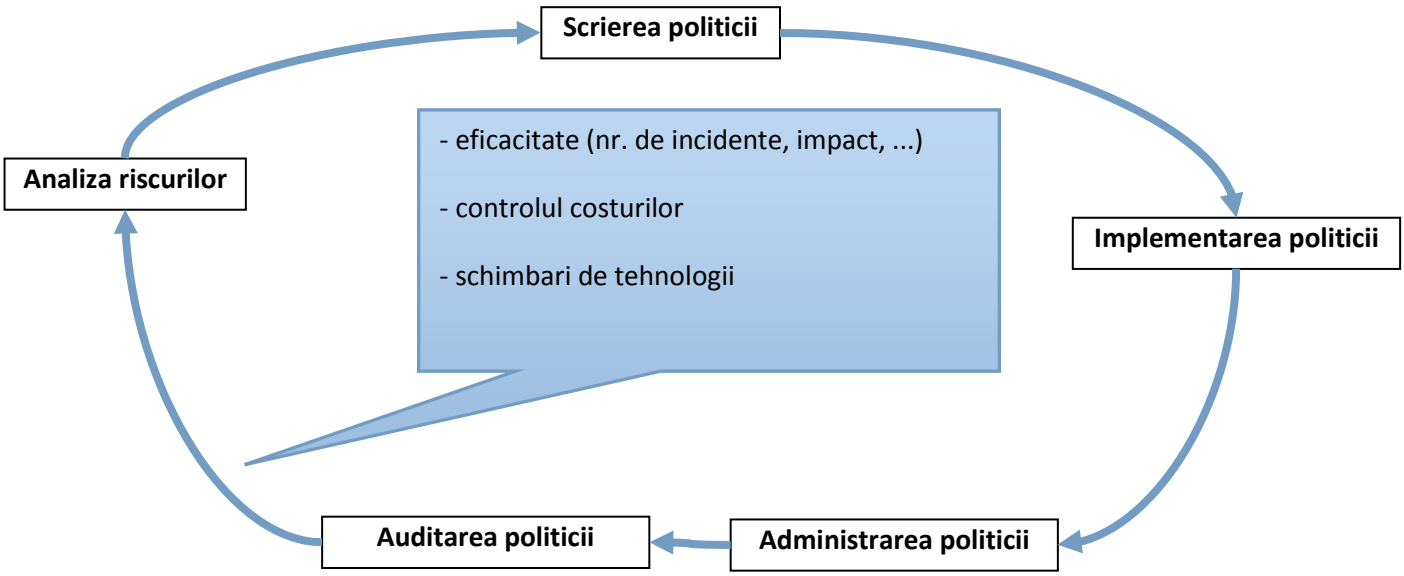
Stabilirea obiectivului

(si nu este numai o problema tehnica)

Costuri ascunse rezultate din:

- ineficienta
- protectii excesive
- pierderi ale unor oportunitati
- ... cel mai bun rezultat se obtine cand nu se intampla nimic.

O abordare eficienta:



Cum se elaboreaza politicile ?

- se dezvolta pornind de la veriga cea mai slaba (se are intotdeauna omul in minte)

- importanta procedurilor (cineva a facut-o si functioneaza, oamenii stiu ce sa faca, auditul se face mai usor)

- se dezvolta la nivelul institutiei (se explica de ce, nu cum; se arata importanta institutiei / afacerii);

- se evita problemele operationale (standarde si proceduri pentrua aceasta);

- se fac usor accesibile si disponibile;

- se auditeaza, se evalueaza, se schimba (ciclic)

- un singur pas la un moment dat

Daca politicile sunt formulate corect si integrate cu grija in contractele de munca, eventuale incalcari ale politicii, cum ar fi navigarea pe site-uri de socializare sau avand continut pentru adulti prin reteaua institutiei, pot fi pedepsite in conformitate cu un acord prestabilit, semnat de catre toti angajatii. O politica de securitate serveste astfel drept o masura prin care un comportament corespunzator poate fi testat si, eventual, pedepsit.

Plecand de la ideea ca “**scopul este sa perfectam activitatea institutiei**” sau “**scopul este sa facem business** ” , putem desprinde urmatoarele idei:

- politica de securitate trebuie sa permita, nu sa interzica;

- politica si planul de securitate trebuie sa faca lucrurile mai usoare, nu mai grele;

- securitatea necesita eforturi si investitii

- este nevoie de timp, este greu, rezultatele nu vor veni curand, dar

- ..... securitatea ofera rezultate ! **Rezultatele asteptate !**