



Cursul universitar

Gestiunea securității informatice

Lidia Popov, dr., lect. univ.

Aspectul organizatoric de asigurare a securității informaționale



Plan

1. Măsurile administrative de protecție a informației

- 1.1. Politica de securitate
- 1.2. Obiectivele fundamentale ale politicii de securitate
- 1.3. Caracteristici ale politicii de securitate
- 1.4. Publicul politicii de securitate
- 1.5. Tipuri de politici de securitate
- 1.6. Procesul dezvoltare a politicilor
- 1.7. Schița documentului politicii de securitate
- 1.8. Planul de securitate

2. Măsurile procedurale de protecție a informației

- 2.1. Managementul personalului
- 2.2. Protecția fizică
- 2.3. Menținerea capacității de funcționare
- 2.4. Reacția la eventualele încălcări
- 2.5. Planificarea lucrărilor de recuperare



Măsuri administrative de protecție a informației



Introducere

Asigurarea securității informațiilor nu este o problemă unidimensională, iar protecția informației la o companie poate fi realizată acționând pe trei dimensiuni – nivelul legislativ, nivelul organizatoric și nivelul tehnic, care împreună pot asigura protecția informației și a sistemelor informatice împotriva influențelor dăunătoare ce afectează subiecții relațiilor informaționale.

Măsurile organizatorice reprezintă una dintre pietrele de temelie ale procesului de asigurare a nivelului corespunzător de protecție a informației la o companie. Aceste măsuri constau din măsuri administrative și măsuri procedurale.



Măsurile administrative de securitate a informațiilor sunt acțiuni generale luate de conducerea organizației referitor la securitatea informației în cadrul acestei organizații. Scopul principal al acestor măsuri este elaborarea unui plan de securitate și asigurarea punerii lui aplicare, alocarea resurselor necesare, precum și monitorizarea continuă a acestui plan. Fundamentul planului de securitate îl reprezintă politica de securitate.



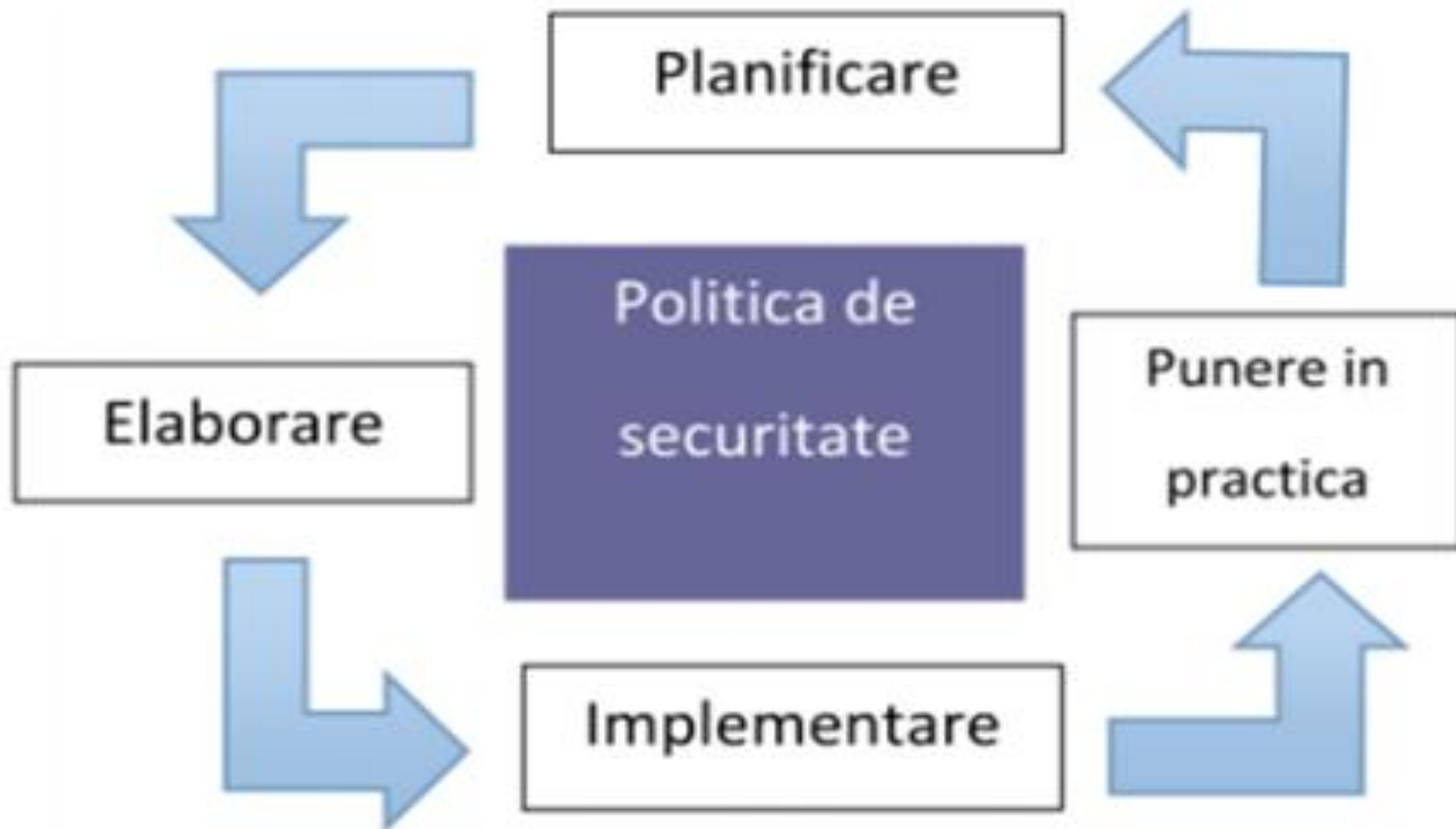
Politica de securitate

Politica de securitate este un set de decizii documentate luate de conducerea organizației pentru a asigura securitatea informațiilor. Politica de securitate reflectă abordarea organizației a procesului de protecție a activelor informaționale ale ei și poate fi considerată o strategie a companiei în domeniul securității informațiilor. Pentru a dezvolta o strategie și a o pune în aplicare sunt necesare, desigur, unele decizii politice luate la nivelul conducerii de vârf a acestei companii.

Securitatea IT se realizează prin implementarea unui set adecvat de politici, de proceduri, și de măsuri atât la nivel software cât și la nivel hardware pentru toate structurile organizatorice. Toate acestea trebuie stabilite, implementate, monitorizate, revizuite și îmbunătățite pentru a se asigura securitatea la acest nivel precum și pentru ca obiectivele economice să poată fi atinse. Așadar elaborarea unei bune politici de securitate trebuie privită ca un proces continuu și nu ca o acțiune.



Cele menționate anterior se reflectă în această imagine



Politicile de securitate servesc drept ghiduri generale pentru utilizarea, prelucrarea și managementul informațiilor.

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 de lucru restrâns, 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.

Politica de securitate

Dimensiunea și forma politicilor de securitate a informațiilor pot varia foarte mult de la companie la companie. Acest lucru poate depinde de numeroși factori, inclusiv de mărimea companiei, de sensibilitatea informațiilor gestionate referitoare la afacerile ei, precum și de varietatea și de tipurile sistemelor informatice și a sistemelor de calcul pe care le utilizează. Pentru o companie mare elaborarea unui document unitar al politicii de securitate, care să se adreseze tuturor tipurilor de utilizatori din cadrul ei și care abordează toate problemele necesare de securitate a informațiilor, se poate dovedi imposibilă.


Un concept mai eficient este de a dezvolta o suită de documente ale politicii care să acopere toate elementele ce asigură securitatea informațiilor, rezultând în final un proces mai eficient pentru întreaga companie.



Politica de securitate

Trebuie remarcat faptul că nu există o singură metodă pentru elaborarea unei politici sau a politicilor de securitate. Trebuie de luat în considerare mai mulți factori, inclusiv tipul de audiență și dimensiunea companiilor. Un alt factor este maturitatea procesului de elaborare a politicilor în vigoare - o companie care nu are în prezent o politică de securitate a informațiilor sau are doar o politică de bază generalizată poate să utilizeze inițial o strategie diferită față de o companie care are deja un concept substanțial al politicii, dar dorește să-l consolideze și să înceapă să folosească politica de securitate în scopuri mai complexe, de exemplu pentru a fi în acord cu legislația.

La început, ar fi o idee bună, pornind de la un cadru de bază a politicii, să se aplice o abordare pe etape, prin elaborarea politicilor necesare majore și apoi prin dezvoltarea unui număr mai mare de politici, prin revizuirea celor deja existente și prin adăugarea la ele a unor instrucțiuni și a documentelor Job Aids însoțitoare, care vor contribui în calitate de suport la realizarea politicii.



Obiectivele fundamentale ale politicii de securitate

O politică de securitate îndeplinește următoarele obiective:

Protejarea persoanelor și a informațiilor;

Stabilirea regulilor pentru comportamentul necesar utilizatorilor, administratorilor de sistem, managerilor și a personalului ce se ocupă de securitate;

Autorizarea personalului de securitate pentru monitorizare, sondare și investigare;

Definirea și aprobarea consecințelor încălcării cerințelor politicii de securitate;

Definirea poziției unanime de bază a companiei privind securitatea;

Ajutorul la minimizare a riscurilor;

Asigurarea respectării reglementărilor și a legislației.

Obiectivele fundamentale ale politicii de securitate

Politica de securitate ar trebui să fie un instrument util pentru protecția securității companiei, ca un ghid și o sursă de informație la care toți utilizatorii se vor adresa în munca lor de zi cu zi. Cu toate acestea, deseori politicile de securitate pot ajunge pur și simplu niște appendice inutile, puțin citite, utilizate sau chiar cunoscute de utilizatori și deconectate de restul politicilor și practicilor de securitate ale companiei, iar ca acest lucru să nu se întâmple politicile trebuie să fie realizabile.



Caracteristici ale politicii de securitate

Cheia pentru a ne putea asigura că *politica de securitate* a companiei este una utilă și utilizabilă este ca ea să fie direct conectată la politicile existente ale companiei și să fie dezvoltată o suită de documente de politici care să se potrivească cu publicul respectiv.

Politicile trebuie să fie folositoare, viabile și realiste. Pentru a realiza acest lucru, este esențială implicarea și suportul actorilor majori în dezvoltarea și susținerea politicilor (cum ar fi managerii superiori, auditorii și juriștii), precum și acelor persoane care vor trebui să utilizeze politicile ca parte a muncii de zi cu zi (cum ar fi experții în materie, administratorii de sistem și utilizatorii finali).



Caracteristici ale politicii de securitate

Pentru a realiza acest lucru, un element important ar fi să se aducă la cunoștință despre importanța și utilitatea politicilor celor care trebuie să urmeze prevederile acestor politici. Adesea utilizatorii par să creadă că politica este ceva care va sta în calea muncii lor zilnice.

Un element important de elaborare a politicilor și de asigurare a aplicării politicilor (și nu de respingere a lor) de către utilizatori este de a face astfel încât să fie clar că politicile le sunt utile. Pentru aceasta, dar și pentru a fi siguri că utilizatorii se vor conforma cerințelor legale, este necesar să li se ofere un cadru, o recomandare pentru cele mai bune practici, bazându-se pe care cu toții își vor putea îndeplini obligațiunile de serviciu.



Caracteristici ale politicii de securitate

Odată ce utilizatorii își vor da seama că *politica este ceva care de fapt le poate ajuta în munca lor*, ei vor fi mult mai receptivi în respectarea acesteia, dar și în acordarea unui suport în scopul dezvoltării politicii.

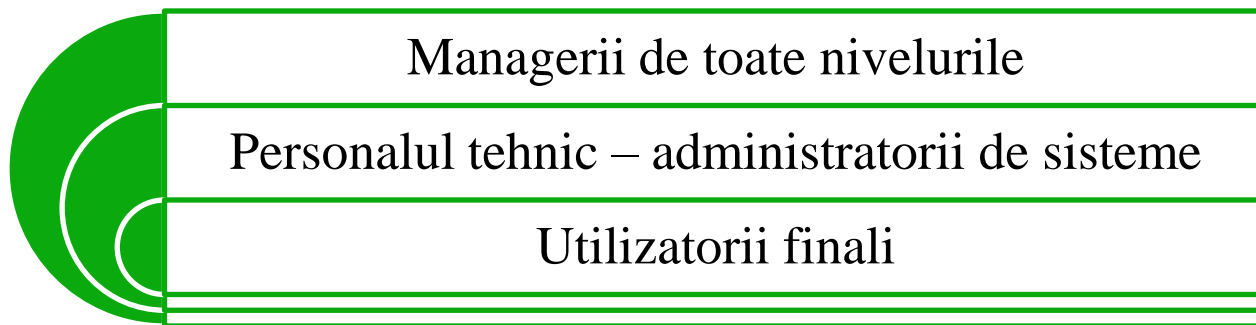
În mod similar, odată ce managerii de rang înalt își dau seama că politica este un instrument pe care ei îl pot folosi pentru a asigura respectarea cerințelor legislative și pentru a promova inițiativele noi atât de mult necesare, ei vor susține tot mai mult politica cu suportul financiar și cu alte resurse necesare, devenind ei înșii promotorii politicii de securitate.



Publicul politicii de securitate

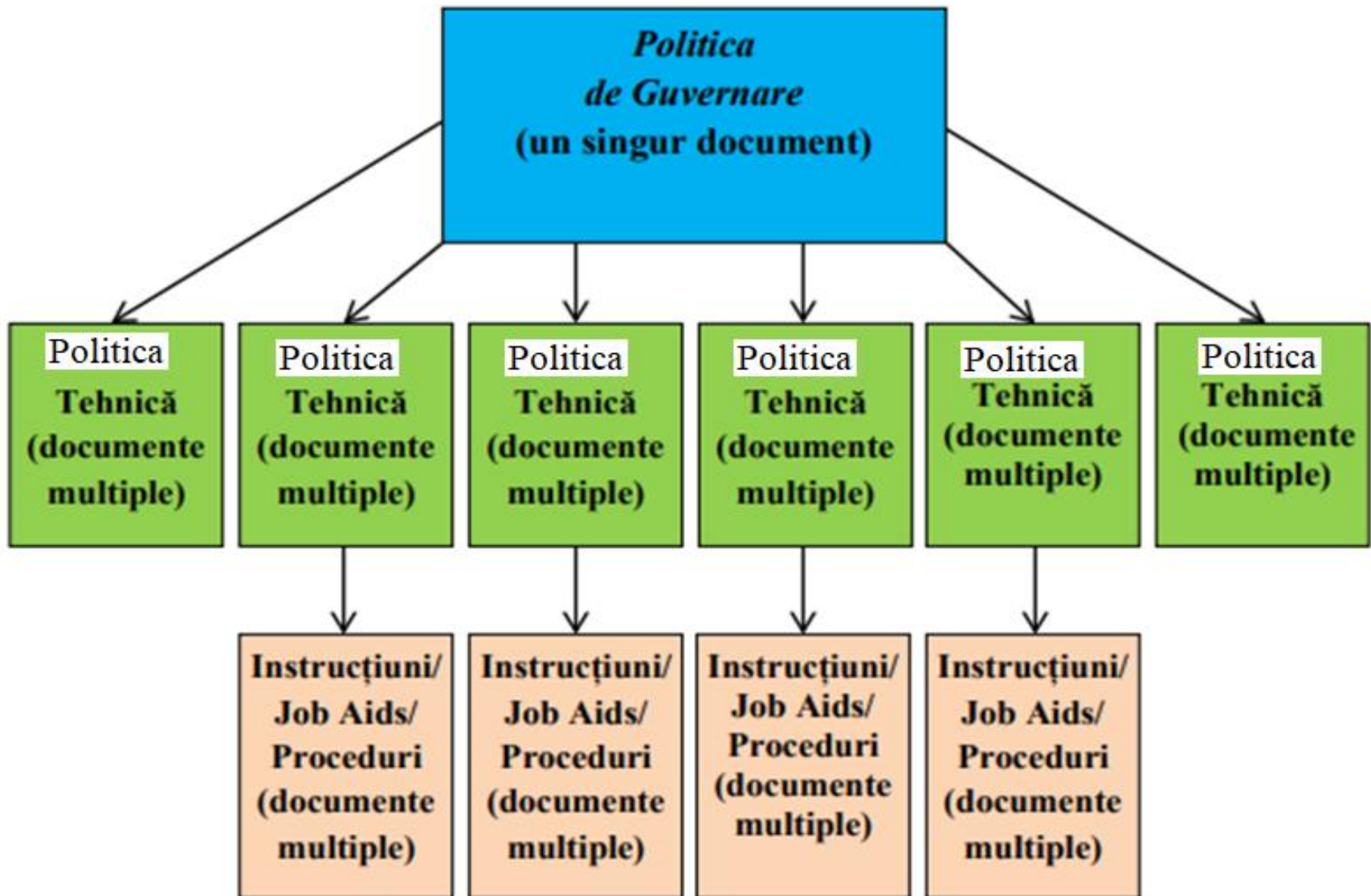
Politicile de securitate sunt destinate, desigur, tuturor angajaților companiei, însă acest grup mare poate fi împărțit în subcategorii ale publicului politicii în conformitate cu cerințele comune impuse de politica de securitate.

Principalele grupuri de acest fel sunt:



Fiecare utilizator se va regăsi obligatoriu în cel puțin unul dintre aceste grupuri (utilizatorul final fi numai în unul din grupuri), iar unii se vor regăsi în două sau chiar în toate trei, iar fiecare document al politicii va fi elaborat în funcție de publicul căruia îi este destinată politica

Tipuri de politici de securitate



Tipuri de politici de securitate

O posibilitate de realizare a politicilor de securitate a informației este de a le structura ierarhic. Ierarhizarea face posibilă o abordare eficientă a politicilor pentru toate grupele de angajați – utilizatorii politicilor de securitate. Acesta este un model de ierarhie a politicilor de securitate a informației care poate fi personalizat pentru a corespunde cerințelor oricărei companii. Pe de altă parte aceasta este o ierarhie pentru un proces destul de matur și bine pus la punct, destinat mai degrabă unei companii mari, unde dezvoltarea politicii a fost susținută pe parcursul mai multor ani.

Pentru companiile mai mici sau pentru cei care abia încep să elaboreze o politică de securitate, la fel este posibil să se folosească modelul dat ca un cadru de bază, însă inițial ar trebui să conțină un număr mai mic de politici tehnice și, eventual, să nu existe instrucțiuni sau job-aids la începutul procesului de elaborare. În loc de încercarea de a dezvolta o ierarhie mare de la început, este mai realist să fie dezvoltată inițial o politică de guvernare și un număr redus de politici tehnice, apoi pe parcurs, să fie mărit numărul de politici și documente ajutătoare concomitent cu creșterea complexității acestor politici.

Tipuri de politici de securitate

Este evident că în companiile mari publicul, căruia îi este destinată *politica de securitate*, va fi mai divers și va fi necesar de a acoperi mai multe subiecte diferite la diferite niveluri. Din acest motiv, într-un mediu corporativ cel mai probabil va funcționa mai bine o suită de documente a politicii de securitate decât un document unitar voluminos.

Structura ierarhică a setului de documente a politicii de securitate reflectă structura ierarhică a rolurilor într-o companie mare. Schema propusă este destinată tuturor categoriilor de public și tuturor subiectelor, utilizând două tipuri de politici susținute în caz de necesitate de documente procedurale și anime:

1. Politica de Guvernare
2. Politica Tehnică
3. Job-aids/Instrucțiuni.



Tipuri de politici de securitate

Politica de Guvernare trebuie să acopere conceptele de securitate a informațiilor la un nivel înalt, să definească aceste concepte, să descrie de ce sunt importante și să detalieze în ele poziția companiei.

Politica de guvernare va fi citită de către managerii și utilizatorii finali. În mod implicit, va fi citită și de către consilierii tehnici (în special consilierii tehnici pe securitate), deoarece ei sunt și utilizatori finali. Toate aceste grupuri vor folosi politica pentru a înțelege mai bine filosofia generală a politicii de securitate a companiei.

Politica de guvernare ar trebui să fie strâns aliniată la HR (resursele umane) existente și viitoare, dar și la alte politici ale companiei, în special acelea în care sunt menționate aspecte legate de securitate, cum ar fi utilizarea e-mailului, mesageriei sau a computerului etc.

În ceea ce privește nivelul de detaliere, politica de guvernare ar trebui să abordeze așa numitul „ce” din punctul de vedere al politicii de securitate.



Tipuri de politici de securitate

Politicile Tehnice vor fi folosite de consilierii tehnici în timp ce își vor îndeplini responsabilitățile legate de securitate pentru sistemul cu care lucrează.

În ceea ce privește nivelul de detaliere, politica tehnică ar trebui să abordeze „**ce?**” (în mai multe detalii), „**cine?**”, „**când?**” și „**unde?**” din punctul de vedere al politicii de securitate.

Documentele de procedură (Job Aids, Instrucțiuni) oferă instrucțiuni detaliate privind modul în care se vor realiza cerințele politicilor. De exemplu, manualul pentru hardening al unui server Windows poate consta din unul sau mai multe documente suport pentru o Politică Tehnică Windows.

Politica le oferă documentelor de procedură un cadru care trebuie de urmat („**ce?**”, „**cine?**”, „**când?**” și „**unde?**” din punctul de vedere al politicii de securitate), iar ei, bazându-se pe acest cadru, pur și simplu trebuie să descrie „**cum?**”.



Procesul dezvoltare a politicilor

Raționamentul principal al *procesului de dezvoltare a politicilor* de securitate ale fiecărei companii va fi nivelul de maturitate al procesului. Este important ca companiile (mai ales cele mai mari) să nu aibă intenții imediate exagerate și să încerce să dezvolte rapid un program de politici cuprinzător și complex.

Este puțin probabil ca acest lucru să aibă succes din mai multe motive, printre care nevoia de un buy-in management, cultura și resursele nepregătite ale companiei etc. În această situație, este recomandabil să se înceapă inițial cu politicile mici, și cu un cadru-schelet al politicii de securitate care să conțină doar politicile esențiale care vor fi elaborate în primul rând. Pe măsură ce procesul crește în maturitate, companiile vor putea să dezvolte, atunci când apare necesitatea, întreaga gamă de politici cu mai multe detalii incluse în fiecare, precum și documentația procedurală însoțitoare.



Procesul dezvoltare a politicilor

Educația, conștientizarea și procesele de comunicare trebuie să devină „mature” pentru a face față promovării unei game tot mai variate de politici, ceea ce ar trebui să coincidă cu sporirea puterii corporative a politicilor în sine. Atunci cultură corporatistă va începe să aprecieze că politicile trebuie urmate și respectate, și de fapt ar putea să înceapă să le utilizeze pentru a impulsiona unele modificări necesare în întreaga companie.

Apare însă o întrebare foarte importantă: de unde totuși e mai bine de început procesul de elaborare a unei politici de securitate, deoarece există mai multe puncte de pornire: legislația nou adoptată poate fi adesea un impuls puternic pentru dezvoltarea politicii, la fel ca și recente incidente de securitate sau administratorii entuziaști care s-au întors recent de la un nou curs de formare. Toate acestea oferă o mare contribuție politicii de securitate, dar cheia spre elaborarea unei politici funcționale este să realizăm un echilibru între toate aceste aspecte



Procesul dezvoltare a politicilor

Bazându-ne exclusiv pe abordarea „*de sus în jos*” prin utilizarea doar a legislației, a regulamentelor și a celor mai bune practici pentru a scrie o politică, rezultatul ar putea fi o politică nerealistă și artificială care nu va fi funcțională în lumea reală.

În mod similar, bazându-ne doar pe o metodă „*de jos în sus*”, axată numai pe cunoștințele administratorului de sistem, am putea elabora o politică prea specifică unui anumit mediu (poate doar pentru o parte dintr-o companie mare), posibil bazată prea mult pe practicile locale curente sau pe cele mai recente sugestii de la cursurile formare, făcând-o prea nerealistă.

Cea mai bună politică va proveni dintr-o combinație a acestor abordări, atât „*de sus în jos*”, cât și „*de jos în sus*”.



Schița documentului politicii de securitate


Fiecare politică de securitate ar trebui să includă așa compartimente ca *Politica de Guvernare*, *Politicile tehnice*, *Documentele de procedură*, și în plus față acestea trebuie să mai conțină neapărat încă câteva secțiuni: introducerea, scopul, domeniul de aplicare, rolurile și responsabilitățile, sancțiunile și încălcările, programul de revizuire și actualizare, informațiile de contact, definițiile și acronimele.



Planul de securitate

Planul de securitate este dezvoltat în baza politicii de securitate. În cadrul acestui plan sunt alocate resursele, numiți responsabili, stabilită ordinea de execuție și control, etc. În baza planului de securitate sunt elaborate norme specifice, regulamente și recomandări pentru activitatea personalului responsabil de securitatea informațiilor. Aceste norme se referă la măsurile procedurale de protecție a informației.

Un plan de securitate împreună cu politica de securitate din care acesta a rezultat sunt proiectate pentru a proteja atât informațiile cât și resursele materiale critice de la o gama larga de amenințări în scopul de a asigura continuitatea activității instituției, de a reduce riscul în afaceri, de a maximiza randamentul investițiilor și a oportunităților de afaceri. ***Scopul planului de securitate*** este să asigure confidențialitatea, integritatea și disponibilitatea datelor, să definească, să dezvolte, și să documenteze politicile și procedurile de informare ce vin în sprijinul scopului și obiectivelor instituției precum și să permită instituției să îndeplinească din punct de vedere legal și etic responsabilitățile cu privire la resursele IT.



Măsuri procedurale de protecție a informației



Măsuri procedurale de protecție a informației

Măsurile procedurale de securitate a informațiilor reprezintă ansamblul reglementărilor prin care se stabilesc măsurile interne de lucru și de ordine interioară destinate realizării protecției informațiilor, acestea fiind măsurile de securitate implementate de oameni.

Aceste măsuri, care se concretizează în diverse norme specifice, regulamente și recomandări pentru activitatea personalului responsabil de securitatea informațiilor, sunt elaborate în baza planului de securitate.



La nivelul procedural de asigurare a securității informațiilor se pot distinge următoarele clase de măsuri:

Managementul personalului;

Protecția fizică;

Mentținerea capacității de funcționare;

Reacționarea la încălcări ale securității;

Planificarea lucrărilor de recuperare.

Managementul personalului

Managementul personalului începe cu admiterea unui nou angajat la serviciu și chiar mai devreme – cu elaborarea fișei postului. Există două principii generale care trebuie luate în considerare: divizarea sarcinilor și minimizarea privilegiilor.

Principiul separarea atribuțiilor prescrie alocarea de roluri și responsabilități astfel încât o persoană să nu poată întrerupe un proces de o importanță critică pentru companie.

De exemplu, nu este de dorit ca transferurile mari de bani ale companiei să fie efectuate de o singură persoană. Este mai sigur să-i fie încredințată unui angajat procesarea cererilor pentru astfel de plăți, iar altuia – să certifice aceste cereri.



Managementul personalului

Principiul minimizării privilegiilor prevede acordarea utilizatorilor doar a drepturilor de acces care sunt necesare pentru ca aceștia să-și îndeplinească atribuțiile oficiale. Scopul acestui principiu este evident de a reduce prejudiciul cauzat de comportamentul greșit, fie el accidental sau intenționat.

Elaborarea preliminară a fișei de post permite evaluarea criticității acesteia și planificarea procedurii de verificare și selectare a candidaților. Din momentul în care unui nou angajat i se oferă accesul la sistemul informatic, este necesar de a realiza administrarea contului său de sistem, de a contabiliza și analiza acțiunile efectuate de acesta în scopul de a identifica situațiile suspecte.

Atunci când un angajat este concediat, mai ales în cazul unui conflict între el și administrație, este necesar ca în regim de urgență acesta să fie lipsit de drepturile de acces la sistemul informatic al companiei, prin transferul de echipament și împuterniciri către alt angajat

Protecția fizică

Securitatea sistemului informatic depinde în primul rând de mediul în care acest sistem funcționează. De aceea este necesar să se ia măsuri pentru a proteja clădirile și teritoriile adiacente, infrastructura, calculatoarele, mediile de stocare a datelor, etc.

Principiul de bază al protecției fizice, a cărui respectare ar trebui să fie monitorizată în mod continuu, poate fi formulat ca „*continuitatea protecției în timp și spațiu*”.

Putem distinge câteva categorii de protecție fizică: controlul accesului fizic; măsuri de combatere a incendiilor; protecția infrastructurii de suport; protecția împotriva interceptării datelor; protecția sistemelor mobile.



Mentținerea capacității de funcționare

Mentținerea capacității de funcționare a sistemelor informatice este fără îndoială vitală, mai ales dacă luăm în considerare faptul că software-ul este unul dintre cele mai importante mijloace de asigurare a integrității informațiilor. Mai întâi de toate, trebuie să putem urmări ce software este instalat pe calculatoare, deoarece în cazul în care utilizatorii îl vor instala la discreția sa, aceasta poate duce la infectarea sistemului, precum și la apariția unor căi de ocolire a instrumentelor și mijloacelor de securitate existente în companie.

Alt aspect ține de suportul continuu în scopul de a asigura lipsa modificărilor neautorizate a software-ului și a drepturilor de acces la acesta. În mod normal controlul funcționalității sistemelor poate fi realizat prin combinarea mijloacelor de control al accesului fizic și logic, precum și utilizarea software-ului utilitar de verificare și asigurare a integrității.

Reacția la eventualele încălcări

Reacția la încălcările regimului de securitate a informațiilor are următoarele obiective: localizarea incidentelor și reducerea riscurilor; identificarea intrușilor; prevenirea încălcărilor repetate. În cazul unei încălcări a regimului de securitate, trebuie imediat luate măsuri, iar succesiunea acțiunilor pentru astfel de cazuri este foarte important să fie planificată în avans și reflectată în documente.

Toți angajații ar trebui să cunoască cum să acționeze și pe cine să contacteze în cazul detectării unei încălcări a securității, precum și să știe ce consecințe îi așteaptă pe ei înșiși în cazul în care vor încălca *regulile de securitate a informațiilor*.



Planificarea lucrărilor de recuperare

Planificarea lucrărilor de recuperare ne va permite să fim pregătiți pentru eventualele incidente ca să putem reduce în regim de urgență prejudiciile cauzate de acestea și să ne menținem capacitatea de a funcționa cel puțin la un nivel minim acceptabil.

Procesul de planificare a lucrărilor de recuperare poate fi realizat în câteva etape:

- ✓ identificarea funcțiilor de importanță critică ale companiei și stabilirea priorităților;
- ✓ identificarea resurselor necesare pentru îndeplinirea funcțiilor critice;
- ✓ definirea unei liste de accidente posibile;
- ✓ dezvoltarea unei strategii de recuperare;
- ✓ pregătirea pentru implementarea strategiei alese;
- ✓ verificarea strategiei.



Planificarea lucrărilor de recuperare

Un lucru foarte important aici este că atunci când planificăm lucrările de recuperare, trebuie să fim conștienți că nu este întotdeauna posibil să asigurăm imediat o funcționare completă a companiei și de aceea este necesar să se identifice funcțiile de importanță critică, fără de care compania își pierde identitatea.

Mai mult ca atât - aceste funcții, la fel, trebuiesc organizate în conformitate cu astfel de priorități, încât să fie posibil ca într-un timp cât mai scurt și cu costuri minime să fie reluată activitatea după fiecare accident petrecut.



Concluzii

Considerăm că nu ar fi corect să afirmăm că *măsurile organizatorice sunt cele mai importante măsuri în asigurarea securității informației* în cadrul unei companii, însă, cu certitudine, fără aplicarea lor celelalte categorii de măsuri nu își vor atinge scopul, făcând ca compania să rămână vulnerabilă pe diverse dimensiuni.

Este important precum ca conducerea de vârf a companiei să fie conștientă de necesitatea implementării măsurilor organizatorice și să insiste în această direcție, însă chiar având suportul total al conducerii este dificil de realizat instantaneu și corect toate măsurile administrative și procedurale de protecție a informației.



Concluzii

În primul rând trebuie de elaborat o politică de securitate, la început cu conținut estul de comun, iar pe parcurs în mod continuu de actualizat și completat cu diverse documente – componente ale politicii, astfel încât programul de securitate să fie unul care să poată fi realizat. Aceasta este chiar mai important decât a avea un program complet însă nerealizabil.

Concentrându-ne pe elaborarea politicii de securitate nu trebuie să uităm și de măsurile procedurale, fiindcă normele specifice, regulamente și recomandările cu aspect de securitate a informațiilor vor contribui esențial la realizarea programul de securitate.



Mulumim pentru atenție!

