E-ISBN 978-9975-75-901-4

ASPECTUL ORGANIZATORIC DE ASIGURARE A SECURITĂŢII INFORMAŢIONALE

Dr., conf. univ., Aureliu ZGUREANU

Academia de Studii Economice a Moldovei,
Republica Moldova, Chişinău, Bănulescu Bodoni, 61,
tel. (+373) 22 41 28, www.ase.md

Abstract

The process of information security assurance within an enterprise starts from planning the measures and methods which support this process. The administrative measures which must be taken by the company's management are found in the security policy. The correctness of this policy will ultimately influence the success of the business. The procedural measures are found in all the regulations establishing the internal working measures and the internal order of information security. These measures are implemented by the company staff.
Organizational measures, composed of administrative and procedural measures, are analysed in this paper. The analysis focuses on methodology development and proper implementation of security policy based on company size and level of development of security policy.

Key words: *information security policy, administrative measures, procedural measures.*

JEL CLASSIFICATION: D89, G18, L88

Asigurarea securităţii informaţiilor nu este o problemă unidimensională, iar protecţia informaţiei la o întreprindere poate fi realizată acţionând pe trei dimensiuni – nivelul legislativ, nivelul organizatoric şi nivelul tehnic, care împreună pot asigura protecţia informaţiei şi a sistemelor informatice împotriva influenţelor dăunătoare ce afectează subiecţii relaţiilor informaţionale.

Măsurile organizatorice reprezintă una dintre pietrele de temelie ale procesului de asigurare a nivelului corespunzător de protecţie a informaţiei la o întreprindere. Aceste măsuri constau din măsuri administrative şi măsuri procedurale.

1. MĂSURI ADMINISTRATIVE DE PROTECŢIE A INFORMAŢIEI

Măsurile administrative de securitate a informaţiilor sunt acţiuni generale luate de conducerea organizaţiei referitor la securitatea informaţiei în cadrul acestei organizaţii.

Scopul principal al acestor măsuri este elaborarea unui plan de securitate şi asigurarea punerii lui aplicare, alocarea resurselor necesare, precum şi monitorizarea continuă a acestui plan. Fundamentul planului de securitate îl reprezintă politica de securitate.

Politica de securitate este un set de decizii documentate luate de conducerea organizaţiei pentru a asigura securitatea informaţiilor. Politica de securitate reflectă abordarea organizaţiei a procesului de protecţie a activelor informaţionale ale ei şi poate fi considerată o strategie a întreprinderii în domeniul securităţii informaţiilor. Pentru a dezvolta o strategie şi a o pune în aplicare sunt necesare, desigur, unele decizii politice luate la nivelul conducerii de vârf a acestei întreprinderi.

Securitatea IT se realizează prin implementarea unui set adecvat de politici, de proceduri, şi de măsuri atât la nivel software cât şi la nivel hardware pentru toate structurile organizatorice. Toate acestea trebuiesc stabilite, implementate, monitorizate, revizuite şi îmbunătăţite pentru a se asigura securitatea la acest nivel precum şi pentru ca obiectivele economice să poată fi atinse. Aşadar elaborarea unei bune politici de securitate trebuie văzută ca un proces continuu şi nu ca o acţiune (fig. 1).

E-ISBN 978-9975-75-901-4

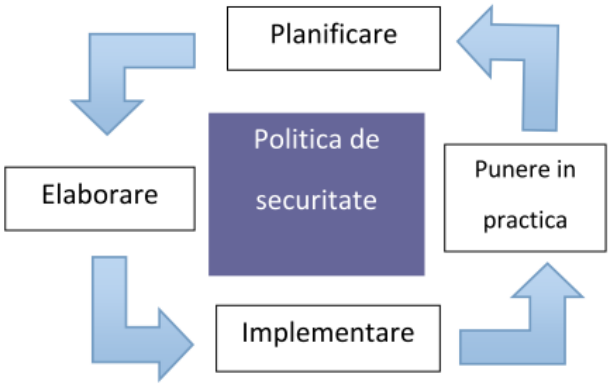

Figura 1. Procesul de elaborare a politicii de securitate

Politicile de securitate servesc drept linii directoare (ghiduri) generale pentru utilizarea, prelucrarea şi managementul informaţiilor.

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

- obiectivele organizaţiei privind securitatea: asigurarea protecţiei datelor împotriva scurgerilor de informaţii către entităţi externe, protejarea datelor faţă de calamităţile naturale, asigurarea integrităţii datelor sau asigurarea continuităţii afacerii;
- personalul răspunzător pentru asigurarea securităţii, care poate fi: un grup de lucru restrâns, un grup de conducere sau fiecare angajat;
- implicarea organizaţiei în ansamblu la asigurarea securităţii: cine va asigura instruirea în domeniul securităţii, cum va fi integrată partea de securitate în structura organizaţiei.

Dimensiunea şi forma politicilor de securitate a informaţiilor pot varia foarte mult de la companie la companie [1]. Acest lucru poate depinde de numeroşi factori, inclusiv de mărimea companiei, de sensibilitatea informaţiilor gestionate referitoare la afacerile ei, precum şi de varietatea şi de tipurile sistemelor informatice şi a sistemelor de calcul pe care le utilizează. Pentru o întreprindere mare elaborarea unui document unitar al politicii de securitate, care să se adreseze tuturor tipurilor de utilizatori din cadrul ei şi care abordează toate problemele necesare de securitate a informaţiilor, 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 informaţiilor, rezultând în final un proces mai eficient pentru întreaga companie.

Trebuie remarcat faptul că nu există o singură metodă pentru elaborarea unei politici sau a politicilor de securitate. Trebuie de luat în considerare mai mulţi factori, inclusiv tipul de audienţă şi dimensiunea întreprinderilor. Un alt factor este maturitatea procesului de elaborare a politicilor în vigoare - o companie care nu are în prezent o politică de securitate a informaţiilor sau are doar o politică de bază generalizată poate să utilizeze iniţial o strategie diferită faţă de o companie care are deja un concept substanţial al politicii, dar doreşte să-l consolideze şi să înceapă să folosească politica de securitate în scopuri mai complexe, de exemplu pentru a fi în acord cu legislaţia [3].

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 şi apoi prin dezvoltarea unui număr mai mare de politici, prin revizuirea celor deja existente şi prin adăugarea la ele a unor instrucţiuni şi a documentelor *Job Aids* însoţitoare, care vor contribui în calitate de suport la realizarea politicii.

O politică de securitate ar trebui să îndeplinească mai multe obiective şi anume:

- protejarea persoanelor şi a informaţiilor;
- stabilirea regulilor pentru comportamentul necesar utilizatorilor, administratorilor de sistem, managerilor şi a personalului ce se ocupă de securitate;
- autorizarea personalului de securitate pentru monitorizare, sondare şi investigare;
- definirea şi aprobarea consecinţelor încălcării cerinţelor politicii de securitate;

E-ISBN 978-9975-75-901-4

- definirea poziţiei unanime de bază a companiei privind securitatea;
- ajutorul la minimizarea riscurilor;
- asigurarea respectării reglementărilor şi a legislaţiei.

Politica de securitate ar trebui să fie un instrument util pentru protecţia securităţii întreprinderii, ca un ghid şi o sursă de informaţie la care toţi utilizatorii se vor adresa în munca lor de zi cu zi. Cu toate acestea, deseori politicile de securitate pot ajunge pur şi simplu nişte apendice inutile, puţin citite, utilizate sau chiar cunoscute de utilizatori şi deconectate de restul politicilor şi practicilor de securitate ale companiei, iar ca acest lucru să nu se întâmple politicile trebuie să fie realizabile.

Cheia pentru a ne putea asigura că politica de securitate a companiei este una utilă şi utilizabilă este ca ea să fie direct conectată la politicile existente ale companiei şi să fie dezvoltată o suită de documente de politici care să se potrivească cu publicul respectiv. Politicile trebuie să fie folositoare, viabile şi realiste. Pentru a realiza acest lucru, este esenţială implicarea şi suportul actorilor majori în dezvoltarea şi susţinerea politicilor (cum ar fi managerii superiori, auditorii şi juriştii), precum şi acelor persoane care vor trebui să utilizeze politicile ca parte a muncii de zi cu zi (cum ar fi experţii în materie, administratorii de sistem şi utilizatorii finali).

Pentru a realiza acest lucru, un element important ar fi să se aducă la cunoştinţă despre importanţa şi 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 şi de asigurare a aplicării politicilor (şi 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 şi pentru a fi siguri că utilizatorii se vor conforma cerinţelor legale, este necesar să li se ofere un cadru, o recomandare pentru cele mai bune practici, bazându-se pe care cu toţii îşi vor putea îndeplini obligaţiunile de serviciu.

Odată ce utilizatorii îşi 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 şi în acordarea unui suport în scopul dezvoltării politicii. În mod similar, odată ce managerii de rang înalt îşi dau seama că politica este un instrument pe care ei îl pot folosi pentru a asigura respectarea cerinţelor legislative şi pentru a promova iniţiativele noi atât de mult necesare, ei vor susţine tot mai mult politica cu suportul financiar şi cu alte resurse necesare, devenind ei înşii promotorii politicii de securitate.

Politicile de securitate sunt destinate, desigur, tuturor angajaţilor companiei, însă acest grup mare poate fi împărţit în subcategorii ale publicului politicii în conformitate cu cerinţele comune impuse de politica de securitate. Principalele grupuri de acest fel sunt: managerii – de toate nivelurile; personalul tehnic – administratorii de sisteme, etc.; utilizatorii finali. Fiecare utilizator se va regăsi obligatoriu în cel puţin 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 funcţie de publicul căruia îi este destinată politica [2].

Tipuri de politici de securitate. O posibilitate de realizare a politicilor de securitate a informaţiei este de a le structura ierarhic, aşa cum este arătat în figura 2 [3]. Ierarhizarea face posibilă o abordare eficientă a politicilor pentru toate grupele de angajaţi - utilizatorii politicilor de securitate. Acesta este un model de ierarhie a politicilor de securitate a informaţiei care poate fi personalizat pentru a corespunde cerinţelor oricărei companii. Pe de altă parte aceasta este o ierarhie pentru un proces destul de matur şi bine pus la punct, destinat mai degrabă unei companii mari, unde dezvoltarea politicii a fost susţinută 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 iniţial ar trebui să conţină un număr mai mic de politici tehnice şi, eventual, să nu existe instrucţiuni 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 iniţial o politică de guvernare şi un număr redus de politici tehnice, apoi pe parcurs, să fie mărit numărul de politici şi documente ajutătoare concomitent cu creşterea complexităţii acestor politici.

E-ISBN 978-9975-75-901-4

Este evident că în companiile mari publicul, căruia îi este destinată politica de securitate, va fi mai divers şi va fi necesar de a acoperi mai multe subiecte diferite la diferite niveluri. Din acest motiv, într-un mediu corporativ cel mai probabil va funcţiona 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 şi tuturor subiectelor, utilizând *două tipuri de politici* susţinute în caz de necesitate de *documente procedurale* şi anime: *Politica de Guvernare*, *Politica Tehnică*, *Job-aids*/*Instrucţiuni*.

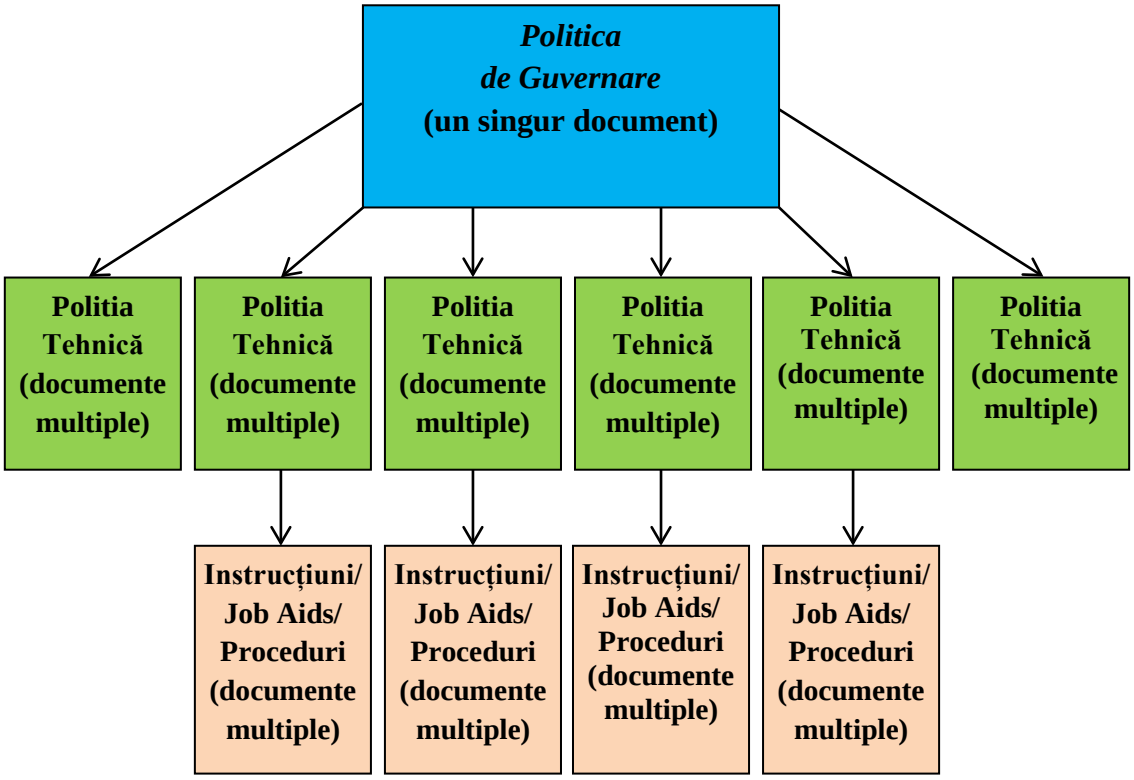

Figura 2. *Structura ierarhică a politicilor de securitate*

Politica de Guvernare trebuie să acopere conceptele de securitate a informaţiilor la un nivel înalt, să definească aceste concepte, să descrie de ce sunt importante şi să detalieze în ele poziţia companiei. Politica de guvernare va fi citită de către managerii şi utilizatorii finali. În mod implicit, va fi citită şi de către consilierii tehnici (în special consilierii tehnici pe securitate), deoarece ei sunt şi utilizatori finali. Toate aceste grupuri vor folosi politica pentru a înţelege mai bine filosofia generală a politicii de securitate a companiei. Acest lucru poate fi folosit pentru a aduce la cunoştinţă tuturor despre influenţa reciprocă dintre securitatea informaţiilor şi toate unităţile componente ale companiei.

Politica de guvernare ar trebui să fie strâns aliniată la HR (resursele umane) existente şi viitoare, dar şi la alte politici ale companiei, în special acelea în care sunt menţionate aspecte legate de securitate, cum ar fi utilizarea e-mailului, mesageriei sau a computerului, etc. Documentul privind politica de guvernare va fi de acelaşi nivel cu politicile globale ale companiei.

Politica de guvernare este susţinută de politicile tehnice care, la rândul lor, acoperă subiectele mai detaliat şi le face să fie abordabile pentru fiecare tehnologie relevantă. Includerea anumitor subiecte la nivelul politicii de guvernare poate ajuta la evitarea necesităţii unei politici tehnice detaliate ce se referă la subiectele respective. De exemplu, aprobarea unei politici de gestionare a parolelor companiei ar înseamnă că detaliile unor elemente specifice în administrarea

E-ISBN 978-9975-75-901-4

parolelor pentru fiecare sistem de operare sau aplicaţie în parte pot fi specificate în politica tehnică relevantă acestor sisteme sau aplicaţii, în loc să fie necesară o politică tehnică comună privind administrarea parolelor pentru toate sistemele. Acest lucru însă poate să nu fie valabil şi în cazul unei companii mai mici, unde sunt mai puţine sisteme şi aplicaţii şi, prin urmare, poate fi suficientă o singură politică tehnică a parolelor. Pentru o companie mai mare însă, versiunea de politică expusă mai sus oferă un proces mai eficient pentru utilizatori, deoarece aceştia vor trebui să facă referire la mai puţine documente - simplificarea acestui proces măresc probabilitatea ca utilizatorii să respecte politica, îmbunătăţind astfel securitatea.

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

Politicile Tehnice vor fi folosite de consilierii tehnici în timp ce îşi vor îndeplini responsabilităţile legate de securitate pentru sistemul cu care lucrează. Acestea vor fi mai detaliate decât politica de guvernare şi vor fi specifice sistemului sau problemei concrete, de exemplu, *Politică Tehnică SC-400* (destinată sistemului SC-400) sau *Politică Tehnică de Securitate Fizică*.

Politicile tehnice vor acoperi multe dintre aceleaşi subiecte ca şi politica de guvernare, precum şi câteva subiecte specifice subiectului general. Acestea vor fi de fapt un manual care va cuprinde modalităţile de asigurare a securităţii unui sistem de operare sau a unui dispozitiv de reţea, etc. Aceste politici descriu ce trebuie făcut, dar nu şi cum să procedăm - acest lucru este rezervat documentelor procedurale care reprezintă următorul nivel de detaliere după politicile de guvernare şi cele tehnice.

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

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

Procedurile şi instrucţiunile sunt ca un supliment al politicii de securitate şi trebuie să fie scrise la următorul nivel de detaliere, care descrie modul în care trebuie făcut ceva. Acestea furnizează informaţii sistematice practice despre modul de implementare a cerinţelor stabilite în documentele politicii. Ele ar putea fi scrise de diverse grupuri din întreaga companie şi ar putea fi menţionate în politica relevantă, dar ar putea şi să nu fie menţionate, în funcţie de cerinţele concrete.

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

Documentele de procedură vor acţiona, de asemenea, ca un instrument de backup pentru cazul în care unii membri ai personalului va pleca, asigurându-ne că cunoştinţele lor nu vor fi pierdute şi că cerinţele de politică pot fi încă executate.

Raţionamentul 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 intenţii imediate exagerate şi să încerce să dezvolte rapid un program de politici cuprinzător şi complex. Este puţin probabil ca acest lucru să aibă succes din mai multe motive, printre care nevoia de un buy-in management, cultura şi resursele nepregătite ale companiei etc. În această situaţie, este recomandabil să se înceapă iniţial cu politicile mici, şi cu un cadru-schelet al politicii de securitate care să conţină doar politicile esenţiale care vor fi elaborate în primul rând.

Pe măsură ce procesul creşte în maturitate, companiile vor putea să dezvolte, atunci când apare necesitatea, întreaga gamă de politici cu mai multe detalii incluse în fiecare, precum şi documentaţia procedurală însoţitoare. Educaţia, conştientizarea şi procesele de comunicare trebuie să devină ‘mature’ pentru a face faţă 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 şi respectate, şi de fapt ar putea să înceapă să le utilizate pentru a impulsiona unele modificări necesare în întreaga companie.

E-ISBN 978-9975-75-901-4

Apare însă o întrebare foarte importantă: de unde totuşi e mai bine de început procesul de elaborare a unei politici de securitate, deoarece există mai multe puncte de pornire: legislaţia nou adoptată (sau cea care va fi în curând) poate fi adesea un impuls puternic pentru dezvoltarea politicii, la fel ca şi recentele incidente de securitate sau administratorii entuziaşti care s-au întors recent de la un nou curs de formare. Toate acestea oferă o mare contribuţie politicii de securitate, dar cheia spre elaborarea unei politici funcţionale este să realizăm un echilibru între toate aceste aspecte.

Bazându-ne exclusiv pe abordarea „*de sus în jos*” prin utilizarea doar a legislaţiei, a regulamentelor şi a celor mai bune practici pentru a scrie o politică, rezultatul ar putea fi o politică nerealistă şi artificială care nu va fi funcţională în lumea reală. În mod similar, bazându-ne doar pe o metodă „*de jos în sus*”, axată numai pe cunoştinţele 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 combinaţie a acestor abordări, atât de sus în jos, cât şi de jos în sus [2]. Pentru a realiza acest lucru, această idee trebuie să fie luată în considerare încă de la început şi trebuie să fie reflectată în diversitatea domeniilor implicate în elaborarea politicilor şi a tipurilor de politică ce vor fi elaborate ulterior.

Această abordare echilibrată va duce cel mai probabil la un proces mai matur de dezvoltare a politicilor şi fa vi funcţională atât pentru companiile mici (în care există un spaţiu redus între „sus” şi „jos”), cât şi pentru companiile mari, unde este nevoie de cunoştinţe vaste pentru a asigura o politică realistă şi viabilă.

Dezvoltarea politicilor trebuie să ţină seama şi de măsura în care politica ar trebui să reflecte practica curentă în raport cu viitorul preferat. Elaborarea unei politici care să reflecte doar exact ceea ce se face astăzi poate fi depăşită deja atunci când este publicată, deoarece o politică, care include măsuri ce nu pot fi implementate în mod adecvat, poate fi imposibil de respectat din motive tehnice şi poate să fie ignorată ca nerealistă şi inoperabilă. Este important ca acest lucru să fie discutat într-o fază incipientă, deoarece altfel am putea ajunge prea departe în dezvoltarea unui model nefuncţional al viitorului preferat, iar acest lucru ar putea să fie depistat doar ulterior, la etapa de identificare a lacunelor politicii, atunci când va fi deja irosit mult timp şi efort, dezvoltând ceva ce nu are de fapt valoare. Cea mai bună politică trebuie să atingă un echilibru între practica actuală şi viitorul preferat şi acesta este scopul pe care ar trebui să-l urmărească echipa de dezvoltare a politicilor.

În cele din urmă, când se analizează ce ar trebui să fie inclus în proiectul iniţial al politicii, trebuie *să ne asigurăm că am luat în considerare toate tipurile de ameninţări cu care se poate confrunta compania.* Ameninţările care provin din exterior de la atacatorii rău intenţionaţi sub formă de viruşi, viermi etc. trebuie obligatoriu să fie luate în considerare atunci când se elaborează o politică de securitate. Însă cel puţin la fel de importante sunt şi dezastrele naturale, foştii sau actualii angajaţi nemulţumiţi, dar şi ignoranţa, care conduce la expunerea accidentală a securităţii. Politicile de securitate ar trebui să cuprindă măsuri pentru combaterea tuturor acestor tipuri de ameninţări.

Fiecare politică de securitate ar trebui să includă aşa compartimente ca *Politica de Guvernare*, *Politicile tehnice*, *Documentele de procedură*, şi în plus faţă acestea trebuie să mai conţină neapărat încă câteva secţiuni: introducerea, scopul, domeniul de aplicare, rolurile şi responsabilităţile, sancţiunile şi încălcările, programul de revizuire şi actualizare, informaţiile de contact, definiţiile şi acronimele [3].

Planul de securitate (sau programul de securitate) este dezvoltat în baza politicii de securitate. În cadrul acestui plan sunt alocate resursele, numiţi responsabilii, stabilită ordinea de execuţie şi control, etc. În baza planului de securitate sunt elaborate norme specifice, regulamente şi recomandări pentru activitatea personalului responsabil de securitatea informaţiilor. Aceste norme se referă la măsurile procedurale de protecţie a informaţiei.

Un plan de securitate împreuna cu politica de securitate din care acesta a rezultat sunt proiectate pentru a proteja atât informaţiile cât şi resursele materiale critice de la o gama larga de

E-ISBN 978-9975-75-901-4

ameninţări în scopul de a asigura continuitatea activităţii instituţiei (a afacerii în cazul unei companii), de a reduce riscul în afaceri, de a maximiza randamentul investiţiilor şi a oportunităţilor de afaceri.

Scopul planului de securitate este să asigure confidenţialitatea, integritatea şi disponibilitatea datelor, să definească, să dezvolte, şi să documenteze politicile şi procedurile de informare ce vin în sprijinul scopului şi obiectivelor instituţiei precum şi să permită instituţiei să îndeplinească din punct de vedere legal şi etic responsabilităţile cu privire la resursele IT.

Deci după formularea politicii de securitate este deja posibil, dar şi necesar, să se pregătească palanul de implementare a acesteia şi, de fapt, să se pună în aplicare acest plan.

2. MĂSURI PROCEDURALE DE PROTECŢIE A INFORMAŢIEI

Măsurile procedurale de securitate a informaţiilor reprezintă ansamblul reglementărilor prin care se stabilesc măsurile interne de lucru şi de ordine interioară destinate realizării protecţiei informaţiilor, acestea fiind măsurile de securitate implementate de oameni. Aceste măsuri, care se concretizează în diverse norme specifice, regulamente şi recomandări pentru activitatea personalului responsabil de securitatea informaţiilor, sunt elaborate în baza planului de securitate.

La nivelul procedural de asigurare a securităţii informaţiilor se pot distinge următoarele clase de măsuri: managementul personalului; protecţia fizică; menţinerea capacităţii de funcţionate; reacţionarea la încălcări ale securităţii; planificarea lucrărilor de recuperare [3].

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

Principiul separarea atribuţiilor prescrie alocarea de roluri şi responsabilităţi astfel încât o persoană să nu poată întrerupe un proces de o importanţă critică pentru întreprindere. 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 încredinţată unui angajat procesarea cererilor pentru astfel de plăţi, iar altuia - să certifice aceste cereri.

Principiul minimizării privilegiilor prevede acordarea utilizatorilor doar a drepturilor de acces care sunt necesare pentru ca aceştia să-şi îndeplinească atribuţiile oficiale. Scopul acestui principiu este evident - de a reduce prejudiciul cauzat de comportamentul greşit, fie el accidental sau intenţionat.

Elaborarea preliminară a fişei de post permite evaluarea criticităţii acesteia şi planificarea procedurii de verificare şi selectare a candidaţilor. 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 şi analiza acţiunile efectuate de acesta în scopul de a identifica situaţiile suspecte.

Atunci când un angajat este concediat, mai ales în cazul unui conflict între el şi administraţie, este necesar ca în regim de urgenţă acesta să fie lipsit de drepturile de acces la sistemul informatic al întreprinderii, prin transferul de echipament şi împuterniciri către alt angajat.

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

Principiul de bază al protecţiei fizice, a cărui respectare ar trebui să fie monitorizată în mod continuu, poate fi formulat ca „continuitatea protecţiei în timp şi spaţiu.“

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

Menţinerea capacităţii de funcţionare 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 integrităţii informaţiilor. Mai întâi de toate, trebuie să putem urmări ce software este instalat pe calculatoare, deoarece în cazul în care utilizatorii îl vor instala la discreţia sa, aceasta poate duce la infectarea sistemului, precum şi la apariţia unor căi de ocolire a instrumentelor şi mijloacelor de securitate existente în companie.

E-ISBN 978-9975-75-901-4

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

Reacţia la încălcările regimului de securitate a informaţiilor are următoarele obiective: localizarea incidentelor şi reducerea riscurilor; identificarea intruşilor; prevenirea încălcărilor repetate.

În cazul unei încălcări a regimului de securitate, trebuie imediat luate măsuri, iar succesiunea acţiunilor pentru astfel de cazuri este foarte important să fie planificată în avans şi reflectată în documente. Toţi angajaţii ar trebui să cunoască cum să acţioneze şi pe cine să contacteze în cazul detectării unei încălcări a securităţii, precum şi să ştie ce consecinţe îi aşteaptă pe ei înşişi în cazul în care vor încălca regulile de securitate a informaţiilor.

Planificarea lucrărilor de recuperare ne va permite să fim pregătiţi pentru eventualele incidente ca să putem reduce în regim de urgenţă prejudiciile cauzate de acestea şi să ne menţinem capacitatea de a funcţiona cel puţin la un nivel minim acceptabil.

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

- identificarea funcţiilor de importanţă critică ale întreprinderii şi stabilirea priorităţilor;
- identificarea resurselor necesare pentru îndeplinirea funcţiilor critice;
- definirea unei liste de accidente posibile;
- dezvoltarea unei strategii de recuperare;
- pregătirea pentru implementarea strategiei alese;
- verificarea strategiei.

Un lucru foarte important aici este că atunci când planificăm lucrările de recuperare, trebuie să fim conştienţi că nu este întotdeauna posibil să asigurăm imediat o funcţionare completă a întreprinderii şi de aceea este necesar să se identifice funcţiile de importanţă critică, fără de care întreprinderea îşi pierde identitatea. Chiar mai mult - aceste funcţii la fel trebuiesc organizate în conformitate cu astfel de priorităţi, încât să fie posibil ca într-un timp cât mai scurt şi cu costuri minime să fie reluată activitatea după fiecare accident petrecut.

CONCLUZII

Nu cred că ar fi corect să afirmăm că măsurile organizatorice sunt cele mai importante măsuri în asigurarea securităţii informaţiei în cadrul unei întreprinderi, însă, cu certitudine, fără aplicarea lor celelalte categorii de măsuri nu îşi vor atinge scopul, făcând ac întreprinderea să rămână vulnerabilă pe diverse dimensiuni.

Este important ca conducerea de vârf a întreprinderii să fie conştientă de necesitatea implementării măsurilor organizatorice şi să insiste în această direcţie, însă chiar având suportul total al conducerii este dificil de realizat instantaneu şi corect toate măsurile administrative şi procedurale de protecţie a informaţiei. În primul rând trebuie de elaborat o politică de securitate, la început cu conţinut estul de comun, iar pe parcurs în mod continuu de actualizat şi 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 şi de măsurile procedurale, fiindcă *normele specifice, regulamente şi recomandările cu aspect de securitate a informaţiilor vor contribui esenţial la realizarea programul de securitate.*

BIBLIOGRAFIE

1. ISO/IEC 27001:2013. Information Technology, Security Techniques, Information Security Management Systems Requirements, Second Edition, 2013.
2. Flowerday S., Information security policy development and implementation, Journal Computers and Security archive, vol. 61, Issue C, August 2016, pp.169-183.
3. Diver S., Information Security Policy - A Development Guide for Large and Small Companies, SANS Institute, 2007, 43 p.