UNIVERSITATEA DE STAT DIN MOLDOVA

FACULTATEA RELAȚII INTERNAȚIONALE, ȘTIINȚE POLITICE ȘI ADMINISTRATIVE

CATEDRA ȘTIINȚE POLITICE ȘI ADMINISTRATIVE

SPECIALITATEA STUDII DE SECURITATE NAȚIONALĂ

La disciplina: Securitatea Informațională

"PROTECȚIA ȘI SECURITATEA SISTEMELOR INFORMAȚIONALE"

***A elaborat**: Rotaru Vasile*

Masterand SSN 2201

***Coordonator**:*
dr., conf. univ., BUSUNCIAN Tatiana

Chișinău 2023

CUPRINS

ÎNTRODUCERE

Societatea îmbrăţişează din ce în ce mai mult tehnologia informaţiei. Informaţia care până nu de mult avea la bază hârtia, îmbracă acum forma electronică. Informaţia pe suport de hârtie mai este încă rezervată documentelor oficiale, acolo unde este necesară o semnătură sau o stampilă. Adoptarea semnăturii electronice deschide însă perspectiva digitizării complete a documentelor, cel puţin din punct de vedere funcţional.

Acest nou mod de lucru, în care calculatorul a devenit un instrument indispensabil şi un mijloc de comunicare prin tehnologii precum poşta electronică sau Internetul, atrage după sine riscuri specifice. O gestiune corespunzătoare a documentelor în format electronic face necesară implementarea unor măsuri specifice. Măsurile ar trebui să asigure protecţia informaţiilor împotriva pierderii, distrugerii sau divulgării neautorizate. Cel mai sensibil aspect este acela de a asigura securitatea informaţiei gestionată de sistemele informatice în noul context tehnologic.

Securitatea informaţiei este un concept mai larg care se referă la asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei. Dinamica tehnologiei informaţiei induce noi riscuri pentru care organizaţiile trebuie să implementeze noi măsuri de control. De exemplu, popularizarea unităţilor de inscripţionat CD-uri sau a memoriilor portabile de capacitate mare, induce riscuri de copiere neautorizată sau furt de date.

Lucrul în reţea şi conectarea la Internet induc şi ele riscuri suplimentare, de acces neautorizat la date sau chiar frauda.

Dezvoltarea tehnologică a fost acompaniată şi de soluţii de securitate, producătorii de echipamente şi aplicaţii incluzând metode tehnice de protecţie din ce în ce mai performante. Totuşi, în timp ce în domeniul tehnologiilor informaţionale schimbarea este exponenţială, componenta umană rămâne neschimbatăAsigurarea securităţii informaţiilor nu se poate realiza exclusiv prin măsuri tehnice, fiind în principal o problemă umană.

Majoritatea incidentelor de securitate sunt generate de o gestiune şi organizare necorespunzătoare, şi mai puţin din cauza unei deficienţe a mecanismelor de securitate.

Este important ca organizaţiile să conştientizeze riscurile asociate cu utilizarea tehnologiei şi gestionarea informaţiilor şi să abordeze pozitiv acest subiect printr-o conştientizare în rândul angajaţilor a importanţei securităţii informaţiilor, înţelegerea tipologiei ameninţărilor, riscurilor şi vulnerabilităţilor specifice mediilor informatizate şi aplicarea practicilor de control.

PARTICULARITĂȚI ALE SISTEMELOR DE SECURITATE

Odată cu trecerea spre prelucrarea masivă a datelor cu ajutorul calculatoarelor electronice, ca urmare a volumului mare al investiţiilor şi a transferării „grijii" informaţiei către sistemele electronice de calcul, s-a pus într-un alt context problema protejării noilor averi, fizice şi informaţionale. Totul trebuie pornit de la schimbarea opticii privind gestiunea fizică a noilor averi, dar şi de la valorificarea pe multiple planuri a datelor memorate, încercându-se să se obţină alte dimensiuni ale funcţiei de informare a conducerii, prin utilizarea informaţiilor arhivate şi păstrate în alte condiţii.

În vederea obţinerii noilor performanţe, datele prelucrate sunt supuse unor operaţiuni suplimentare în faza de culegere, astfel încât să poată fi valorificate ulterior pe mai multe planuri. Preluarea datelor din două sau mai multe documente operative în unul sau mai multe fişiere, având suportul de înregistrare specific noii variante de prelucrare, constituie o îndepărtare vizibilă de modul tradiţional de păstrare a documentelor primare, de gestionare a lor, şi duce la apariţia mai multor persoane care pot accesa aceleaşi date. Mai mult, prin agregarea înregistrărilor anterioare, pot rezulta chiar noi informaţii.

Cum noile resurse fizice ale sistemelor de calcul sunt destul de scumpe, se constată o tendinţă de centralizare a prelucrărilor de date, din motive de economie, dar, în acelaşi timp,

sporeşte grija asigurării securităţii lor, întrucât riscul pierderii lor sau al consultării neautorizate este şi mai mare. Într-un astfel de caz, nu trebuie uitat principiul dominant al prelucrării automate a datelor, GIGI (Gunoi la Intrare, Gunoi la Ieşire), conform căruia o eroare strecurată într-un sistem integrat se propagă cu o viteză inimaginabilă, în zeci sau sute de locuri din sistem,generând, la rândul ei, o multitudine de erori în rapoartele ce se vor obţine ulterior.

Alt element, deosebit de important, îl constituie factorul uman. Dacă în vechile sisteme erau uşor de controlat locurile de păstrare a informaţiei, acum, într-un mediu puternic informatizat, persoanele cu atribuţii de urmărire a modului de realizare a securităţii datelor au o misiune mult mai dificilă. Se pot înregistra două cazuri: fie că nu pot intui căile prin care datele pot fi accesate pe ascuns, în vederea sustragerii sau modificării lor, fie că nu reuşesc să descopere de unde şi cine, cu ajutorul unui calculator aflat la distanţă de locul păstrării datelor, are acces neautorizat în sistem. Surpriza poate veni tocmai de la persoanele care lucrează cu cea mai mare asiduitate la anumite aplicaţii. Loialitatea excesivă, în acest caz, poate da de gândit.

Prin trecerea la prelucrarea automată a datelor (p.a.d.) s-au schimbat şi suporturile informaţiei,

precum şi mijloacele de lucru, situaţie în care apar noi aspecte, şi anume:

Densitatea informaţiei este mult mai mare în mediul informatic decât în sistemele clasice, bazate pe hârtie. Prin utilizarea discurilor optice sau a stick-urilor USB, zeci de volume, însumând zeci de mii de pagini de hârtie, pot fi introduse cu multă uşurinţă într-un buzunar. CD-urile, DVD-urile, cardurile, memoriile flash, hard-discurile portabile şi alte suporturi moderne pot fi astfel subtilizate discret, cu eforturi minime dar cu efecte distructive majore.

Obscuritatea sau invizibilitatea constituie o altă problemă, întrucât conţinutul documentelor electronice şi al rapoartelor derivate stocate pe suporturile enumerate mai sus nu poate fi sesizat pe cale vizuală la un control de rutină. De multe ori, cei puşi să controleze nu au pregătirea informatică şi nici echipamentele necesare pentru a observa o eventuală sustragere de fişiere.

Accesibilitatea datelor din sistemele de calcul este mai mare, cel puţin pentru o nouă categorie de infractori, catalogaţi „hoţi cu gulere albe", făcându-se trimitere vădită la nivelul de cultură, în primul rând informatică, al acestora.

Lipsa urmelor eventualelor atacuri criminale constituie un alt element îngrijorător al noului mediu de lucru. Ştersăturile din vechile documente pentru schimbarea sumelor, precum şi adăugările de noi înregistrări „cu creionul" nu mai există, modificările în fişierele electronice sunt efectuate cu multă lejeritate şi foarte greu de depistat ulterior.

Remanenţa suporturilor, după ce au fost şterse, poate constitui o cale sigură de intrare în posesia informaţiilor memorate anterior. Se cunosc numeroase programe de restaurare a fişierelor şterse.

Agregarea datelor. Puse laolaltă, datele capătă altă valoare decât cea avută prin păstrarea lor în mai multe locuri separate unele de altele. Uneori, informaţiile de sinteză sunt valorificate prin programe speciale în vederea obţinerii, tot cu ajutorul calculatorului, a strategiei şi tacticii firmei într-un anumit domeniu. Edificator este cazul benzilor magnetice ale firmei IBM, care conţineau direcţiile de cercetare pe următorii 15 ani, intrate în posesia unei firme dintr-o ţară concurentă.

Necunoaşterea calculatoarelor. Pentru foarte multe persoane, îndeosebi de vârstă înaintată, calculatorul este investit cu forţe supraomeneşti, ceea ce le conferă o încredere oarbă în datele obţinute prin intermediul lui. De asemenea, din motive de nepricepere, aceşti anagajaţi pot fi victime uşoare ale corupătorilor ... informatizaţi.

Progresul tehnologic. Rezultatele cercetărilor tehnico-ştiinţifice se transformă zi de zi în tehnologii din ce în ce mai performante de accesare a datelor. Nu acelaşi lucru se poate spune şi

despre progresele înregistrate în domeniul securităţii datelor.

Comunicaţiile şi reţelele, devenind tot mai performante, au extins aria utilizatorilor, atât din punct de vedere numeric, cât şi al dispersiei în teritoriu, întregul spaţiu terestru fiind accesibil reţelelor foarte mari. Odată cu noile progrese, şi aria utilizatorilor rău intenţionaţi s-a mărit, precum şi variantele de furt informatizat.

Integrarea puternică a sistemelor apare ca o consecinţă a îmbunătăţirii formelor de comunicaţie şi a proliferării reţelelor de calculatoare. Pe acelaşi canal de comunicaţie sunt transmise tot felul de date. În plus, introducând o dată eronată în sistem, de la un banal punct de vânzare, ea pătrunde cu rapiditate în zeci de fişiere şi, implicit, aplicaţii ale firmei. Comerţul şi afacerile electronice au deschis şi mai mult apetitul „specialiştilor" în fraudă.

Apariţia utilizatorilor finali informatizaţi constituie un veritabil succes, dar sporeşte şi riscul pierderii datelor importante din calculatorul principal al companiilor.

Standardele de securitate, în pofida atâtor altor domenii în care se înregistrează mutaţii vizibile în intervale scurte de timp, nu se concretizează în forme general valabile şi, cât timp un lucru nu este interzis prin reguli scrise, el ori se consideră că nu există, ori se trage concluzia că este permis.

În concluzie, odată cu dezvoltarea noilor sisteme informaţionale şi cu transferarea către acestea a secretelor firmelor, trebuie văzut în ele, în acelaşi timp, ajutorul numărul unu, dar şi elementele cele mai tentante pentru noii criminali. Hardul şi softul pot fi manevrate cu multă uşurinţă de către om. În acest caz, ca şi în altele intrate în obişnuinţa cotidiană, „inteligenţa" calculatorului lasă de dorit, putându-se spune că tot omul (a)sfinţeşte calculatorul, motiv esenţial pentru sporirea preocupărilor tuturor specialiştilor din domeniul securităţii sistemelor informaţionale.

CONTROLUL ACCESULUI ÎN SISTEMELE DE SECURITATE

După fatidica zi de 11 septembrie 2001, sensul controlului accesului în sistem s-a schimbat radical, atât prin prisma *mijloacelor de exercitare*, cât şi a *domeniilor de aplicare*. În privinţa mijloacelor, dominantă a fost discuţia de la sfârşitul anilor '90, dacă trebuie să se introducă sau nu sistemele de identificare biometrică a persoanelor, făcându-se asocierea cu luarea amprentelor digitale doar pentru elucidarea unor cazuri criminale. Opoziţia cea mai puternică venea din partea sistemului bancar, dar nu numai. Alte instrumente păreau incomode sau periculoase şi, ca atare, erau refuzate în serie. După data susmenţionată lucrurile s-au schimbat radical, în privinţa

identificării biometrice – tendinţă ce va fi demonstrată într-un paragraf distinct al prezentului capitol. Domeniile de aplicare s-au extins, totul venind din convingerea intimă a proprietarilor şi administratorilor de sisteme, văzându-se astfel alte modalităţi de verificare a persoanelor ce doresc accesul în mai toate instituţiile prezidenţiale, guvernamentale şi altele de tip public sau privat, iar aeroporturile şi-au extins zonele supuse unei atenţii speciale.

Nici sistemele informaţionale nu au rămas aceleaşi. Doar simpla trimitere la ceea ce a făcut Microsoft pe linia securizării este destul de elocventă, căci aproape orice mişcare a personalului este sub control, apelându-se la dependenţa totală a acestuia de carduri speciale.

În acest spirit, dorim ca, la finalul parcurgerii capitolului de faţă, cititorii să:

- dobândească suficiente cunoştinţe pentru stabilirea tipurilor de control al accesului adecvate pentru o anumită organizaţie şi pentru implementarea acestora;
- cunoască modele de control şi a modalităţile de combinare a lor;
- deţină suficiente informaţii pentru stabilirea modalităţilor de identificare şi autentificarea persoanelor necesare unei anumite organizaţii.

De regulă, controalele sunt introduse pentru diminuarea riscurilor la care sunt expuse sistemele şi pentru reducerea potenţialelor pierderi. Controalele pot fi *preventive*, *detective* sau *corective*.

Controalele *preventive*, după cum sugerează şi numele lor, au ca scop preîntâmpinarea apariţiei unor incidente în sistem; cele *detective* vizează descoperirea unor apariţii ciudate în sistem, iar controalele *corective* sunt folosite pentru readucerea la normalitate a sistemului după anumite incidente la care a fost expus.

Ca să poată fi atinse obiectivele enumerate, controalele pot fi *administrative*, *logice sau tehnice* şi *fizice*.

Controalele administrative sunt exercitate prin politici şi proceduri, instruire cu scop de conştientizare, verificări generale, verificări la locurile de muncă, verificarea pe timpul concediilor şi o supraveghere exigentă.

Controalele logice sau tehnice cuprind restricţiile de accesare a sistemului şi măsurile prin care se asigură protecţia informaţiilor. Din această categorie fac parte sistemele de criptare, cardurile inteligente, listele de control al accesului şi protocoalele de transmisie.

Controalele fizice încorporează, în general, gărzile de protecţie şi pază, securitatea clădirilor, cum sunt: sistemele de încuiere a uşilor, securizarea camerelor cu servere şi laptop-uri, protecţia

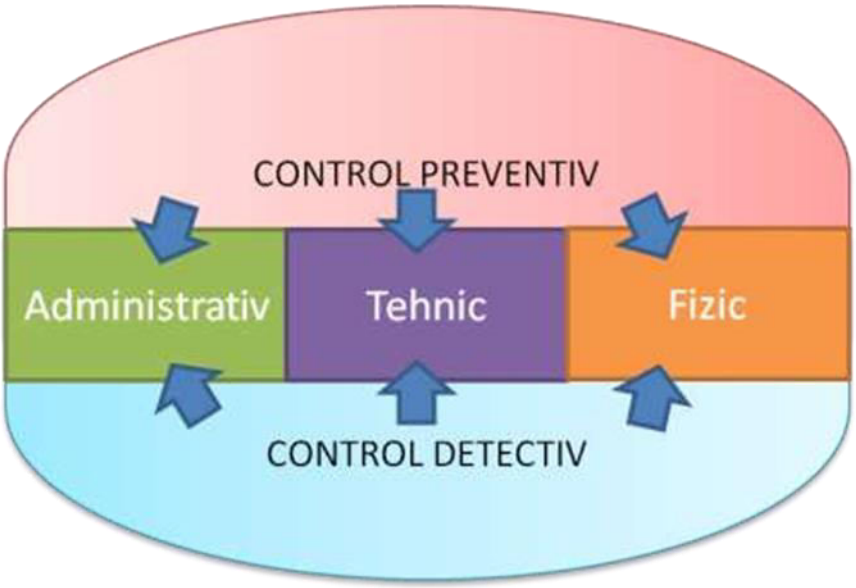
cablurilor, separarea atribuţiilor de serviciu, precum şi realizarea copiilor de siguranţă a fişierelor.

Controalele vizează responsabilizarea persoanelor care accesează informaţii sensibile. Responsabilizarea este înfăptuită prin mecanisme de control al accesului care necesită, la rândul lor, exercitarea funcţiilor de *identificare*, *autentificare* şi *auditare*. Controalele trebuie să fie în deplină concordanţă cu politica de securitate a organizaţiei, iar *procedurile de asigurare* au scopul de a demonstra că prin mecanismele de control se implementează corect politicile de securitate pentru întregul ciclu de viaţă al sistemului informaţional.

Prin combinarea controlului preventiv şi detectiv cu mijloacele celorlalte tipuri de control – administrativ, tehnic (logic) şi fizic – se obţin următoarele perechi:

- preventiv/administrativ;
- preventiv/tehnic;
- preventiv/fizic;
- detectiv/administrativ;
- detectiv/tehnic;
- detectiv/fizic.

Shematic se poate de observat sub schema de mai jos



Controlul preventiv/administrativ

În această variantă, accentul se pune pe resposabilităţile administrative care contribuie la

atingerea obiectivelor controlului accesului. Aceste mecanisme cuprind politicile şi procedurile organizaţionale, verificările de fond înainte de angajare, practicile de încetare a contractului de muncă în condiţii normale şi anormale, planificarea plecărilor în concediu, etichetarea sau marcarea materialelor speciale, supravegherea mai exigentă, cursuri de instruire în scopul conştientizării importanţei securităţii, conştientizarea modului de comportare, precum şi procedurile de semnare a contractului în vederea obţinerii accesului la sistemul informaţional şi la reţea.

Controlul preventiv/tehnic

Împerecherea preventiv-tehnic vizează utilizarea tehnologiilor pentru consolidarea politicilor de control al accesului. Controlul tehnic se mai numeşte şi control logic şi poate fi realizat prin sistemele de operare, prin aplicaţii sau printr-o componentă suplimentară hard/soft. Dintre controalele preventive/tehnice fac parte protocoalele, criptarea, cardurile inteligente, biometria (cu scopul de autentificare), pachetele software pentru realizarea controlului accesului local sau de la distanţă, parolele, meniurile, softul de scanare a viruşilor ş.a.

Controlul preventiv/fizic

În cea mai mare parte, măsurile de control preventiv/fizic sunt de tip intuitiv. Ele vizează restricţionarea accesului fizic în zonele ce conţin informaţii sensibile ale sistemului. Zonele respective sunt definite printr-un aşa-zis *perimetru de securitate*, aflat sub controlul accesului.

În această categorie intră împrejmuirile cu gard, ecusoanele, uşile multiple (după trecerea printr-o uşă, aceasta se blochează automat, iar la următoarea trebuie cunoscut sistemul de deschidere, persoana fiind captivă între două uşi, motiv pentru care se numesc şi *uşi-capcană*), sistemele de intrare pe bază de cartelă magnetică, aparatura biometrică (pentru identificare), servicii de pază, câini de pază, sisteme de controlare a mediului (temperatură, umiditate ş.a.), schiţa clădirii şi a căilor de acces, locurile special amenajate pentru depozitarea suporturilor de informaţii.

Controlul detectiv/administrativ

Câteva dintre controalele detective/administrative se suprapun controalelor preventive/administrative pentru că ele pot fi exercitate cu scopul prevenirii posibilelor violări ale politicilor de securitate sau pentru detectarea celor în curs. Din această categorie fac parte procedurile şi politicile de securitate, verificările de fond, planificarea plecărilor în concediu, marcarea sau etichetarea materialelor speciale, o supraveghere mai exigentă, instruiri cu scopul

conştientizării importanţei securităţii. În plus, cu scop detectiv/administrativ sunt controalele ce vizează rotirea personalului la locurile de muncă, exercitarea în comun a unor responsabilităţi, precum şi revizuirea înregistrărilor cu scop de auditare.

Controlul detectiv/tehnic

Măsurile controlului detectiv/tehnic vizează scoaterea în evidenţă a violării politicii de securitate folosindu-se mijloace tehnice. Aceste măsuri se referă la sistemele de detectare a intruşilor şi la rapoartele privind violările securităţii, generate automat, pe baza informaţiilor colectate cu scopul de a fi probă în auditare. Rapoartele pot evidenţia abaterile de la funcţionarea „normală" sau pot detecta semnături cunoscute ale unor episoade de acces neautorizat.

Datorită importanţei lor, informaţiile folosite în auditare trebuie să fie protejate la cel mai înalt nivel posibil din sistem.

Controlul detectiv/fizic

De regulă, aceste controale necesită *intervenţia omului* pentru evaluarea a ceea ce oferă *senzorii* sau *camerele* pentru a stabili dacă există un pericol real pentru sistem. În acest caz, controlul se exercită prin camere video, detectoare termice, de fum, de mişcare.

PROGRAMUL DE SECURITATE

Organizaţiile au nevoie să-şi protejeze valorile patrimoniale vitale, începând cu resursele umane, continuând cu clădiri, terenuri, utilaje, echipamente speciale şi încheind cu una dintre cele mai importante averi ale noului mileniu, informaţia. Tocmai din această cauză se concep programe de securitate informaţională. Înainte ca acest program să fie abordat, se cuvine efectuată structurarea iniţiativei încă din faza intenţională, realizându-se sau definindu-se politicile, standardele, normele şi procedurile. În acest context, programul de securitate trebuie săse supună elementelor enunţate anterior.

Fără politici riguroase, programele de securitate vor fi aproape fără suport, ineficiente şi nu se vor alinia strategiei şi obiectivelor organizaţiei. Politicile, standardele, normele şi procedurile constituie fundaţia programului de securitate al organizaţiei. Politicile eficiente, clar formulate, vor servi proceselor de auditare şi eventualelor litigii. Combinând elementele specificate, o entitate poate implementa controale specifice, procese, programe de conştientizare şi multe altele, tocmai pentru a-i aduce un plus de linişte. Spune românul: paza bună trece primejdia rea.

O politică, deseori, înseamnă mai multe lucruri, atunci când ne referim la securitatea informaţională a unei organizaţii. Cineva poate să se rezume doar la firewall-urile folosite pentrucontrolarea accesului şi a traseelor pe care circulă informaţiile, altcineva se gândeşte la lacătele,cardurile de acces, camerele de luat

vederi ce înregistrează totul din perimetrele controlate. Dar,câte alte accepţiuni nu i se pot da!

Atunci când discutăm despre politici de securitate, trebuie pornit de la vârful piramidei manageriale, unde se află *top managerii*. Ei au misiunea de a formula *Declaraţia politicii organizaţiei* (*Statement of Policy*). Aceasta este o formulare generală, o declaraţie din care să reiasă:

- importanţa resurselor informaţionale pentru atingerea obiectivelor strategice ale organizaţiei;
- formularea clară a sprijinului acordat tehnologiilor informaţionale în unitate;
- angajamentul top managerilor de a autoriza sau coordona activităţile de definire a standardelor, procedurilor şi normelor de securitate de pe nivelurile inferioare.

În afara declaraţiei politicii de securitate la nivelul top managerilor, există şi politici obligatorii, politici recomandate şi politici informative.

Politicile obligatorii sunt politici de securitate pe care organizaţiile sunt obligate să le implementeze ca efect al acordurilor, regulamentelor sau al altor prevederi legale. De regulă, aicise încadrează instituţiile financiare, serviciile publice sau orice alt tip de organizaţie care serveşteinteresului public. Aceste politici sunt foarte detaliate şi au elemente specifice, în funcţie de domeniul de aplicare.

De regulă, politicile obligatorii au două scopuri de bază:

- asigurarea că o organizaţie urmează procedurile standard sau politicile de bază din domeniul ei de activitate;
- de a oferi încredere organizaţiilor că ele urmează standardele şi politicile de securitate din domeniul de activitate.

Politicile recomandate, prin definiţie, nu sunt obligatorii, dar sunt puternic susţinute, cu prezentarea consecinţelor foarte dure în cazul înregistrării eşecurilor. O organizaţie este direct interesată ca toţi angajaţii ei să considere aceste politici ca fiind obligatorii. Cele mai multe politici se încadrează în această categorie. Ele sunt foarte clar formulate la toate nivelurile. Cei mai mulţi angajaţi vor fi riguros controlaţi prin astfel de politici, definindu-le rolurile şi responsabilităţile în organizaţie.

Politicile informative au scopul de a informa cititorii. Nu poate fi vorba de cerinţe specifice, iar interesaţii de aceste politici pot să se afle în interiorul organizaţiei sau printre partenerii ei.

După aceste descrieri, putem să facem o scurtă prezentare a elementelor comune tuturor politicilor de securitate, astfel:

- *domeniul de aplicare*: declararea domeniului de aplicare înseamnă prezentarea intenţiei vizate de politică şi ea va scoate în relief şi legăturile existente cu întreaga documentaţie a organizaţiei. Formularea trebuie să fie scurtă şi se plasează la începutul documentului;
- *declararea politicii top managerilor* se include la începutul documentului şi are dimensiunea

unui singur paragraf, specificând scopul global al politicii;

- *responsabilităţile* constituie conţinutul unei secţiuni distincte şi cuprind persoanele implicate în asigurarea bunei funcţionări a politicii;
- *consecinţele*: printr-o astfel de formulare se prezintă pierderile posibile dacă politica nu va fi respectată;
- *monitorizarea*: se specifică modul în care se monitorizează respectarea şi actualizarea continuă a politicii;
- *excepţiile*: se menţionează cazurile în care apar excepţii şi modalităţile de tratare a lor; de regulă, au o durată limitată de aplicare, de la un caz la altul.

Pe nivelul inferior politicilor se află trei elemente de implementare a politicii: standardele, normele şi procedurile. Ele conţin detaliile politicii, cum ar fi posibilităţile de implementare, ce standarde şi proceduri să fie întrebuinţate. Ele sunt făcute publice la nivel de organizaţie, prin manuale, Intranet, cărţi, cursuri ş.a.

De cele mai multe ori, standardele, normele şi procedurile sunt tratate laolaltă, dar nu este cea mai inspirată idee, fiindcă tratarea separată a lor este justificată de următoarele argumente:

- fiecare dintre ele serveşte unei funcţii diferite şi are propria audienţă; chiar şi distribuţia lor fizică este mai lejeră;
- controalele securităţii pe linia confidenţialităţii sunt diferite pentru fiecare tip de politică;
- actualizarea şi întreţinerea politicii ar deveni mai anevoioase, prin prisma volumului documentaţiei, dacă s-ar trata nediferenţiat.

Standardele

Standardele specifică utilizarea anumitor tehnologii, într-o viziune uniformă. De regulă, standardele sunt obligatorii şi sunt implementate la nivel de unitate, tocmai pentru asigurarea uniformităţii. Elementele principale ale unui standard de securitate informaţională sunt:

- *scopul şi aria de aplicare*, prin care se oferă o descriere a intenţiei standardului (realizarea unui tip de server pe o anumită platformă);
- *roluri şi responsabilităţi* la nivel de corporaţie pe linia definirii, execuţiei şi promovării standardului;
- *standardele cadrului de bază*, prin care sunt prezentate declaraţiile de pe cel mai înalt nivel, aplicabile platformelor şi aplicaţiilor;
- *standardele tehnologiei* conţin declaraţiile şi descrierile aferente (configuraţia sistemului sau serviciile nesolicitate de sistem);
- *standardele administrării* reglementează administrarea iniţială şi în timpul exploatării platformei

şi aplicaţiilor.

Normele

Normele sunt oarecum asemănătoare standardelor, referindu-se la metodologiile sistemelor securizate, numai că ele sunt acţiuni recomandate, nu obligatorii. Sunt mult mai flexibile decât standardele şi iau în considerare naturile diverse ale sistemelor informaţionale. Ele specifică modalităţile de dezvoltare a standardelor sau garantează aderenţa la principiile generale ale securităţii.

Elementele principale ale unei norme de securitate informaţională sunt:

- *scopul şi aria de aplicare*, descriindu-se intenţia urmărită prin regula respectivă;
- *roluri şi responsabilităţi* pe linia definirii, execuţiei şi promovării normei;
- *declaraţii de orientare*: este un proces pas-cu-pas de promovare a tehnologiilorrespective;
- *declaraţii de exploatare*: se definesc obligaţiile zilnice, săptămânale sau lunare pentru o corectă exploatare a tehnologiei respective.

Procedurile

Procedurile prezintă paşii detaliaţi ce trebuie să fie parcurşi pentru execuţia unei activităţi. Se descriu acţiunile concrete pe care trebuie să le efectueze personalul. Prin ele se oferă cele mai mici detalii pentru implementarea politicilor, standardelor şi normelor. Uneori se foloseşte în locul acestui concept cel de *practici*.

Politicile de securitate sunt tratate ştiinţific prin *modelele de politici de securitate*, grupate în *modele de securitate multinivel* şi în *modele de securitate multilaterală*.

Cele mai cunoscute modele de politici de securitate sunt: modelul Bell-LaPadula (de securitate multinivel), modelul matricei de control al accesului, modelul Biba (modelul de integritate), compartimentarea şi modelul reţea, modelul zidului chinezesc, modelul BMA (British Medical Association).

Fără politici riguroase, *programele de securitate* vor fi aproape fără suport, ineficiente şi nu se vor alinia strategiei şi obiectivelor organizaţiei. *Politicile, standardele, normele şi procedurile* constituie fundaţia programului de securitate al organizaţiei. Politicile eficiente, clar formulate, vor servi proceselor de auditare şi eventualelor litigii. Combinând elementele specificate, o entitate poate implementa controale specifice, procese, programe de conştientizare şi multe altele, tocmai pentru a-i aduce un plus de linişte.

În afara declaraţiei *politicii* de securitate la nivelul top managerilor, există şi politici obligatorii, politici recomandate şi politici informative.

Standardele sunt obligatorii şi sunt implementate la nivel de unitate, pentru asigurarea uniformităţii. *Normele* sunt oarecum asemănătoare standardelor, referindu-se la metodologiile sistemelor securizate, numai că ele sunt acţiuni recomandate, nu obligatorii. *Procedurile* prezintă paşii detaliaţi ce trebuie să fie parcurşi pentru execuţia unei activităţi

SECURITATEA LA NIVELUL INTREGULUI SISTEM DE SECURITATE

Un sistem informatic de încredere este format din totalitatea echipamentelor, programelor, componentelor fizice realizate prin soft (firmware) şi a mecanismelor procedurale care concură la asigurarea securităţii prelucrării automate a datelor.

În SUA, Centrul de Apărare a Securităţii Calculatoarelor al Agenţiei Naţionale de Securitate a emis unele recomandări astfel încât să se ştie ce înseamnă o bază informatică de încredere. Prin intermediul lor, centrul a stabilit *clase de evaluare* în care să poată fi încadrate produsele de realizare a securităţii sistemelor informatice, după ce sunt supuse unor teste speciale. Astfel, au fost definite patru clase, de la D la A, şi câteva subclase, cum ar fi A1 şi A2.Clasa D este cea mai de jos. În cadrul claselor, numerele mai mari sugerează un sistem mai sigur.

Clasele şi subclasele stabilite sunt:

D. Nesigure sau neevaluate.

C. Capabil să asigure controlul accesului discreţionar.

C1. Orice sistem de operare comercial care asigură separarea fazelor de execuţie ale sistemului de cele ale utilizatorilor obişnuiţi.

C2. Orice sistem de operare comercial dublat de un pachet suplimentar pentru asigurareasecurităţii.

B. Capabil să realizeze controlul obligatoriu al accesului.

B1. Toate informaţiile sunt astfel etichetate încât să corespundă unei anumite categorii desecuritate.

B2. Securitatea organică. Echipamentele şi softul sunt concepute şi realizate astfel încâtsă asigure o securitate obligatorie.

B3. Domenii de securitate. Similar cu B2, numai că este mai bună prin extindereacomponentelor cărora li se asigură securitatea.

A. Securitatea verificată. Măsurile de securitate sunt consemnate în scris şi aprobate ca fiind eficiente.

A1. Verificarea proiectării. De regulă, înseamnă controlul codurilor-sursă din programele de sistem care au funcţii de securitate.

A2. Verificarea implementării. În acest caz sunt examinate programele de sistem executabile şi se

urmăreşte dacă ele coincid cu codul-sursă verificat.

Obiectivul principal al creării unor bariere izolatoare pentru sistemele informatice constă în luarea unor măsuri care să prevină posibilitatea utilizatorilor de programe de a efectua unele schimbări în condiţiile lor de execuţie sau a datelor prelucrate, de a specifica statutul, actual şi viitor, al celorlalţi utilizatori ai programului sau de a prelua controlul asupra datelor altora, ca o excepţie de la regulile normale de acces.

Pentru realizarea acestor obiective, fiecare adresă de program al utilizatorului, numele programatorului, conţinutul registrelor, datele utilizatorilor trebuie să fie protejate împotriva folosirilor neautorizate, în sensul neasigurării transparenţei lor atunci când altui utilizator i se va aloca acelaşi spaţiu de lucru.

Pentru ca un sistem informatic să fie considerat asigurat din punctul de vedere al izolării lui, trebuie să fie îndeplinite două condiţii:

să se folosească un anumit mod de asigurare a securităţii prelucrării pentru a izola sistemul de inamicii săi din afară;

să se apeleze la strategii de apărare, prin izolarea utilizatorilor între ei şi de sistemul de operare al calculatorului. Utilizatorii care prelucrează date ce aparţin categoriilor speciale trebuie să fie izolaţi în mod deosebit.

Sunt posibil de aplicat cel puţin şase strategii de izolare, ele putând fi mai multe. În categoria celor şase intră:

- selectarea modului de prelucrare;
- izolarea temporară;
- izolarea spaţială;
- izolarea realizată prin caracteristicile arhitecturii sistemului;
- izolarea criptografică;
- restricţii la privilegiile sistemului.

Selectarea modului de prelucrare. Atunci când prelucrarea se efectuează în mod local sau în sistem de teleprelucrare, de către unul sau mai mulţi utilizatori în acelaşi timp (în mod serial sau multiprogramare), accesul direct (on-line) sau prin programare sau neprogramare influenţează, în mod vădit, gradul de izolare a sistemului.

Izolarea temporară se aplică, de regulă, în cazul prelucrărilor speciale, dar poate fi folosită şi în modul multiprogramare asupra terminalelor ce intră sau ies într-o/dintr-o reţea, în funcţie de un

calendar, care se întocmeşte luând în considerare categoria datelor şi principiul „trebuie să ştie”.

Izolarea spaţială se realizează prin dedicarea componentelor de prelucrare şi izolarea lor faţă de un alt utilizator.

Arhitectura sistemului este cea care facilitează multiprogramarea, contribuind la izolarea utilizatorilor faţă de sistemul de operare şi între ei înşişi, asigurându-se prelucrarea datelor secrete pe niveluri de securitate.

Controlul accesului la sistemele de prelucrare automată a datelor este un act de decizie a conducerii. În ultimă instanţă, şeful unei companii are responsabilitatea definirii informaţiilor care trebuie să se afle sub control, cine să-l efectueze, prin ce persoane şi în ce condiţii se atribuie drepturi speciale de control şi cum pot fi ele revocate. În practică, responsabilitatea se deleagă spre nivelurile inferioare, spre şefii compartimentelor şi administratori.

În fiecare regulă privind accesul trebuie să se reflecte două principii esenţiale:

Privilegiul minim. Numai acele informaţii sau operaţiuni de prelucrare pe care utilizatorul trebuie să le exercite şi îi revin ca sarcini de serviciu vor fi lăsate la dispoziţia sa, iar ele vor fi stabilite de responsabilii de drept, şi nu de utilizator.

Expunerea minimă. Din momentul în care un utilizator are acces la informaţii speciale sau la alte materiale cu regim similar, acesta are responsabilitatea de a le proteja. Nici oaltă persoană, în timpul sesiunii de lucru, nu va trebui să ia cunoştinţă de ceea ce se prelucrează, se memorează sau se transmite în altă parte. Mai mult chiar, o atenţie deosebită se va acorda restricţiilor referitoare la măsurile de securitate, îndeosebi la caracteristicile deosebit de performante sau la slăbiciunile pe care le au. În acest caz nueste loc de publicitate.

În general, controlul accesului se poate realiza prin modalităţi de genul tabelelor de autorizare, al listelor de control al accesului, al profilurilor de securitate.

Tabelele de autorizare, numite şi tabele de securitate, există în formatul cod-maşină; ele sunt componente ale sistemului de operare, alături de alte programe de control, cu rol de urmărire a bunei funcţionări a sistemului. Importanţa lor rezidă şi în faptul că au un nivel de protecţie similar celor mai bine protejate programe de control.

Tabelele de autorizare se află sub directa preocupare a unor veritabili specialişti, iar pentru utilizatori este important să se cunoască faptul că tabelele trebuie să reflecte, în acest mediu de lucru, ceva identic listelor de control al accesului la valorile deosebite ale firmei în varianta prelucrării manuale a datelor şi a profilelor de securitate ale utilizatorilor.

Listele de control al accesului. Responsabilul cu securitatea sistemului trebuie să actualizeze permanent o listă de control al accesului pentru fiecare program executat pe calculator şi pentru fiecare fişier de date. Ele trebuie să conţină:

elementele de identificare a anumitor valori patrimoniale;

identificarea fără echivoc a oricărui utilizator autorizat;

ceea ce se permite fiecărui utilizator să facă cu o anumită valoare patrimonială;

condiţiile în care se garantează accesul.

Profilurile de securitate trebuie să fie în atenţia responsabilului cu securitatea pentru fiecare utilizator autorizat. Profilul va fi definit prin patru elemente:

- identificarea utilizatorului;
- identificarea tuturor proiectelor pe utilizatorii care le posedă;
- identificarea tuturor categoriilor în care se încadrează utilizatorii, inclusiv cele referitoare la responsabilităţile pe linie de securitate a sistemului;
- identificarea tuturor fişierelor la care utilizatorul poate să aibă acces şi ce anume poatesă efectueze asupra lor.

Noţiunile de „proiect" şi „categorie" din enunţurile de mai sus au acelaşi statut ca şi utilizatorii şi, deci, trebuie să aibă şi ele profilul lor.

De fiecare dată când un utilizator intră în contact cu calculatorul de la un terminal conversaţional sau printr-un lot de lucrări, operaţiunea de certificare a identităţii se impune cu acuitate. Informaţia necesară identificării este parola.

Parolele sunt folosite pentru a permite accesul în sistemele de calcul, la fişierele şi bazele de date ale acestuia. N-ar fi exclus ca ele să fie folosite în viitor şi pentru accesarea înregistrărilor sau câmpurilor acestora, cu condiţia de a fi eficiente şi ieftine. Parolele trebuie să fie asociate cu utilizatorii, proiectele şi categoriile de informaţii.

Despre parole s-a vorbit mai pe larg într-un capitol anterior.

În general, nu trebuie să se permită accesul în sistem până când nu se verifică dacă parola face parte dintr-o listă de parole sau se certifică un alt element de identificare.

Trebuie instituite criterii de condiţionare a accesului local sau de la distanţă, precum şi a celui intern (memorie primară, memorie virtuală, memorie secundară şi suporturi externe).

De o importanţă deosebită, după ce s-a autorizat accesul, este obţinerea unui privilegiu de acces, prin intermediul codurilor speciale, consemnate în tabelele de autorizare.

CONCLUZII

În cele din urmă, conceptul de sistem de protecție a informațiilor computerizate poate fi definit drept un set de norme juridice, organizatorice, administrative și softwaretehnice, menite să contracareze amenințările la adresa funcționării normale a sistemului, pentru a minimiza posibilele pierderi materiale și morale pentru utilizatorii și proprietarii sistemului. Dat fiind că computerele și alte dispozitive digitale au devenit esențiale pentru marea parte a societății contemporane, acestea au devenit din ce în ce mai mult o țintă pentru atacuri. Pentru ca sistemele informatice să fie utilizate cu încredere, persoana/compania trebuie să se asigure, în primul rând, că dispozitivul nu este compromis în niciun fel și că toate comunicațiile vor fi în siguranță. O imagine holistică a tuturor posibilităților de protecție este dificil de creat, deoarece nu există încă o teorie unificată pentru protecția sistemelor informatice. Pentru organizarea unei protecții fiabile, este necesară identificarea clară a tipurilor de atacuri de informații care ar trebui protejate. O amenințare la adresa securității este un potențial impact asupra unui sistem care poate afecta direct sau indirect resursele sistemului informatic. Considerăm că măsurile de protecție ar trebui să fie adecvate gradului de amenințare, precum și corespunzătore importanței informației care este păstrată în sistem. Numai o analiză amănunțită a amenințărilor și a tipurilor de securitate ale sistemelor informatice poate oferi o siguranță relativă.

BIBLIOGRAFIE

1. Ce este securitatea sistemelor informatice? https://www.quora.com/What-is-computersystem-security
2. Cerinte ISO 27001 - Securitatea sistemelor informatice http://www.intermanagement.eu/stire/Cerinte+ISO+27001+Securitatea+sistemelor+informatice.
3. Factorul uman - element crucial în asigurarea securității cibernetice. http://moldova.md/ro/content/factorul-uman-element-crucialasigurarea-securitatii-cibernetice
4. Gorobievschi S. Tehnici, instrumente și metode de comunicare managerială și utilizarea lor în cadrul firmelor contemporane.// În,: Managementul industrial. Coord.: A.Cojuhari, dr.hab., prof.univ.; V. Mămăliga, dr. econ., conf. univ. Chișinău: UTM, 2017, pp. 356-389
5. Harta uimitoare a atacurilor cibernetice https://www.molddata.md /?pag=news&opa=view&id=341&tip=noutati
6. Legea privind aprobarea Concepţiei securităţii informaţionale a R.Moldova https://www.google.com/search?q=Legii+privind+Concep%C5%A3ia+securit%C4%83%C5%A3ii+informa%C5%
7. Mihai Ioan-Cosmin; „Securitatea sistemului informatic”, ISBN 978-9 de curs şi aplicaţii. https://bogdanelb.files.wordpress.com/2009/12/curs_securit_sist_ inf.pdf, p. 5
8. Securitatea informației https://ro.wikipedia.org/wiki/ Securitatea_informa%C8%9Biei
9. Securitatea sistemelor informaţionale. http://formare.contatic.ase.ro/pluginfile.php/46/mod_resource/content/1/Securitatea%20sistemelor%20informationale73-627-369-8, Galați, Ed. Dunărea de Jos, 2007
10. Păduraru M.Vulnerabilităţi ale sistemelor informatice https://www.juridice.ro /412111/vulnerabilitati-ale-sistemelor-informatice.html
11. Popa Sorin Eugen. Securitatea sistemelor informatice. Note.pdf

12. Securitatea sistemelor informatice http://cadredidactice.ub.ro/sorinpopa /files/2011/10/Curs_Securit_Sist_Inf.pdf, p.6