



MEHARI 2007

Concepte și Mecanisme

MEHARI este marcă înregistrată a CLUSIF

Recunoaștere

CLUSIF dorește să mulțumească membrilor echipei de lucru care au contribuit la crearea acestui document.

CLUSIF dorește de asemenea să mulțumească dlui. Valentin P. Măzăreanu și echipei sale (Alina Marin, Raluca Ungureanu) care au acceptat să furnizeze această traducere. Dl. Valentin P. Măzăreanu își desfășoară activitatea în cadrul Facultății de Economie și Administrarea Afacerilor, Universitatea „Al.I.Cuza” Iași și este director general al Paideia Consulting Iași. Pentru mai multe informații despre activitatea dlui. Valentin P. Măzăreanu vă invităm să accesați www.managementul-riscurilor.ro.

Vă rugăm să trimiteți întrebările și comentariile dumneavoastră la adresa mehari@clusif.asso.fr

Cuprins

Cuprins	3
1 Introducere	4
2 Evaluarea mizelor de securitate și clasificarea informației și a bunurilor	6
2.1 Introducere	6
2.2 Definierea mizelor de securitate: scara de valori și clasificarea defecțiunilor	7
3 Evaluarea stării serviciilor de securitate	9
3.1 Introducere	9
3.2 Servicii de securitate	9
3.3 Evaluarea calității serviciului de securitate	11
3.4 Procesul de recenzie a vulnerabilității	14
3.5 Sumar al recenziei vulnerabilității	15
4 Analizarea situațiilor de risc	16
4.1 Introducere	16
4.2 Scenarii de risc	16
4.3 Analiza unui scenariu de risc: privire generală asupra abordării „globale”	17
4.4 Utilizarea bazelor de cunoștințe MEHARI	33
4.5 Procesul analizei situației de risc	33
4.6 Sumar al abordării analiza riscului	35
5 Identificarea situațiilor de risc	36
5.1 Abordarea directă care folosește scara de valori a defecțiunilor	36
5.2 Identificarea sistematică folosind baza de cunoștințe	36
5.3 Cele două abordări sunt complementare	37
6 Utilizarea modulelor Mehari	38
6.1 Planuri de securitate pe bază de analiza riscului	38
6.2 Planuri de securitate pe baza unui audit	45
6.3 Securitatea proiectelor de dezvoltare	48
7 Recenzia principalelor îmbunătățiri în comparație cu versiunile anterioare ale mehari	51
7.1 Crearea tabelului impactului intrinsec	51
7.2 Măsurile de conformare ISO 17799 după un audit MEHARI	51
7.3 Amintirea îmbunătățirilor anterioare ale lui MEHARI	51

1 Introducere

Fiecare CISO (Chief Information Security Officer – Ofițer Șef pentru Securitatea Informațională) se confruntă atunci când acceptă o nouă funcție cu aceleași două provocări de bază, acestea fiind:

- Care este mandatul – cât de cuprinzătoare este misiunea și care sunt obiectivele?
- Care ar trebui să fie planul de atac – ce metodologii și unelte există care să întrunească scopurile managementului securității?

Deși este destul de ușor să fii de acord cu mandatul, există multe posibilități pentru a face față celei de-a doua provocări.

Majoritatea oamenilor sunt de acord că securitatea sistemului informațional implică minimizarea riscurilor asociate cu sistemul informațional al întreprinderii sau al organizației. Totuși, din cauză că „minimizarea” nu este ușor cuantificabilă, unele persoane sugerează că definiția ar fi mai bine formulată prin „riscurile devin acceptabile”.

Acest lucru, în sine, nu este nici el suficient, deoarece nu specifică clar ce este acceptabil sau inacceptabil. Din nou, majoritatea persoanelor au o idee despre cum să judece ce este inacceptabil; iar un risc se poate spune că este inacceptabil atunci când un bun foarte valoros sau critic este foarte vulnerabil.

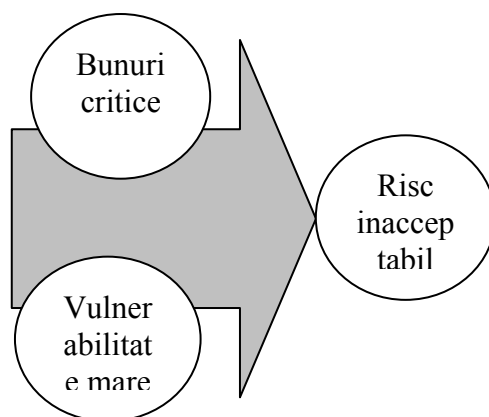


Figura 1. Bunuri critice + Vulnerabilitate mare → Risc inacceptabil

Formularea inacceptabilității în acest mod simplu ne permite să afirmăm că scopul managementului securității este de a preveni ca bunurile de valoare ale organizației să fie foarte vulnerabile.

Ținând cont de acest lucru, putem să ne uităm acum la unele moduri pentru a găsi răspunsuri posibile la ce-a de-a doua provocare a unui CISO:

- Începeți cu cele mai valoroase bunuri, și analizați, pentru fiecare din ele, modul în care ar putea fi supuse riscului. Apoi stabiliți măsuri preventive și de protecție corespunzătoare ca rezultat la aceasta.
- Începeți cu o evaluare a vulnerabilității fiecărui bun, și apoi reduceți vulnerabilitatea până când se ajunge la un nivel acceptabil al riscului.
- Construiți scenarii de risc care combină valoarea bunurilor și vulnerabilitatea lor. Apoi analizați riscurile și decideți ce acțiuni trebuie realizate.
- „Amestecați și potriviți” aceste trei abordări în funcție de circumstanțe.

Este clar, deci, că nu există o singură metodă a managementului securității, ci un spectru de abordări care pot fi folosite în funcție de modelul de afacere și dimensiunea organizației, de cultura de securitate a acesteia, de reguli de conducere, sau chiar de stilul personal de management și de abordarea CISO.

Deși nu există o formulă magică pentru a alege abordarea care trebuie folosită, toate abordările trebuie să se folosească de unelte de nădejde. Valoarea reală a oricărei metodologii este de a asigura un set consistent și complet de unelte, cu mijloacele de a te mișca flexibil între ele. În acest mod, profesioniștii în securitate sunt ajutați la implementarea sistemului lor de management al securității fără a li se impune o abordare sau un rezultat anume.

MEHARI a fost dezvoltat în această idee. Reprezintă mai mult decât o metodologie. El este și un set de unelte. În funcție de nevoile și circumstanțele unei organizații, el se asigură că se poate concepe o soluție adecvată pentru managementul securității, indiferent de abordarea folosită.

Abordările diferite, și utilizarea modulelor MEHARI, sunt ilustrate în diagrama de mai jos.

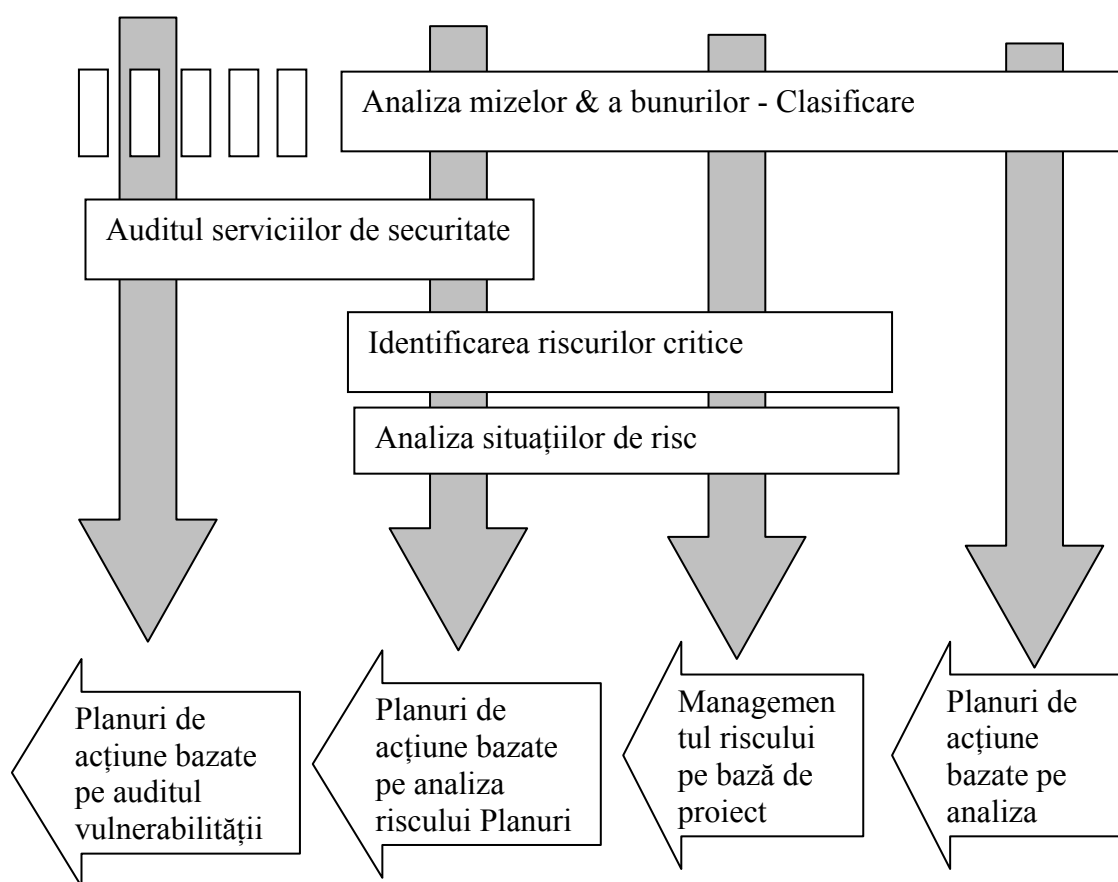


Figura 2. Utilizarea modulelor MEHARI pentru diferite abordări ale securității.

Vom începe prin descrierea diferitelor componente. Mai târziu, vom arăta cum poate fi folosit MEHARI în diferite circumstanțe. Acesta va fi prezentat ca un exercițiu de învățare – și nu este în mod sigur făcut pentru a dicta singurul mod în care poate fi utilizat.

2 Evaluarea mizelor de securitate și clasificarea informației și a bunurilor

2.1 Introducere

În toate formele de management, și decizii manageriale, trebuie făcută o evaluare a ceea ce se află în joc, și care va fi impactul deciziei asupra bunurilor companiei. În managementul securității, exact asta e situația, doar că întrebarea este pusă dintr-un unghi diferit. În loc să caute să maximizeze câștigurile, scopul este să minimizeze pierderile.

Miza managementului securității nu este să caute oportunități pentru profit, ci să limiteze posibilitatea pierderilor.

2.1.1 Scopurile unei evaluări a mizelor securității

O astfel de analiză caută să găsească răspunsuri la întrebarea dublă: „Ce s-ar putea întâmpla și, dacă s-ar întâmpla, ar fi grav?”

Acest lucru arată că în sectorul securității, mizele pot fi văzute ca fiind consecințele evenimentelor care perturbă operațiunile planificate ale unei întreprinderi sau organizații.

2.1.2 De ce și când ar trebui făcută o evaluare?

Întrebarea de bază: „Ce s-ar putea întâmpla și, dacă s-ar întâmpla, ar fi grav?” este întrebarea care este pusă de fiecare dată când reflectăm asupra modului în care ar trebui să desfășurăm operațiunile. Asta se poate întâmpla atunci când se începe un nou proiect IT, în timpul unei recenzii a unei strategii, sau când este creat un plan de securitate.

Întrebarea ce s-ar putea întâmpla este una bună care dă dovadă de bun simț și prudență. Reflectarea la cât de grave ar putea fi efectele, izvorăște din nevoia de a aloca mai mult timp și atenție evenimentelor mai grave. Motivele din spatele acestui fapt sunt atât de natură economică cât și culturală:

- Bugetele sunt întotdeauna limitate, și de aceea este normal să dăm prioritate protecției împotriva evenimentelor grave.
- Securitatea aduce deseori constrângeri. Este mai ușor să le accepți atunci când miza este mare.

Dacă suntem de acord că măsurile de securitate ar trebui să fie în concordanță cu nivelul de gravitate al potențialelor defecțiuni, atunci există mai multe moduri de a continua:

- Analize tipice pentru fiecare defecțiune, însoțite de alegerea soluțiilor corespunzătoare,
- Abordări mai sistematice cu soluții generice folosite împotriva defecțiunilor tipice și praguri de gravitate pentru defecțiuni. Această a doua abordare conduce la noțiunea de „clasificare”, care va fi discutată mai târziu.

Oricare abordare ar fi aleasă, primul pas îl reprezintă identificarea potențialelor defecțiuni și a gravității lor.

Atunci când se face acest lucru, este preferabil să se facă sistematic, și nu degajat, astfel încât resursele necesare să poată fi dedicate și coordonate corespunzător.

2.2 Definirea mizelor de securitate: scara de valori și clasificarea defecțiunilor

Analiza mizelor de securitate cuprinde:

- Identificarea defecțiunilor suspectate,
- evaluare a gravității acestor defecțiuni, sub forma unei scări de valori a defecțiunilor,
- Clasificarea bunurilor¹ folosind cele trei criterii de bază (Disponibilitate, Integritate, Confidențialitate). Pot fi completate tabelele folosite pentru analiza riscului.

Scara de valori a defecțiunilor și clasificarea informațiilor și a bunurilor sunt două modalități separate de a exprima mizele de securitate.

Prima este mai detaliată și oferă mai multe informații managerilor de securitate. Cea de-a doua este mai globală, și mai utilă în comunicarea nivelului de sensibilitate, dar mai puțin precisă.

2.2.1 Scara de valori a defecțiunilor

Identificarea defecțiunilor sau a potențialelor evenimente este un proces care începe cu activitățile întreprinderii și este formată din identificarea posibilelor defecțiuni în procesele operaționale. Va rezulta în:

- descriere a posibilelor tipuri de defecțiuni,
- definiție a parametrilor care influențează gravitatea fiecărei defecțiuni,
- evaluare a pragurilor critice ale acestor parametri care modifică nivelul de gravitate al defecțiunii.

Acest set de rezultate formează o scară de valori pentru defecțiuni, numită în MEHARI scara de valori a defecțiunilor.

2.2.2 Clasificarea informațiilor și a bunurilor

Se obișnuiește, în securitatea sistemelor IT, să se vorbească despre clasificarea informațiilor și despre clasificarea bunurilor.

O astfel de clasificare constă în definirea, pentru fiecare tip de informație și pentru fiecare bun IT, și pentru fiecare criteriu de clasificare (clasic: Disponibilitate, Integritate, și Confidențialitate), a indicatorilor reprezentativi ai gravității în eventualitatea că acest criteriu se pierde sau este redus pentru acest bun. Astfel:

- Clasificarea confidențialității pentru o informație reprezintă gravitatea dezvăluirii acesteia unei persoane neautorizate
- Clasificarea integrității pentru o informație reprezintă gravitatea modificării sale ilicite sau neautorizate
- Clasificarea integrității software-ului reprezintă gravitatea modificării sale ilicite sau neautorizate
- Clasificarea disponibilității pentru o informație reprezintă gravitatea ca aceasta să nu fie disponibilă atunci când este necesară pentru a fi procesată
- Clasificarea disponibilității pentru un server reprezintă gravitatea ca acesta să nu fie disponibil atunci când este necesar pentru a rula un proces

¹ Se distinge de obicei bunurile primare (activitățile de afaceri și informațiile legate de acestea) și bunurile auxiliare.

- Etc.

Clasificarea informațiilor și a bunurilor auxiliare reprezintă scara de valori a defecțiunilor definită mai devreme transpusă în indicatori de sensibilitate asociați cu bunurile IT.

2.2.3 Procesul pentru analizarea mizelor de securitate

Procesul pentru crearea scării de valori a defecțiunilor și a clasificării bunurilor sistemelor informaționale sunt descrise în: « Analiza MEHARI a mizelor și Ghidul de Clasificare».

3 Evaluarea stării serviciilor de securitate

3.1 Introducere

Fiecare manager de securitate, din orice organizație, trebuie, la un moment dat, să ia în considerare vulnerabilitatea curentă a organizației, când se confruntă cu diferite posibile riscuri, precum accidente, erori umane, sau acte intenționate.

Vulnerabilitatea este definită în dicționar ca reprezentând expunerea la pericol. Vulnerabilitatea unui sistem informațional reprezintă totalitatea punctelor sale slabe prin care un accident, eroare sau act intenționat ar putea dăuna organizației.

În practică, măsurile de securitate, inclusiv controlul evenimentelor sau al acțiunilor umane, etc. limitează nivelul de vulnerabilitate.

În această măsură, analiza vulnerabilității necesită evaluarea stării securității.

MEHARI consideră că securitatea este implementată prin servicii de securitate. O analiză a vulnerabilității necesită astfel o recenzie a calității acelor servicii de securitate. Pe scurt, această recenzie se va numi Recenzie a Vulnerabilității, sau Auditul de Securitate.

Un audit de securitate pentru a analiza securitatea existentă poate reprezenta baza, sau o parte integrantă, a unui număr de abordări pentru managementul securității. **Oricare ar fi abordarea pentru managementul securității, o evaluare a calității serviciilor de securitate este considerată deseori ca fiind indispensabilă.**

Există mai multe motive pentru asta:

- În primul rând, este întotdeauna mai bine să îți cunoști punctele slabe. Chiar dacă, în
- configurația actuală a sistemului informațional, un punct slab poate fi considerat acceptabil deoarece nu ar rezulta nici o consecință gravă, este mai bine să fie consemnat pentru ca să fie luat în considerare în orice evoluție a sistemului, a mediului său, sau în potențialele atacuri noi.
- În al doilea rând, pentru mulți utilizatori, un punct slab care este lăsat în acea stare este considerat ca fiind o demonstrație că managementul de top nu acordă o prea mare importanță securității din organizație. Cu cât este mai important și mai vizibil punctul slab, cu atât mai negativă va fi percepția asupra securității.
- În ultimul rând, orice atac care reușește să exploateze un punct slab va face întotdeauna o impresie negativă dacă se vorbește despre el, oricare ar fi consecințele reale (a reuși accesarea unui sistem care aparține serviciilor militare de informații și apoi să se vorbească despre asta, va avea întotdeauna un impact asupra mediei, chiar dacă sistemul nu era sensibil).

3.2 Servicii de securitate

3.2.1 Definiție

Un serviciu de securitate reprezintă un răspuns la o nevoie de securitate, exprimată în termeni generici și funcționali care descriu ce ar trebui să facă serviciul, și care se referă în general la anumite tipuri de amenințare.

Un serviciu de securitate descrie o funcție de securitate.

Această funcție este independentă față de mecanismele sau soluțiile reale care asigură implementarea eficientă a serviciului.

De exemplu: serviciul de control al accesului este proiectat (după cum sugerează și numele său) să controleze accesul utilizatorilor, sau să acorde accesul doar utilizatorilor autorizați.

3.2.2 Serviciile și sub-serviciile de securitate

Serviciile de securitate oferă funcții care pot, ele însele, să necesite servicii complementare, sau sub-servicii, după cum vor fi numite. În exemplul anterior, controlul accesului necesită identificarea persoanelor autorizate să acceseze anumite bunuri, ceea ce necesită un serviciu de autorizare care să știe cine este utilizatorul, ceea ce necesită un serviciu de autentificare care să filtreze accesul, care necesită un serviciu de filtrare, și așa mai departe.

Un serviciu de securitate poate, astfel, să fie compus dintr-o serie de sub-servicii care sunt combinate pentru a răspunde unei anumite nevoi. **Fiecare componentă este, în terminologia MEHARI, un sub-serviciu al serviciului de securitate principal.** Fiecare sub-serviciu își menține propriile sale caracteristici pentru propriile sale funcții specifice.

3.2.3 Mecanisme și soluții de securitate

Un „**Mecanism**” reprezintă un mod specific de asigurare a funcției unui serviciu sau sub-serviciu (fie total sau parțial). Acesta poate lua forma, de exemplu, unei proceduri, unui algoritm, sau a unei tehnologii anume.

Pentru sub-serviciul de autentificare, menționat mai sus, mecanismele posibile pentru autentificarea în sistemele informaționale o reprezintă parolele, token-urile, procese și algoritmi pe bază de smart card, sisteme biometrice, și așa mai departe.

Pentru un sub-serviciu dat sunt posibile de obicei mai multe mecanisme. Selecția acestora poate deseori avea un efect direct asupra calității sub-serviciului în discuție.

O **soluție de securitate** reprezintă implementarea reală a unui mecanism și include componentele de hardware și/sau software necesare pentru desfășurarea sa, procedurile de instalare, și suportul operațional, precum și structurile organizaționale necesare pentru utilizarea sa corectă.

3.2.4 Tipuri de servicii de securitate

Unele servicii pot fi considerate a fi măsuri generale, în timp ce altele sunt tehnice.

- Măsurile generale reprezintă măsurile de securitate care sunt considerate a fi în general utile, sau chiar necesare, pentru securitatea sistemului informațional. Totuși, efectul lor poate fi observat la nivelul organizației, operațiunii de securitate sau al conștientizării, dar fără o influență directă asupra situațiilor de risc specifice.
- Măsurile tehnice au un rol specific, un obiectiv direct și un efect imediat în anumite situații de risc care pot fi definite.

3.2.5 Baza de cunoștințe a serviciilor de securitate

MEHARI cuprinde o bază de cunoștințe a serviciilor și sub-serviciilor de securitate. Aceasta combină mai mult de 200 de sub-servicii aplicabile în securitatea sistemelor informaționale. Acestea sunt serviciile care vor fi auditate.

3.3 Evaluarea calității serviciului de securitate

Serviciile de securitate pot varia în performanță; acestea vor fi mai mult sau mai puțin eficiente în activitatea lor, și mai mult sau mai puțin robuste în capacitatea lor de a rezista atacurilor directe, în funcție de mecanismele și procesele folosite.

3.3.1 Parametri obligatorii

Pentru a măsura performanța serviciului, trebuie luați în considerare mai mulți parametri:

- Eficiența,
- Robustețea,
- Permanența.

3.3.1.1 Eficiența serviciului de securitate

Pentru serviciile de natură tehnică, eficiența reprezintă o măsură a capacității lor de a asigura eficient funcția necesară atunci când se confruntă cu utilizatori mai mult sau mai puțin competenți sau cu circumstanțe mai mult sau mai puțin neobișnuite.

Să luăm, drept exemplu, sub-serviciul „Managementul autorizării accesului la sistemul informațional”, care implică atribuirea drepturilor de acces utilizatorilor. Funcția acestui serviciu este de a se asigura că doar acele persoane care au autorizația managementului lor primesc efectiv accesul corespunzător la sistemul informațional.

În practică, eficiența unui serviciu depinde de strictetea controalelor asupra autenticității cererii de autorizare, și de corelarea relației ierarhice dintre solicitant și utilizator. Dacă nu se solicită decât o simplă corespondență, fără semnătură sau certificat, oricine cunoaște puțin procesul de autorizare ar putea să își aloce necorespunzător drepturi de acces, iar calitatea sub-serviciului ar fi considerată ca fiind slabă.

Eficiența unui serviciu care administrează acțiunile umane reprezintă astfel măsura competenței necesare pentru a permite unui utilizator să treacă de verificările existente, sau chiar să le abuzeze.

Pentru serviciile care vizează evenimente naturale (precum detectarea incendiilor, stingerea incendiilor, și așa mai departe), eficiența lor corespunde capacității lor de a se aplica unor evenimente mai mult sau mai puțin excepționale sau obișnuite.

Dacă este vorba, de exemplu, despre un baraj care trebuie să împiedice un râu să se reverse din cauza ploilor abundente, eficiența este direct legată de nivelul apei (puterea inundației) căreia i se împotrivesc. **În practică, puterea va fi măsurată deseori ca o funcție a caracterului mai mult sau mai puțin excepțional al evenimentului.**

Serviciile care oferă măsuri generale nu pot, în principiu, să fie evaluate ca funcție a efectului lor direct, ci doar prin rolul lor indirect.

Eficiența măsurilor generale corespunde capacității lor de a crea planuri de acțiune sau modificări comportamentale semnificative.

3.3.1.2 Robustețea serviciului de securitate

Robustețea unui serviciu de securitate măsoară capacitatea acestuia de a se opune unei acțiuni care este menită să treacă de serviciu, sau să îi restricționeze eficiența.

Robustețea privește doar acele servicii care sunt considerate ca fiind tehnice.

În exemplul precedent (managementul autorizării accesului), robustețea sub-serviciului depinde – mai ales – de cât de ușor este să modifici direct tabelul drepturilor de acces ale utilizatorului, care ar permite astfel cuiva să își atribuie drepturi de acces fără a mai trebui să urmeze procesele normale de control.

Atunci când avem de-a face cu servicii pentru administrarea accidentelor sau a evenimentelor naturale (precum detectarea incendiilor, stingerea automată a incendiilor, și așa mai departe), robustețea lor va acoperi și capacitatea lor de a evita să fie scurt-circuitate sau evitate (fie accidental, sau intenționat).

3.3.1.3 Permanența serviciului de securitate

Calitatea globală a unui serviciu de securitate necesită ca serviciul să fie **garantat în timp**.

Pentru aceasta, orice distrugere a serviciului de securitate sau orice schimbare în parametri care poate interacționa cu eficiența sau robustețea sa trebuie detectată și luate măsuri de remediere.

Permanența depinde, astfel, de viteza de detectare și de capacitatea de a reacționa.

Permanența măsurilor generale reprezintă capacitatea acestora de a fi evaluate în funcție de implementare sau eficiență și necesită de asemenea ca indicatorii și procedurile de control să funcționeze eficient.

3.3.2 Definiția nivelurilor de calitate pentru serviciile de securitate

Calitatea unui serviciu de securitate evaluează eficiența acestuia, robustețea lui, și permanența. Global, de aceea, calitatea unui serviciu de securitate include capacitatea sa de a rezista unui atac prin apărarea sa – deși nici un castel nu poate fi considerat ca fiind complet apărât.

Calitatea serviciului de securitate se notează pe o scară între 1 și 4. Această scară reflectă competența sau hotărârea necesară pentru a trece de sistemele apărare, pentru a le scurt-circuita, sau pentru a împiedica sau a face inutilă detectarea neutralizării serviciului.

Deși această scară de valori permite valori decimale, este util să se dea informații despre valorile întregi pentru un serviciu de securitate.

Calitatea serviciului de securitate evaluată ca fiind de nivelul 1:

Acest serviciu are un nivel minim. Ar putea fi complet ineficient (sau să nu opună rezistență) atunci când se confruntă cu un utilizator obișnuit, fără nici un fel de calificare deosebită, sau slab educat, de asemenea, în domeniul evenimentelor naturale, este posibil să nu fie de folos în problemele de zi cu zi. Pentru măsurile generale, vor avea un efect mic sau nici unul asupra comportamentului sau eficienței organizației.

Calitatea serviciului de securitate evaluată ca fiind de nivelul 2:

Serviciul este de obicei eficient și continuă să opună rezistență în fața hacker-ului obișnuit sau puțin competent. Totuși, nu este cu siguranță suficient atunci când se confruntă cu un profesionist cu experiență în acel domeniu (acesta ar putea fi un profesionist IT, un hoț bine echipat, sau un expert în spargeri fizice). În ceea ce privește evenimentele naturale, serviciul va fi rareori suficient pentru a acoperi evenimentele grave – deși acestea se întâmplă rar. Pentru măsuri generale, un serviciu la acest nivel ar îmbunătăți doar situațiile de zi cu zi.

Calitatea serviciului de securitate evaluată ca fiind de nivelul 3:

Serviciul este mai eficient și rezistă în fața atacurilor și a evenimentelor descrise mai sus, dar ar putea fi insuficient contra atacurilor specializate (hackeri bine echipați și cu experiență, ingineri de sistem specializați, mai ales dacă aceștia au unelte sau experiență în domeniu, spioni profesioniști, și așa mai departe), sau contra dezastrilor naturale cu adevărat excepționale. Pentru măsuri generale, un serviciu la acest nivel ar avea un oarecare efect asupra unui număr mare de circumstanțe, totuși, nu ar oferi cu siguranță nici o garanție pentru probleme sau atacuri grave.

Calitatea serviciului de securitate evaluată ca fiind de nivelul 4:

Acesta este cel mai înalt nivel, și serviciul de securitate va rămâne activ și eficient în fața tuturor evenimentelor și agresiunilor descrise mai sus. Ar putea totuși să fie depășit în circumstanțe excepționale: cei mai buni spărgători de coduri din lume cu cele mai bune unelte de spart coduri din lume (ceea ce este posibil dacă unele țări vor ca acest lucru să se întâmple) sau o combinație excepțională de circumstanțe excepționale.

Procesul folosit de MEHARI pentru a evalua calitatea serviciului de securitate a fost construit pentru a oferi evaluări de calitate care să corespundă cu definițiile de mai sus.

3.3.3 Chestionarele MEHARI pentru evaluarea serviciilor de securitate

Setul de metodologie MEHARI , pe lângă metoda în sine, include și baze de cunoștințe. Una dintre aceste baze este o bază de audit pentru servicii de securitate. Ea este sub formă de chestionare, cu un sistem de evaluare aplicat pentru răspunsuri.

Structura detaliată a chestionarelor și sistemul de evaluare sunt descrise în „*Ghidul MEHARI de evaluare pentru servicii de securitate*”.

3.3.4 Evaluarea directă a calității serviciilor de securitate

MEHARI oferă de asemenea, pentru acele servicii de securitate definite în baza de cunoștințe, un „*Manual de Referințe pentru Serviciile de Securitate*”, care descrie fiecare serviciu, funcția sa, mecanismele și posibilele soluții, precum și acele criterii care ar putea fi folosite pentru a măsura calitatea serviciului.

Astfel, este posibil să se evalueze direct calitatea serviciilor de securitate folosind definițiile pentru calitatea serviciilor și indicațiile oferite în manualul menționat mai sus.

3.4 Procesul de recenzie a vulnerabilității

Serviciile de securitate, așa cum sunt ele definite în MEHARI, sunt funcții de securitate iar aceste funcții sunt implementate prin soluții de securitate care sunt, sau vor fi, instalate în organizație.

În practică, evaluarea vulnerabilității constă în analizarea sau auditul acelor soluții care au fost implementate pentru a asigura funcțiile de securitate.

Totuși, există în general un număr de diferite soluții în cadrul unei organizații date pentru a asigura aceeași funcție de securitate.

De exemplu, controlul accesului fizic în incintă este oferit desigur de diferite mecanisme și soluții – precum pentru accesul la camerele cu computere, sau alte centre tehnice, precum instalațiile PABX, camerele de conferință, și instalațiile electrice importante.

Este de asemenea posibil ca controlul accesului logic la diferite sisteme (mainframe-uri, UNIX, NT, și așa mai departe) să poată fi administrat în mai multe moduri în funcție de sistem.

Înainte ca măcar să ne gândim la un proces de analiză și evaluare a serviciilor de securitate, este necesar, mai întâi, să se identifice acele soluții care trebuie analizate și auditate.

În MEHARI acesta este motivul pentru ceea ce se numește „planul de audit” sau „schema de audit”.

3.4.1 Schema de audit

În mod ideal, fiecare serviciu de securitate ar trebui să fie examinat, și toate aceste soluții care oferă aceste servicii în organizație ar trebui identificate, astfel încât să poată fi auditate individual.

Acest lucru ar conduce probabil la o cantitate mare de muncă pentru un rezultat al cărui nivel al detaliilor ar fi foarte excesiv.

În mod eficient, deseori o singură echipă sau serviciu selectează diferitele soluții care pot fi folosite. Alegerile sunt deseori luate pe baza constrângerilor practice și nu pe baza viziunilor diferite ale cerințelor de securitate. Diferitele soluții de securitate pot folosi mecanisme diferite în timp ce rămân consecvente în ceea ce privește securitatea.

Pe această bază, *MEHARI sugerează crearea unei scheme de audit care să facă distincție între variațiile care vor fi analizate la nivel tehnic, coincidând cu domeniile de responsabilitate.*

Se poate hotărî că este cel mai bine să se analizeze securitatea fizică a birourilor de management, camerele sistemelor informaționale, și alte zone separate una de cealaltă. Procesul detaliat pentru construirea unei scheme de audit este descris în detaliu în „*Ghidul MEHARI de evaluare pentru serviciile de securitate*”.

Această abordare poate părea că simplifică prea mult necesitatea de a analiza fiecare variație la nivel de sub-serviciu, dar experiența a dovedit că, în afara cazurilor excepționale, este bine adaptată la o analiză globală a vulnerabilității și a riscului.

3.4.2 Procesul propriu-zis de recenzie a vulnerabilității

Odată ce a fost definită schema de audit, și variațiile utile au fost identificate, tot ce mai rămâne de făcut este să se evalueze starea serviciilor de securitate corespunzătoare. Acest lucru poate fi făcut prin chestionarele MEHARI pentru audit (unele dintre care e posibil să trebuiască multiplicare), sau prin analiză directă după cum a fost explicat mai devreme. Procesul va rezulta într-o declarație a calității

serviciilor de securitate. Pentru o descriere mai detaliată, vezi „*Ghidul MEHARI de evaluare pentru serviciile de securitate*”.

3.5 Sumar al recenziei vulnerabilității

În sumar, recenzia vulnerabilității rezultă în următoarele elemente livrabile:

- schemă de audit care face distincția între diferite domenii de soluții care trebuie analizate separat.
- evaluare, pentru fiecare domeniu, a serviciilor de securitate. Aceasta va lua în considerare eficiența fiecărui serviciu, robustețea sa, și permanența sa. Această evaluare este realizată fie direct, sau folosind chestionarele MEHARI.
- Un sumar al vulnerabilităților.

4 Analizarea situațiilor de risc

4.1 Introducere

Aproape fiecare document care privește securitatea tratează managementul riscului sau analiza riscului. Totuși, conceptul privind ceea ce constituie un risc nu este neapărat clar sau universal înțeles.

Este incendiul un risc?

Este neplata unei facturi sau un client insolvent un risc?

Este defăimarea de către competitor un risc?

Describe riscul o situație, o serie de evenimente, sau o măsură a pericolului?

Atât de multe întrebări, la care nu se poate răspunde pe deplin în acest document!

Această secțiune va aborda concepte mai clare care sunt mai ușor de înțeles:

- Scenarii de risc sau situații de risc
- Evaluarea nivelurilor de risc, sau pe scurt evaluarea riscului.

Un scenariu de risc reprezintă descrierea unei defecțiuni și modul în care defecțiunea poate avea loc. Defecțiunea reprezintă daunele potențiale, sau deteriorarea directă cauzată de defecțiune, și orice consecințe indirecte. Este neobișnuit să vorbim despre o situație de risc, acolo unde se înțelege că organizația este potențial expusă la un astfel de scenariu.

O situație de risc este deseori identificată ca rezultat al unei analize a mizelor. Totuși ar putea de asemenea să fie identificată la nivelul unui proiect, sau detectată prin căutare sistematică. MEHARI ajută în aceste domenii prin oferirea unei baze de cunoștințe cu scenarii de risc.

Această secțiune presupune că situația/situațiile de risc au fost identificate. Metoda structurată pentru identificarea situațiilor de risc va fi abordată în capitolul 5 al acestui document.

Evaluarea nivelurilor de risc caută să cuantifice noțiunea de pericol. Metoda de evaluare folosită de către MEHARI va fi descrisă în acest Capitol.

4.2 Scenarii de risc

Mai devreme în acest document, s-a explicat că analiza mizelor necesită identificarea potențialelor defecțiuni și o evaluare a gravității lor.

Descrierea defecțiunii evidențiază doar tipul de consecință potențială și poate degradarea inițială a procesului. Pentru a descrie mai bine și a analiza întreg scenariu de risc, este necesar să definim cauzele și originea riscului, sau circumstanțele din care se naște scenariul.

Fiecare scenariu va fi deci descris după cum urmează:

- Tipul de consecință (uneori în relație cu scara de valori predefinită),
- Tipul de bunuri implicate de către scenariu (uneori în relație cu bunurile critice predefinite),
- Tipurile de cauze care pot conduce la situația de risc.

Mai jos este descris un scenariu care poate avea loc:

Descrierea scenariului	
<i>Descrierea evenimentului și a consecinței (consecințelor sale)</i>	<i>Descriere a cauzei și a originii sale</i>
Distrugerea datelor de bază folosite pentru plata salariilor (calculare & parametri)	... datorită unei erori operaționale: o defecțiune a dischetei care nu permite citirea datelor
Distrugerea datelor de bază folosite pentru plata salariilor (calculare & parametri)	... datorită ștergerii intenționate a fișierelor de către un membru al personalului pentru operațiuni

4.3 Analiza unui scenariu de risc: privire generală asupra abordării „globale”

Scopul acestei analize este de a evalua doi parametri caracteristici ai riscului care sunt administrați de către organizație, presupunând că scenariul are loc. Acești parametri sunt:

- Potențialitatea riscului. Aceasta reprezintă, într-un mod calitativ, probabilitatea ca riscul să se producă. Producerea nu poate fi modelată în termeni de probabilitate, care reprezintă o perspectivă cantitativă, așa că MEHARI preferă termenul de „potențialitate”. Potențialitatea reprezintă o funcție a contextului și măsurile de securitate aplicate.

- Impactul riscului asupra organizației, care reprezintă gravitatea consecințelor directe și indirecte ale producerii riscului. Acest impact reprezintă o funcție a impactului maxim, sau a impactului intrinsec, care a fost definită în timpul clasificării în ceea ce privește mizele (sau nivelul pe scara de valori), redusă de către oricare măsuri de securitate adecvate care au fost implementate.

Pentru a cuantifica riscul care corespunde scenariului analizat, se vor face evaluări ale potențialității și ale impactului pe o scară de 4 niveluri. Aceste niveluri sunt descrise mai jos.

4.3.1 Evaluarea potențialității unui scenariu de risc

Obiectivul aici este de a răspunde la întrebarea simplă:

„Cât de probabilă este producerea riscului analizat, și anume că scenariul are loc și creează daune reale?”.

Pentru a face producerea riscului mai mult sau mai puțin probabilă pot intra în joc mulți factori. MEHARI oferă o abordare analitică care face distincția între diferiți factori de risc. El evidențiază ceea ce poate face riscul mai probabil sau, invers, care măsuri de securitate ar putea reduce probabilitatea apariției lui.

Înainte de a examina acești factori, este util să înțelegem scara valorilor de potențialitate.

Scara valorilor de potențialitate:

Nivelul 4: foarte probabil

La acest nivel, scenariul poate fi considerat că va avea loc cu siguranță, și relativ în termen scurt. Atunci când se produce, nimeni nu este surprins.

Nivelul 3: Probabil

Acestea sunt scenariile care se pot produce cu ușurință, într-un termen mai mult sau mai puțin scurt. Speranța că riscul nu se produce este ridicolă, dar dă dovadă cu siguranță de un anumit nivel de optimism. Atunci când se produce, oamenii sunt dezamăgiți, dar nimeni nu este surprins.

Nivelul 2: Improbabil

Acestea sunt scenariile care, în mod rezonabil, pot fi considerate că nu se vor produce niciodată. Experiența din trecut arată că ele nu s-au produs niciodată. Ele rămân, totuși, „posibile”, și nu sunt nerealiste.

Nivelul 1: foarte improbabil

Producerea riscului este total improbabilă. Astfel de scenarii nu sunt strict imposibile deoarece există întotdeauna o posibilitate infinit de mică ca ele să se producă.

Nivelul 0: Neluat în considerare

Aceste scenarii sunt atât de imposibile încât nu sunt incluse în setul de scenarii care trebuie analizate. Deseori, și din motive diferite, scenariile care nu trebuie analizate sunt clasificate la acest nivel.

Evaluarea directă a potențialității este deseori destul de dificilă. Abordarea MEHARI recomandă analiza mai multor factori:

- Expunerea naturală la situația de risc
- Pentru scenariile care privesc actele voluntare, riscul asumat de către răufăcători
- Condițiile în care are loc scenariul

4.3.1.1 Expunerea naturală

Prima chestiune privind potențialitatea o reprezintă nivelul de expunere la risc.

Activitățile unei organizații, contextul său economic, social sau geografic, toate influențează modul în care este expusă la diferite tipuri de risc, independent de măsurile în vigoare.

- O companie high-tech lider de piață este mai expusă la piraterie și spionaj industrial decât altele.
- O companie aflată pe malurile unui râu este mai expusă la riscul de inundație decât altele.
- O organizație care se ocupă de multe tranzacții financiare este mai expusă la posibilitatea de fraudă.

Posibila existență a factorilor care ar putea expune organizația la un tip dat de risc trebuie deci să fie examinată.

Organizația este deosebit de expusă sau protejată atunci când se confruntă cu acest tip de situație?

Potențialitate

Pentru o situație de risc dată, anumite organizații sunt mai expuse decât altele. Cu cât este mai expusă organizația, cu atât mai mare este riscul.

Expunerea la un risc dat poate depinde de mai mulți factori:

- Locul unde se află și mediul său înconjurător, pentru riscuri naturale,
- Câștigurile potențiale pentru răufăcători voluntari: precum furtul, jaful, sau satisfacția intelectuală.
- Probabilitatea ca un act intenționat să vizeze organizația (invers proporțional cu numărul de ținte potențiale)

Este relativ obișnuit ca expunerea naturală la un tip de risc să crească printr-o combinație de circumstanțe:

- Anunțarea unui plan de redundanță, pentru reavoință internă,
- Concentrarea mediei asupra circumstanțelor sau evenimentelor care ar putea deranja populații externe (precum accidente de mediu), sau acordarea unei atenții speciale asupra organizației (de exemplu, anunțarea unor măsuri de securitate puternice).

Invers, este uneori posibil să se implementeze măsuri pentru a reduce expunerea naturală. Aceste măsuri sunt numite, în MEHARI, măsuri structurale:

- Administrarea mediului (fizică, socială, etc.): mutarea,
- Dispersarea potențialelor ținte ale atacurilor intenționate,
- Motivația și managementul crizei.

Expunerea naturală a organizației la un risc dat va fi clasificată pe o scară de la 1 la 4, după cum este descris mai jos:

Expunerea naturală la risc

Nivelul 1: Expunere foarte mică

Independent de orice măsură de securitate, probabilitatea ca un astfel de scenariu să aibă loc este foarte redusă și practic neglijabilă.

Nivelul 2: Expunere mică (abia expus)

Chiar și fără măsuri de securitate, combinația dintre mediu (cultural, uman, geografic sau altul) și context (strategic, competitiv, social) face ca probabilitatea ca un astfel de scenariu să se producă, pe termen scurt sau mediu, mică.

Nivelul 3: Expunere medie (nu deosebit de expusă)

Mediul și contextul întreprinderii sunt de așa măsură încât, dacă nu se face nimic pentru a-l evita, un astfel de scenariu este menit să aibă loc pe termen mai mult sau mai puțin scurt.

Nivelul 4: Expunere mare: (deosebit de expusă)

Mediul și contextul întreprinderii sunt de așa măsură încât, dacă nu se face nimic pentru a-l evita, un astfel de scenariu este inevitabil pe termen foarte scurt.

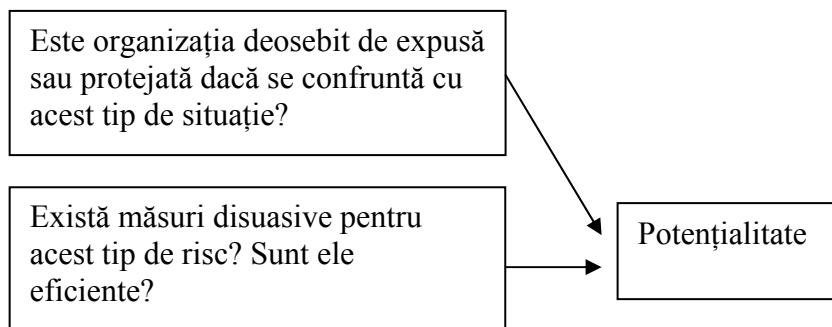
Această evaluare este, de fapt, o primă reflecție asupra nivelului de potențialitate al unui scenariu în absența oricărei măsuri de securitate.

În exemplul de mai devreme „Distrugerea datelor de bază folosite pentru plata salariilor (calcul & parametri) datorită ștergerii intenționate a fișierelor de către un membru al personalului pentru operațiuni”, ar trebui făcută o analiză pentru a vedea dacă există relații conflictuale cu personalul pentru operațiuni, dacă aceștia sunt motivați sau nemotivați, și dacă o astfel de acțiune răuvoitoare va beneficia cuiva anume. Atunci când nu se pot găsi motive anume, entitatea este considerată ca fiind abia expusă (observând că acest lucru nu s-a întâmplat niciodată), cu un nivel de expunere de gradul 2.

O metodă bună de a evalua expunerea naturală este să fie considerată ca o măsură cu potențialitate intrinsecă, sau ca potențialitate fără nici o măsură de securitate în vigoare.

4.3.1.2 Riscul perceput de către răufăcătorul unui act intenționat

A doua chestiune se limitează la acele scenarii care privesc actele intenționate efectuate de către o persoană reală. Multe dintre aceste acte sunt de natură răuvoitoare. Un astfel de act poate reprezenta un risc pentru răufăcător, care va avea un efect disuasiv. Existența factorilor disuasivi ar trebui examinată pentru a struni dorințele potențialilor răufăcători.



Hotărârea asupra unui act răuvoitor poate reprezenta în mod clar un risc pentru răufăcător.

Cu cât percepția riscului este mai mare, cu atât este mai puțin probabil ca răufăcătorul să îl încerce, și astfel riscul pentru organizație este mai redus.

Riscul așa cum este el perceput de către răufăcătorul unui act intenționat depinde de:

- Mijloacele existente pentru a detecta acțiunea și pentru a putea fi găsit răufăcătorul,
- Calitatea dovezilor pentru imputare,
- Sancțiunile aplicate,
- Cunoașterea de către răufăcător a mijloacelor folosite în cazurile anterioare.

Ca și consecință la acest lucru, există unele acțiuni sau măsuri care generează reducerea riscului, numite măsuri disuasive în MEHARI:

- **Detectarea** acțiunilor voluntare încercate și **înregistrarea** acțiunilor efectuate,
- **Atribuirea** acțiunilor intenționate, încercate sau efectuate,
- **Autentificarea** puternică incontestabilă,
- Reglementarea, cu **sancțiuni severe**,
- **Comunicarea** despre sistemele de detectare și înregistrare.

Existența acestor măsuri trebuie deci examinată, dar de asemenea și eficacitatea lor.

Această eficacitate va fi măsurată pe o scară de la 1 la 4, după cum este descris mai jos.

Eficacitatea măsurilor disuasive:

Nivelul 1: Efectul măsurilor disuasive este mic sau nul.

Potențialul atacator poate considera în mod logic că el sau ea nu se supune la nici un risc personal, deoarece este improbabil să existe vreun mod de a identifica răufăcătorul. Acesta poate deci să considere că nu va fi identificat, sau că va avea posibilitatea de a folosi argumente puternice pentru a refuta orice acuzații privind acțiunile realizate, sau că orice pedeapsă va fi foarte ușoară.

Nivelul 2: Efectul măsurilor disuasive este mediu.

Potențialul atacator poate considera în mod logic că el sau ea se supune doar unui risc mic. În orice caz, orice potențial prejudiciu personal va fi suportabil.

Nivelul 3: Efectul măsurilor disuasive este mare.

Potențialul atacator poate considera în mod logic că el sau ea se supune unui risc mare, și ar trebui să își dea seama că va fi identificat cu siguranță, și că pedeapsa va fi gravă.

Nivelul 4: Efectul măsurilor disuasive este foarte mare.

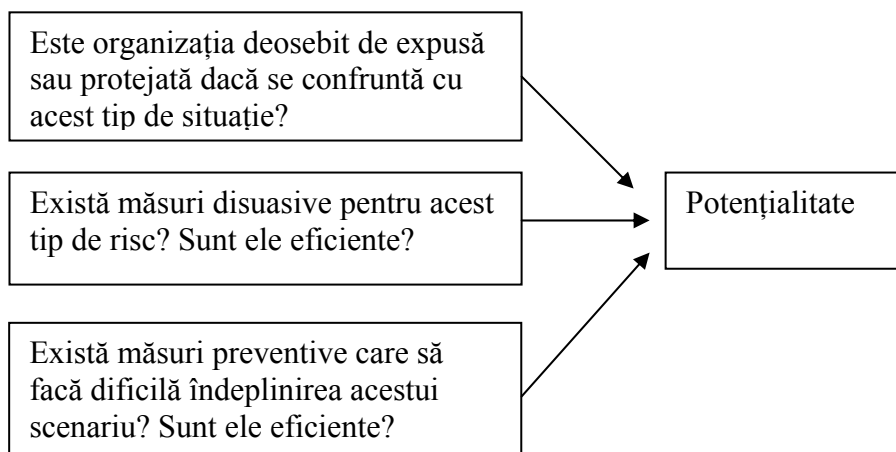
Potențialul atacator poate considera în mod logic că el sau ea ar trebui să abandoneze orice idee de a realiza acțiunea. El ar trebui să-și dea seama că va fi identificat cu siguranță, și că pedeapsa care va rezulta va depăși cu mult orice potențial câștig.

Această evaluare oferă un al doilea nivel de gândire asupra potențialității scenariului.

De exemplu în scenariul descris mai devreme „Distrușgerea datelor de bază folosite pentru plata salariilor (calcul & parametri) datorită ștergerii intenționată a fișierelor de către un membru al personalului pentru operațiuni”, există necesitatea de a examina numărul de persoane care au acces la casetele de stocare a fișierelor bazei de date, pentru a vedea dacă aceste persoane au deseori ocazia de a fi singuri în camera computerelor, și pentru a verifica dacă casetele de stocare se află sub supravegherea camerelor de filmat cu circuit închis. Fără o supraveghere strictă și vizibilă, personalul poate considera pe bună dreptate că nu există nici un risc pentru ei. O astfel de gândire ar putea duce la presupunerea că nu există măsuri disuasive în vigoare pentru acest scenariu (nivelul 1).

4.3.1.3 Condiții pentru ca riscul să se producă

Cea de-a treia și ultima chestiune care trebuie abordată privește condițiile în care scenariul s-ar putea produce, și natura mai mult sau mai puțin obișnuită a acestor condiții.



Un scenariu de risc va ajunge un adevărat dezastru doar dacă anumite condiții sunt îndeplinite simultan.

Cu cât aceste condiții sunt mai obișnuite, cu atât este mai mare riscul de producere.

Natura obișnuită a acestor condiții de producere poate depinde de:

- Natura obișnuită sau excepțională a condițiilor externe (vreme, tip de accident, etc.),
- Nivelul relativ redus de competență necesar pentru un act intenționat,
- Cunoștințele, care sunt mai mult sau mai puțin necesare, despre organizație și contextul său,
- Mijloacele și resursele necesare (umane, financiare, timp, etc.),
- Gradul de noroc sau șansă necesar.

Ca și consecință la acestea, există acțiunile sau măsurile care generează reducerea riscului, numite în MEHARI „măsuri preventive”:

- Măsuri pentru securitatea fizică,
- Măsuri pentru controlul accesului,
- Controale preventive integrate în procesele și aplicațiile computerelor.

Existența acestor măsuri trebuie deci examinată, dar de asemenea și eficacitatea lor.

Eficacitatea va fi măsurată pe o scară de la 1 la 4, după cum este descris mai jos:

Eficacitatea măsurilor preventive:

Nivelul 1: Efectul măsurilor preventive este mic sau nul.

Orice persoană din organizație, sau apropiată ei, sau chiar cineva care cunoaște câte ceva despre ea, poate pune în mișcare acest scenariu, cu mijloacele pe care le are la dispoziție (sau care sunt ușor de obținut).

Cauza acestui scenariu o poate reprezenta circumstanțe perfect obișnuite (utilizare greșită, eroare, condiții nefavorabile obișnuite).

Nivelul 2: Efectul măsurilor preventive este mediu.

Un profesionist poate derula scenariul, fără necesitatea mijloacelor sau uneltelor speciale în afară

de cele disponibile în profesie.

Același rezultat poate fi produs de circumstanțe naturale rare.

Nivelul 3: Efectul măsurilor preventive este mare.

Doar un specialist, sau un profesionist cu unelte sau mijloace speciale, sau un grup de profesioniști care colaborează și care își folosesc mijloacele și uneltele împreună ar putea avea succes.

Nivelul 4: Efectul măsurilor preventive este foarte mare.

Doar câțiva experți hotărâți, cu mijloace excepționale ar putea reuși.

Doar conjuncția unor circumstanțe foarte rare sau extrem de excepționale ar permite ca acest scenariu să aibă loc.

Această evaluare oferă un al treilea și ultim nivel de gândire asupra potențialității scenariului.

Pentru scenariul de exemplu descris mai devreme „Distrugerea datelor de bază folosite pentru plata salariilor (calcul & parametri) datorită ștergerii intenționate a fișierelor de către un membru al personalului pentru operațiuni”, există necesitatea de a analiza dacă întreg personalul de operațiuni, sau aproape tot, este capabil de a reuși într-un astfel de scenariu, sau dacă este nevoie de o expertiză anume pentru a reuși, sau dacă este nevoie de o expertiză specială. În cazul acestui exemplu, întreg personalul pentru operațiuni ar putea fi considerat capabil să reușească, și astfel nivelul măsurilor preventive este mic (nivelul 1).

4.3.1.4 Evaluarea potențialității unui scenariu de risc

Odată ce a fost evaluată expunerea naturală la risc care este analizată, precum și eficacitatea măsurilor disuasive și preventive de a limita potențialitatea au fost evaluate, apoi următorul pas este evaluarea potențialității scenariului care rezultă.

Evaluarea globală va utiliza reflecțiile și rezultatele anterioare, și va aplica definițiile nivelurilor de potențialitate descrise mai devreme.

Pentru scenariul de exemplu utilizat mai devreme „Distrugerea datelor de bază folosite pentru plata salariilor (calcul & parametri) datorită ștergerii intenționate a fișierelor de către un membru al personalului pentru operațiuni”, cu un nivel 2 de expunere naturală și măsuri disuasive și preventive de nivel 1, potențialitatea care rezultă ar putea fi considerată a fi 2, sau „Improbabilă”.

Potențialitatea este, astfel, o evaluare globală a probabilității scenariului de a avea loc până la final, pe o scară de 4 niveluri. Include potențialitatea intrinsecă, măsurată prin expunerea naturală, și doi factori de reducere a riscului: disuasiunea (pentru actele intenționale) și prevenția.

4.3.2 Evaluarea impactului unui scenariu de risc

Aici, obiectivul este de a răspunde la simpla întrebare:

„Dacă riscul care este analizat are loc într-adevăr, care ar fi gravitatea finală a consecințelor?”

Mulți factori pot face consecințele riscului, sau impactul acestuia, mai mult sau mai puțin grave.

MEHARI oferă o abordare analitică care identifică factorii de risc, în timp ce evidențiază influențele care pot face consecințele mai grave, sau dimpotrivă, care măsuri de securitate ar putea reduce gravitatea impactului său.

Înainte de a analiza acești factori, mai jos este definită o scară a impactului, identică în toate sensurile cu cea introdusă în secțiunea analizei mizelor de mai sus din acest document și mai detaliată în „*Ghidul analizei și al clasificării mizelor*”.

Scara impactului:

Nivelul 4: Vital

La acest nivel, defecțiunea posibilă este atât de gravă încât pune în pericol până și existența sau supraviețuirea organizației sau a uneia dintre principalele sale activități.

Dacă organizația ar supraviețui, ar rămâne urme durabile și grave.

Nivelul 3: Foarte grav

Acesta reprezintă defecțiuni foarte grave pentru organizație, fără a compromite neapărat viitorul său.

În termeni financiari, acest lucru ar reduce mult rezultatele anuale, deși acționarii ar putea continua să-și păstreze acțiunile.

În termeni de imagine, nivelul pierderii de imagine a brandului ar necesita multe luni pentru a fi recuperat, deși costul pentru a face acest lucru este greu de evaluat.

Dezastrele care creează dezorganizare evidentă pentru o perioadă de mai multe luni ar fi și ele evaluate la acest nivel.

Nivelul 2: Grav

Acest nivel reprezintă defecțiuni care au un impact accentuat asupra operațiunilor entității, rezultatelor sale sau imaginii sale, dar consecințele sunt de obicei suportabile.

Nivelul 1: Nesemnificativ

Daunele care rezultă dintr-o defecțiune la acest nivel nu au practic nici un impact observabil asupra rezultatelor entității sau a imaginii sale, chiar dacă mai multe persoane vor trebui să cheltuiască mult timp și energie pentru a aduce situația la normal.

Evaluarea directă a impactului final, rezidual a unui risc este deseori dificilă. În abordarea MEHARI, este mai întâi analizat impactul intrinsec, apoi mai mulți factori de reducere. Aceștia sunt:

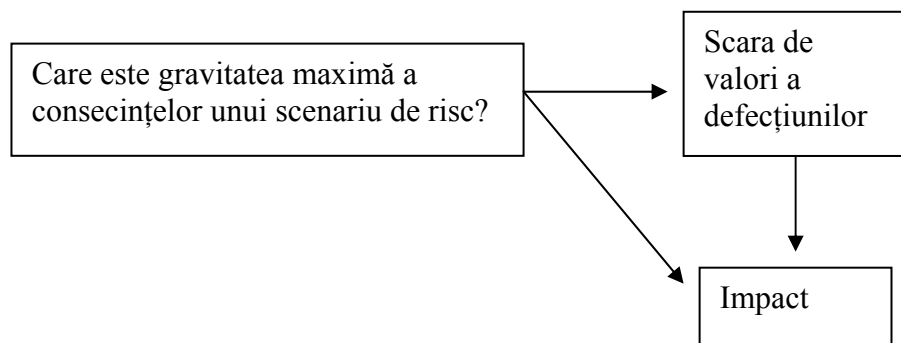
- Atenuarea consecințelor directe ale riscului prin izolarea sau limitarea acestuia,
- Atenuarea consecințelor directe ale riscului prin măsuri paliative,
- Transferul întregului risc sau a unei părți din acesta asupra unei terțe părți.

4.3.2.1 Impactul intrinsec

Dacă scenariul analizat a fost creat ca rezultat al unei analize a mizelor și începând cu o potențială defecțiune, gravitatea defecțiunii a fost deja evaluată folosind scara de valori.

Dacă scenariul este creat fără o analiză a mizelor anterioară, de exemplu ca parte a unui proiect, gravitatea intrinsecă ar trebui evaluată folosind procesul descris în „*Ghidul MEHARI al analizei și al clasificării mizelor*”.

Se presupune de aceea că o evaluare preliminară a impactului scenariului asupra scării de valori a fost făcută.



Merită observat faptul că această primă evaluare este o estimare maximă. De fapt, în timpul acestui pas, măsurile de securitate care ar putea reduce gravitatea consecințelor riscului potențial nu ar trebui luate în calcul.

Aceste măsuri vor fi luate în calcul în timpul analizei riscului.

Prima evaluare a impactului, dedusă din scara de valori a defecțiunilor sau evaluată direct, poate fi considerată ca impact intrinsec, cu alte cuvinte cel mai rău caz (sau valoarea maximă) pentru consecințele riscului fără nici o măsură de securitate.

Pentru scenariul de exemplu utilizat mai devreme „Distrușterea datelor de bază folosite pentru plata salariilor (calcul & parametri) datorită ștergerii intenționate a fișierelor de către un membru al personalului pentru operațiuni”, scara de valori a defecțiunilor oferă o valoare de referință pentru ștergerea unor astfel de date (iar dacă nu apare nici o defecțiune privind datele despre plată în scara de valori, impactul corespunzător ar fi considerat neglijabil). Pentru a continua cu exemplul, scara de valori a defecțiunilor pentru pierderea acestor date ar fi considerată ca arătând nivelul 3 (foarte grav).

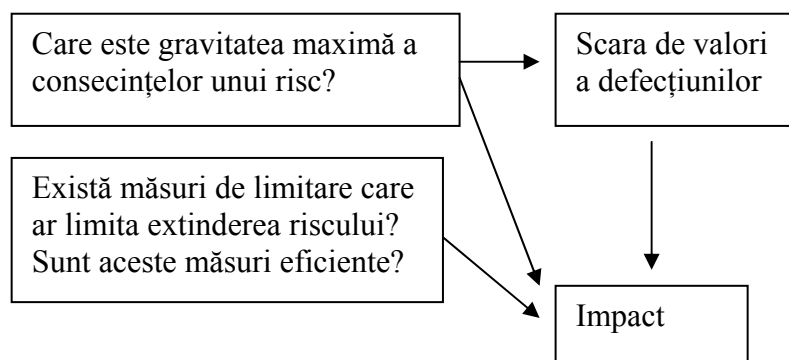
4.3.2.2 Limitarea consecințelor directe: limitarea riscului

Prima chestiune care trebuie adresată privind limitarea riscului este limitarea consecințelor directe ale producerii riscului.

Anumite daune care rezultă dintr-un eveniment pot, de fapt, fi limitate în spațiu sau timp de către precauțiile sau intervențiile anterioare:

- Un incendiu poate fi limitat la o zonă prin mai multe mijloace (pereți parafoc, alți separatori) sau prin intervenție directă (detectare și stingere).
- Inundația poate fi limitată în consecințele sale directe prin intervenție (detectarea scurgerilor sau umezelii, închiderea conductelor) sau prin mijloace specializate (inundare controlată, scurgere naturală).
- O eroare poate fi limitată în efectele sale spațiale (propagare) sau în timp, prin sisteme de detectare sau proceduri de control.
- Proliferarea unui virus poate fi oprită folosind sisteme antivirus.
- Hacking-ul poate fi limitat în timp sau importanță prin sisteme de detectare a intruziunii și alte mijloace asociate.

În mod clar, trebuie pusă problema dacă există factori care ar limita gravitatea consecințelor directe ale unui risc, spațial sau temporal, și asta în comparație cu nivelul maximal inițial de gravitate evaluat la început.



Consecințele directe unui scenariu de risc care are loc efectiv se pot întinde sau propaga în timp și spațiu, sau pot fi limitate.

Riscul va fi mai mare dacă limitarea este mai slabă.

Limitarea consecințelor directe ale unui risc depinde de:

- Izolarea bunurilor unul de altul, sau compartimentarea.
- Detectarea măsurilor specifice riscului în discuție,
- Capacitatea organizației de a reacționa atunci când se confruntă cu acest tip de risc.

Corolar: Există acțiuni sau măsuri de reducere a riscului, și anume măsuri de limitare, de asemenea numite și „măsuri de protecție”² în MEHARI.

- Măsuri pentru izolare și compartimentare fizică,
- **Măsuri de detectare** (intruziune, accidente, erori, etc.),
- **Post-controale** integrate în procese și aplicații ale computerului,
- Capacități de investigație asupra detectării anomaliilor,
- Capacități de intervenție rapidă.

Existența și eficacitatea acestor măsuri trebuie să fie examinată.

Eficacitatea lor va fi evaluată pe o scară de la 1 la 4, după descrierea de mai jos:

Eficacitatea măsurilor de limitare sau de protecție

Nivelul 1: Efectele limitării și limitarea consecințelor directe sunt foarte slabe sau nule.

Fie dauna și consecințele sale directe nu pot fi limitate, fie nu va fi detectată pentru ceva timp.

Măsurile de corectare posibile vor avea deci doar o influență restrânsă asupra nivelului consecințelor directe.

Nivelul 2: Efectele limitării și limitarea consecințelor directe sunt medii.

Chiar dacă dauna și consecințele sale directe pot fi limitate, timpul pentru a le detecta este mare,

² Aceste măsuri, numite măsuri de protecție în Mehari, sunt deseori măsuri de detecție / reacție
Concepte și mecanisme

sau reacția este încetată.

Măsurile de corectare posibile pot avea o oarecare influență asupra impactului, dar consecințele directe sunt încă foarte mari.

Nivelul 3: Efectele limitării și limitarea consecințelor directe sunt mari.

Evenimentul este detectat rapid, cu reacție imediată.

Măsurile de corectare posibile vor avea o anumită influență asupra impactului direct, care rămâne real dar limitat în scop, și manevrabil.

Nivelul 4: Măsurile au un efect foarte puternic.

Începutul scenariului este detectat în timp real și măsurile sunt puse în funcțiune imediat.

Consecințele directe sunt imediat limitate la deteriorare datorită accidentului, erorii sau acțiunii intenționate (uneori răuvoitoare).

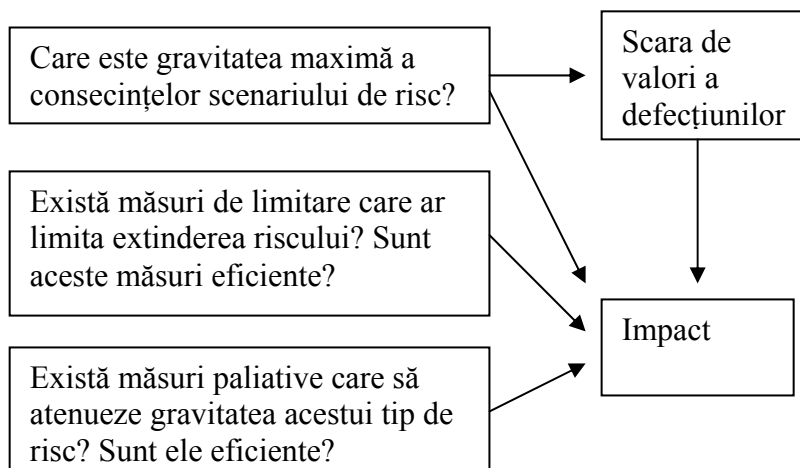
Această evaluare oferă un prim nivel de reflecție asupra nivelului real al consecințelor directe ale scenariului.

Pentru scenariul de exemplu folosit în această secțiune „Distrușterea datelor de bază folosite pentru plata salariilor (calcul & parametri) datorită ștergerii intenționate a fișierelor de către un membru al personalului pentru operațiuni”, ar trebui făcută o examinare pentru a identifica dacă există măsuri de limitare care să asigure intervenția înainte ca vinovații să ștergă complet fișierele cu date și istoria acestora. Răspunsul este probabil nu, dacă datele istorice nu au un sistem de management specific, care să permită detectarea anomaliilor.

4.3.2.3 Limitarea consecințelor indirecte ale unui risc: măsuri paliative

A doua chestiune care trebuie adresată, privind consecințele unui risc, este legată de posibilele reacții odată ce evenimentul a fost detectat și dauna limitată.

Nici o organizație nu ar putea să nu reacționeze, totuși, nivelul consecințelor reale va depinde de calitatea reacției.



Situația de criză generată de producerea unui risc poate fi anticipată și pregătită.

Cu cât pregătirea este mai puțină, cu atât mai mare va fi riscul.

Nivelul de pregătire pentru o situație de criză depinde de:

- Identificarea în prealabil a modurilor de operare degradate acceptabile: funcții minime care trebuiesc îndeplinite și servicii indispensabile,
- Anticiparea și pregătirea soluțiilor paliative corespunzătoare,
- Pregătirea și educarea personalului pentru a face față situațiilor de criză (managementul de criză, comunicarea de criză, etc.).

Corolar: există acțiuni sau măsuri pentru reducerea consecințelor indirecte. Acestea sunt numite „măsuri paliative” în MEHARI, și includ:

- Examinarea în prealabil a ce servicii minime ar trebui oferite precum și planificarea de urgență,
- **Pregătirea planurilor de întreținere și de recuperare** (planuri de rezervă, planuri de continuitate a afacerii, planuri de restaurare, etc.),
- Pregătirea și educarea echipelor (teste tehnice, media-training, etc.).

Existența și eficacitatea acestor măsuri trebuie examinată.

Eficacitatea lor va fi evaluată pe o scară de la 1 la 4, după descrierea de mai jos:

Eficacitatea măsurilor paliative

Nivelul 1: Efectele limitării consecințelor indirecte sunt foarte mici sau nule.

Fie sunt folosite măsuri complet improvizate fie se consideră că acestea nu vor avea nici un efect.

Nivelul 2: Efectele limitării consecințelor indirecte sunt medii.

Soluțiile de recuperare sau paliative au fost planificate în mare, dar lipsesc detaliile. S-a considerat că, din cauza lipsei detaliilor, va exista o lipsă de eficiență corespondentă ale măsurilor paliative. Timpul pentru a restabili operațiunile normale nu poate fi prevăzut cu precizie, sau nu va schimba fundamental gravitatea daunelor cauzate.

Nivelul 3: Efectele limitării consecințelor indirecte sunt mari.

Măsurile paliative nu numai că au fost bine planificate și organizate, ci și testate și validate. Timpul pentru a restabili operațiunile normale poate fi estimat sau cunoscut precis, și este de așa natură încât va reduce considerabil gravitatea consecințelor indirecte ale scenariului.

Nivelul 4: Efectele limitării consecințelor indirecte sunt într-adevăr foarte mari.

Operațiunile normale vor continua fără o întrerupere observabilă.

Această evaluare oferă un al doilea tip de reflecție asupra nivelului real al consecințelor indirecte ale scenariului.

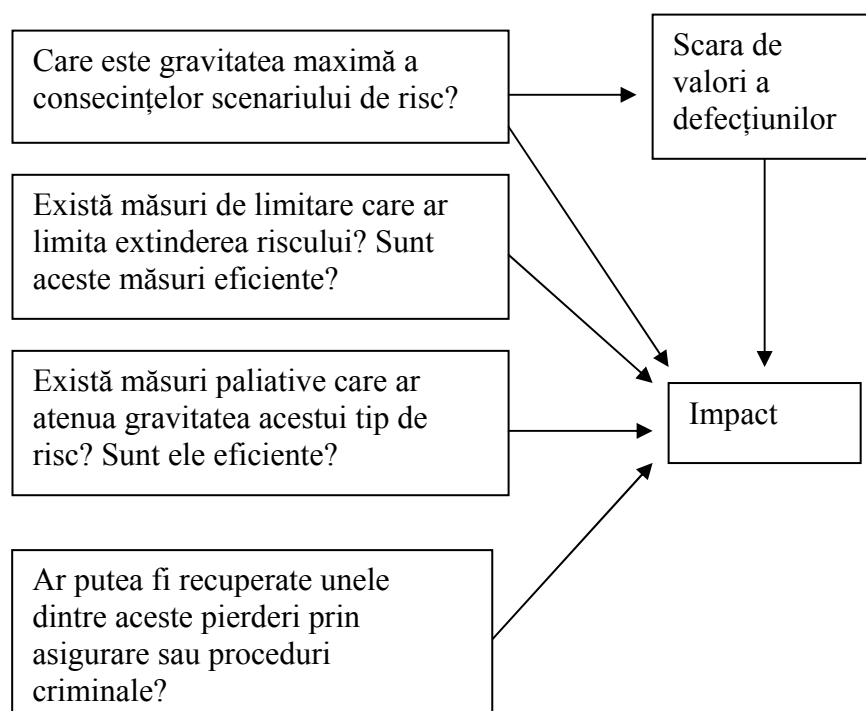
Pentru scenariul de exemplu folosit în această secțiune „Distrușgerea datelor de bază folosite pentru plata salariilor (calcul & parametri) datorită ștergerii intenționată a fișierelor de către un membru al personalului pentru operațiuni”, ar trebui făcută o analiză pentru a vedea dacă sunt făcute back-up-uri ca măsuri paliative, și dacă acestea vor asigura restaurarea bazei de date, măcar pentru datele istorice pentru ultimul an. Acest lucru ar reduce nivelul de impact la 2 (distrușgerea datelor pentru anul curent fiind

evaluată ca fiind de nivel 2 în timpul analizei mizelor), sau ar limita chiar pierderea datelor la luna curentă, ceea ce ar reduce nivelul impactului la 1. Rezultatul va depinde desigur de faptul dacă se fac sau nu back-up-uri, dar și de vârsta lor maxim posibilă (și deci frecvența lor).

4.3.2.4 Limitarea pierderilor totale: transferul riscului

Cea de-a treia și ultima chestiune despre consecințele unui risc privește posibilitatea de a reduce pierderile prin transferarea unora dintre ele asupra unei părți terțe.

În mod tipic, acest lucru ar privi asigurarea sau procedurile criminale.



Pierderile totale pot fi potențial transferate parțial asupra părților terțe precum asigurarea, sau prin proceduri criminale.

Caracterul eficient al acestui transfer depinde de:

- Identificarea în prealabil a situațiilor de risc IT specifice care ar trebui acoperite de asigurare,
- Polițe de asigurare corespunzătoare pentru riscurile care ar trebui acoperite,
- Analiza precisă a situațiilor care sunt excluse, și măsurile ulterioare care sunt luate,
- Pregătirea elementelor de dovadă, cu considerarea procedurilor criminale potențiale, și validarea acceptabilității lor în tribunal („juridic”).

Corolar: există acțiuni sau măsuri pentru a reduce riscul, numite „măsuri de recuperare” în MEHARI. Acestea includ:

- Analiza specifică a riscurilor care ar trebui acoperite de către polițele de asigurare,
- Acoperirea riscurilor care sunt peste nivelul acceptat de către asiguratorii,
- Pregătirea specifică a procedurilor criminale.

Existența și eficacitatea acestor măsuri va fi evaluată pe o scară de la 1 la 4, după descrierea de mai jos:

Măsuri de recuperare:

Nivelul 1: Efectul măsurilor de recuperare este mic sau nul.

Ceea ce poate fi recuperat prin asigurare sau procese legale nu este nimic în comparație cu daunele cauzate de impactul global al scenariului și consecințele sale.

Nivelul 2: Efectul măsurilor de recuperare este mediu.

Ceea ce poate fi recuperat nu este neglijabil, dar organizația este responsabilă pentru cea mai mare parte a impactului scenariului. În cazul unui incident major, nu este sigur că transferul riscului ar permite organizației să continue operațiunile.

Nivelul 3: Efectul măsurilor de recuperare este ridicat.

Ceea ce este recuperat prin asigurare sau procese legale este destul pentru a atenua serios impactul scenariului. În orice caz, operațiunile pot continua.

Nivelul 4: Efectul măsurilor de recuperare este foarte ridicat.

Oricât de grav este dezastrul, impactul rezidual este așteptat să rămână suportabil.

NOTĂ:

Definițiile de mai sus corespund cu ceea ce se așteaptă asiguratorii în general. De fapt, polițele de asigurare nu sunt făcute ca să facă consecințele unui risc complet neglijabile ci de obicei pentru a evita insuportabilul, sau măcar pentru a limita scopul consecințelor unui risc grav dar suportabil.

Această evaluare oferă un al treilea și ultim nivel de reflecție asupra nivelului real al consecințelor globale ale unui scenariu.

Pentru scenariul de exemplu folosit în această secțiune „Distrușgerea datelor de bază folosite pentru plata salariilor (calcul & parametri) datorită ștergerii intenționate a fișierelor de către un membru al personalului pentru operațiuni”, ar trebui făcută o analiză pentru a vedea dacă polițele de asigurare ar reduce nivelul de risc, și dacă un caz legal ar avea succes (ceea ce ar presupune, printre altele, că persoana în cauză ar fi găsită vinovată, și ar avea destui bani pentru a acoperi daunele). În cazul acestui exemplu, răspunsul se pare că este nu.

4.3.2.5 Evaluarea impactului global al scenariului de risc

Impactul intrinsec care a fost definit prin scara de valori și evaluarea eficacității măsurilor de atenuare care ar limita impactul riscului (măsuri de protecție, paliative și de recuperare) va oferi impactul global al scenariului.

Pentru evaluarea nivelului global al riscului, vezi definițiile date mai devreme.

În timpul evaluării globale ar trebui luate în considerare nivelurile precedente de reflecție.

În scenariul de exemplu folosit în această secțiune, impactul global rezidual poate fi evaluat la nivelul 2 (grav), sau chiar 1 (neglijabil) dacă, în ciuda absenței măsurilor de protecție sau de recuperare, măsurile paliative sunt considerate a fi suficient de eficiente.

Impactul este deci o evaluare globală a nivelului consecințelor, pe o scară de 4 niveluri, care ia în considerare impactul intrinsec și cei trei factori de atenuare (de protejare, paliativ și de recuperare).

4.3.3 Gravitatea rezultantă unei situații de risc

Gravitatea unui scenariu de risc sau a unei situații de risc este o funcție a potențialității sale și a impactului său.

Aceasta nu este o simplă formulă matematică care folosește cele două valori, ci o judecată asupra acceptabilității (sau nu) a situației.

Ca funcție a potențialității și a impactului riscului care este analizat, singura întrebare care mai rămâne este:

Este situația de risc acceptabilă așa cum este ea, sau dacă nu ce ar trebui făcut?

Pentru scenariul de exemplu folosit în această secțiune „Distrușgerea datelor de bază folosite pentru plata salariilor (calcul & parametri) datorită ștergerii intenționate a fișierelor de către un membru al personalului pentru operațiuni”, trebuie luată o decizie pentru a vedea dacă este sau nu acceptabil ca personalul de operațiuni să poată șterge baza de date, chiar dacă producerea este improbabilă în timp ce impactul său este limitat, dar totuși ridicat.

Dacă se analizează mai multe situații de risc, la diferite momente în timp, se poate să merite crearea unui tabel al deciziilor pentru a asigura coerența deciziilor luate la momente diferite sau de către persoane diferite.

Acest tabel al deciziilor poate fi reprezentat printr-un „tabel al acceptabilității riscului” sau „tabel al aversiunii față de risc” care definește, ca funcție a impactului estimat și a potențialității, dacă riscul este acceptabil.

MEHARI propune trei categorii de risc:

- Riscuri insuportabile, care necesită măsuri urgente, peste ciclurile normale de buget.
- Riscuri inadmisibile, care trebuiesc reduse sau eliminate la un moment dat. Acest lucru ar trebui integrat în ciclul de planificare (planul de securitate).
- Riscuri tolerabile.

Primele două categorii corespund cu ceea ce a fost numit mai devreme riscuri inacceptabile.

Un tabel de probă al acceptabilității riscului este arătat mai jos. În acest exemplu, S reprezintă gravitatea globală evaluată ca funcție a impactului (I) și potențialității (P). Un nivel al gravității de valoare 4 corespunde unui risc insuportabil, de nivelul 3 unui risc inadmisibil și valorile mai mici riscurilor tolerabile.

I=4	S = 2	S = 3	S = 4	S = 4
I=3	S = 2	S = 3	S = 3	S = 4
I=2	S = 1	S = 2	S = 2	S = 3
I=1	S = 1	S = 1	S = 1	S = 2
	P=1	P=2	P=3	P=4

Figura 4: Tabelul acceptabilității riscului

4.3.4 Privire generală asupra procesului de analiză a riscului

Abordarea care a fost descrisă mai sus poate fi rezumată prin figura de mai jos:

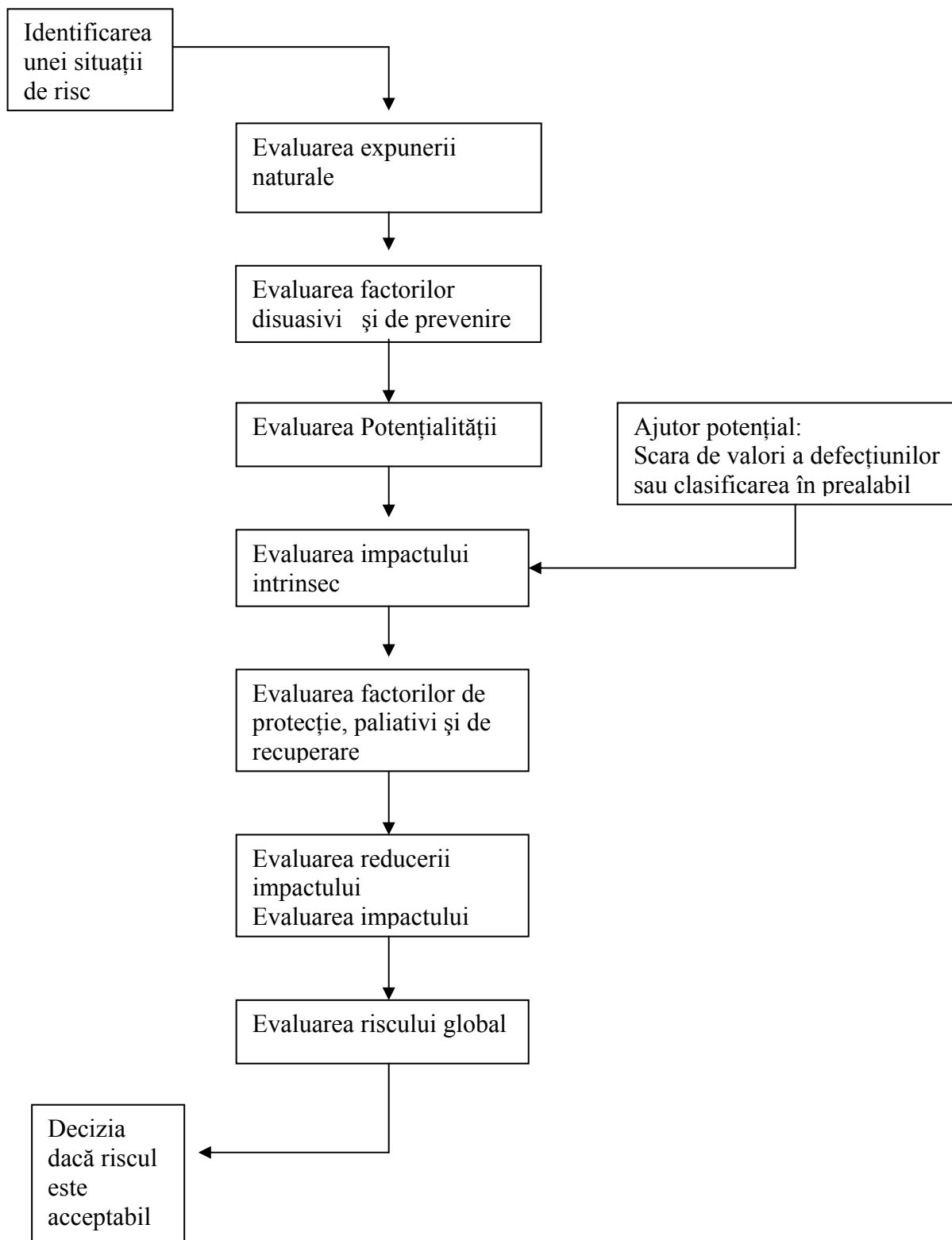


Figura 5: Analiza situației de risc

4.4 Utilizarea bazelor de cunoștințe MEHARI

Printre bazele sale de cunoștințe, MEHARI oferă o bază a scenariului de risc („Manualul MEHARI de referințe”).

Există mai multe situații în care se cuvine să se folosească această bază de cunoștințe:

- Scenariile bazei de cunoștințe sunt descrise într-un mod general, astfel încât să poată fi folosite pentru situații de risc întâlnite mai frecvent. Frecvent, o anumită situație de risc, detectată în timpul unui proiect sau datorită cererii managementului pentru mai multe detalii, corespunde foarte îndeaproape cu unul din scenariile din bază.

Astfel, scenariul de exemplu folosit în această secțiune „Distrușterea datelor de bază folosite pentru plata salariilor (calcul & parametri) datorită ștergerii intenționate a fișierelor de către un membru al personalului pentru operațiuni”, corespunde scenariului 10.31 din baza MEHARI: „distrușterea masivă a arhivelor și a datelor de către personalul de operațiuni”.

- Există și abordări care constau în analiza tuturor situațiilor de risc care par critice. Baza de cunoștințe poate fi folosită pentru a selecta scenariile, și apoi pentru a continua cu analiza acestora.

4.4.1 Folosirea manualului de referințe pentru scenariul de risc

Paragrafele anterioare au oferit definiții generice ale expunerii naturale la risc și ale eficacității măsurilor disuasive și de prevenire. De asemenea, au fost oferite definiții generice pentru impactul intrinsec, eficacitatea măsurilor de protecție, paliative și de recuperare.

Manualul MEHARI de referințe pentru scenarii oferă, pentru acești factori diverși, și pentru fiecare scenariu din bază, definiții care sunt ajustate corespunzător pentru cazul în discuție. Pe lângă definiții, baza oferă, sub formă de comentarii, detalii privind întrebările pertinente care ajută la evaluarea fiecăruia dintre acești parametri.

Procesul detaliat de analiză a riscului care folosește bazele de cunoștințe MEHARI este descris într-un document specific: „Ghidul MEHARI de analiză a riscului”.

4.4.2 Folosirea procedurilor automatizate MEHARI

MEHARI oferă, în baza sa de cunoștințe, mai multe ajutoare pentru analiza riscului:

- Asistență în evaluarea expunerii naturale,
- Proceduri automatizate pentru evaluarea factorilor de atenuare a riscului (disuasivi, preventivi, de protecție, paliativi și de recuperare) ca funcție a calității serviciilor de securitate dacă au fost evaluate în prealabil de către un audit MEHARI.
- Un tabel generic al impactului intrinsec care poate fi mărit ca rezultat al unei proceduri de clasificare sau direct dintr-o scară de valori a defecțiunilor.
- Proceduri automatizate pentru calcularea potențialității și a impactului, ca funcție a expunerii naturale, și a impactului intrinsec și a factorilor de atenuare a riscului.

Pentru a facilita abordarea globală a MEHARI, aceste ajutoare sunt aplicabile pentru fiecare dintre scenariile la care se face referință în baza de scenarii MEHARI.

Procesul de analiză a riscului care folosește baza de scenarii MEHARI și procedurile sale automatizate sunt detaliate în „Ghidul MEHARI de analiză a riscului”.

4.5 Procesul analizei situației de risc

În sumar, procesul de analiză a situației de risc include o abordare de bază, sau globală, cu posibila

asistență a procedurilor automatizate, în funcție de modul în care este descrisă situația și de existența unui audit anterior a serviciilor de securitate.

Procesul total și capacitățile de asistență pe care le poate oferi MEHARI pentru studiul situațiilor de risc (fie extrase din baza MEHARI sau asemănătoare) sunt arătate mai jos:

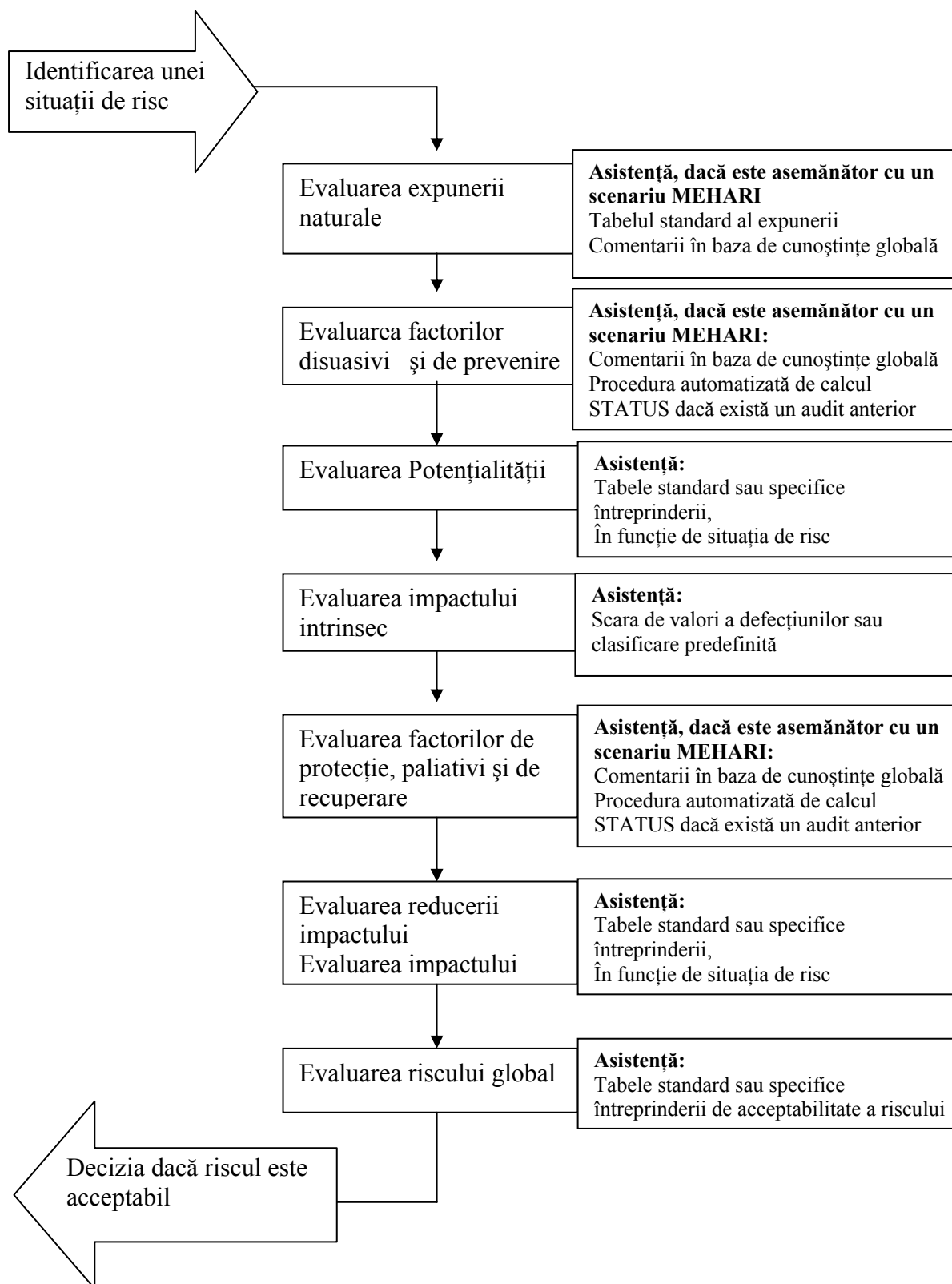


Figura 6: Procesul de analiză a riscului, și ajutorul și asistența MEHARI

Merită menționat faptul că procedurile automatizate menționate mai sus sunt opționale pentru fiecare pas. Practic, asta înseamnă că rezultatele generate de ele ar trebui considerate întotdeauna ca propuneri, și să fie validate înainte de a fi acceptate și aplicate în organizație.

4.6 Sumar al abordării analiza riscului

În sumar:

- situație de risc poate fi caracterizată de către potențialitatea sa intrinsecă și de impact, în absența oricăror măsuri de securitate.
- Potențialitatea intrinsecă și impactul pot fi evaluate.
- Măsurile de securitate pot reduce riscul intrinsec prin factori semnificativi de reducere a riscului.
- Factorii de reducere a riscului pot, ei înșiși, să fie evaluați.
- Pe această bază, este posibil să evaluăm potențialitatea reală, impactul rezidual, caracteristici riscului, și să deducem un indicator al gravității riscului.
- MEHARI oferă unelte pentru a asista pe parcursul acestui proces de analiză și evaluare.

5 Identificarea situațiilor de risc

Capitolul anterior a tratat analiza unei anumite situații de risc. Identificarea acelor situații de risc care trebuie analizate reprezintă evident un stagiul anterior important pentru care uneltele sunt cheia.

Există două modalități principale de identificare a riscului:

- abordare directă, care folosește scara de valori a defecțiunilor,
- abordare organizată și sistematică cu o evaluare automatizată care folosește baza de scenarii oferită de MEHARI.

5.1 Abordarea directă care folosește scara de valori a defecțiunilor

Fiecărui tip de defecțiune, identificată în timpul unei analize de securitate a mizelor și trecută în scara de valori a defecțiunilor, îi corespunde un set de scenarii care au fost identificate prin căutarea cauzelor posibile pentru defecțiune, sau prin originile sale posibile (vezi explicația din subsecțiunea Scenarii de risc).

Este, astfel, ușor să se construiască o bază a scenariilor de risc ca rezultat al scării de valori a defecțiunilor.

Toate scenariile cu un nivel înalt al consecințelor (nivelul 3 sau 4) ar trebui să fie considerate ca fiind critice și examinate mai în detaliu.

5.2 Identificarea sistematică folosind baza de cunoștințe

MEHARI oferă de asemenea asistență în identificarea sistematică a situațiilor de risc.

Identificarea sistematică va folosi baza de cunoștințe MEHARI a scenariilor de risc și procedurile automatizate descrise deja în capitolul anterior. Acest lucru se bazează pe:

- analiză preliminară a mizelor de securitate, întrucupată de o scară de valori a defecțiunilor și clasificarea bunurilor primare și secundare.
- Un audit de securitate.

Procedurile automatizate sunt folosite pentru a evidenția acele scenarii care ar putea avea o gravitate inacceptabilă (de obicei 3 și mai mult) folosind tabelul de acceptabilitate a riscului.

Din baza de scenarii specifică și evaluarea automatizată a gravității lor, este ușor să se selecteze scenariile critice. Asta înseamnă acele scenarii care trebuie analizate folosind o abordare de analiză a riscului precum s-a descris în capitolul anterior.

NOTĂ: Ar fi înțelept să se ia în considerare, pentru această selecție automată, un tabel al acceptabilității care este relativ sever. Acest tabel poate fi diferit atunci când este folosit pentru a identifica scenarii critice față de cel folosit pentru identificarea gravității finale și totale a situației de risc. Luați în considerare tabelul (relativ sever) arătat mai jos:

I=4	S = 3	S = 3	S = 4	S = 4
I=3	S = 2	S = 3	S = 3	S = 4
I=2	S = 1	S = 2	S = 3	S = 3
I=1	S = 1	S = 1	S = 1	S = 3
	P=1	P=2	P=3	P=4

Funcția gravității (S) Potențialității (P) și a Impactului (I)

5.3 Cele două abordări sunt complementare

În mod clar, cele două modalități de identificare a situațiilor de risc critice (selecția directă, folosind scara de valori a defecțiunilor, și identificarea automată, folosind bazele de cunoștințe) încep cu puncte de vedere diferite și vor evidenția, inevitabil, scenarii diferite.

Prima abordare va evidenția scenariile care sunt cel mai aproape de activitățile de bază ale organizației și de problemele managerului, astfel încât să fie mai relevante pentru utilizatori. A doua abordare este mai detaliată, deși mai generică, și va scoate la iveală în plus acele scenarii care au un impact mai slab dar o potențialitate mai mare care ar fi putut trece altfel nevăzute în folosirea unei abordări directe.

Cele două abordări sunt complementare și ar trebui derulate simultan.

6 Utilizarea modulelor Mehari

Modulele MEHARI pot fi aplicate într-o mare varietate de moduri. La fel, există multe abordări de management al securității diferite care pot beneficia de MEHARI și bazele sale de cunoștințe. Nu există, astfel, motive pentru a impune o utilizare standard a modulelor.

Acest capitol țintește să ilustreze valoarea adăugată a MEHARI în managementul securității, prin trei abordări structurate pe care cei care le-au conceput au avut ocazia să le implementeze, și care și-au dovedit eficacitatea.

6.1 Planuri de securitate pe bază de analiza riscului

În general, planurile de securitate sunt create pentru a defini, desfășura și implementa sau consolida servicii de securitate.

Această subsecțiune va descrie planuri care sunt create folosind o analiză a riscului organizată și metodică.

Înainte de a merge mai departe, ar părea util să se facă distincția între două niveluri diferite de decizie:

- Mai întâi, un nivel central de decizie, care asigură consecvența acțiunilor și faptul că sunt potrivite pentru mizele colective ale organizației.
- Un al doilea nivel este cel al unităților autonome, care iau decizii locale necesare pentru securitate. Aceasta este o situație clasică pentru organizațiile mari, dar devine mai comună, pentru organizațiile împărțite în Unități de Afaceri separate, fiecare responsabilă pentru propriile rezultate.

Deciziile la primul nivel sunt strategice, în timp ce cele de la al doilea nivel sunt de natură operațională.

Un alt mod de a distinge între aspectele strategice și operaționale este de a lua în considerare caracterul pe termen lung sau scurt al deciziilor.

- Nivelul strategic privește deciziile pe termen lung, cele care sunt asociate cu funcțiile de bază ale organizației și sunt independente de procesele sau tehnologia care este implementată.
- Nivelul operațional se ocupă cu deciziile de zi cu zi care pot fi schimbate ca funcție a proceselor sau tehnologiei care evoluează.

Nivelul strategic asigură consecvența deciziilor în timp accentuând importanța deciziilor care au un impact pe termen lung.

NOTĂ:

Distincția între deciziile strategice și cele operaționale poate fi neadecvată sau inaplicabilă pentru anumite situații.

O astfel de distincție este, totuși, adecvată pentru viziunea organizațiilor mari cu multe unități separate. Ea poate fi de asemenea adecvată pentru acțiunile pe termen lung. Este, totuși, util să facem această distincție din motive de consecvență sau cicluri de planificare.

Pentru acțiunile selectate sau limitate, distincția oficială dintre deciziile strategice și operaționale poate aduce o complexitate mai mare, și ar trebui deci ignorată.

Totuși, indiferent de stilul de management sau abordare, este logic să distingem între principiile fundamentale care conduc acțiunile pe termen lung din planurile operaționale pe termen scurt.

6.1.1 Abordarea la nivel strategic: identificarea elementelor permanente și independente ale planurilor de securitate operaționale

Scopurile nivelului strategic sunt:

- Să definească scopurile de securitate care vor ghida managerii care iau deciziile privind managementul riscului,
- Să identifice tipurile de soluții care ar trebui implementate ca o prioritate.

Ea reprezintă deci o perspectivă globală, strategică care răspunde la două nevoi diferite:

- Să implice managementul sau unitatea de top al companiei în selecția obiectivelor de securitate. Acest lucru implică acceptarea de către ei a unui anumit număr de riscuri și adoptarea uneltelor de management adecvate pentru nivelul lor.
- Să ofere managerilor de securitate, și managementului în general, elemente adecvate pentru a menține consecvența în deciziile operaționale care sunt luate.

Există trei componente principale la acest nivel, care pot constitui trei pași separați atunci când se creează un plan strategic:

- Crearea sau validarea formală a unei politici de securitate a corporației.
- Fixarea țăelurilor de securitate și convenirea asupra parametrilor de măsurare a riscului.
- Crearea sau validarea formală a unei carte de management al securității a corporației.

Conținutul acestor elemente diferite va fi descris mai jos. Observați că aceste elemente pot fi considerate ca fiind independente de planurile operaționale, dat fiind faptul că, pentru acțiuni care sunt limitate în timp sau spațiu, anumite aspecte pot fi considerate de prisos, și pot fi ignorate.

6.1.1.1 Politica de securitate

Politica de securitate dictează orientările generale de securitate ale organizației.

Este un document de bază important care ar trebui distribuit către întreg personalul. Ar trebui, deci, să fie independent în totalitate de orice metodă sau tehnologie de lucru profesională.

Crearea unei politici de securitate nu face întotdeauna parte din crearea planurilor de securitate. Într-adevăr, este preferabil ca acest document să fie creat cu ceva timp înainte. Totuși, dacă acesta nu există, crearea sa este recomandată viguros dacă organizația este dedicată unui management al securității bazat pe o analiză a riscului globală și sustenabilă.

Politica de securitate ar trebui să acopere patru domenii principale:

- Structura organizațională generală, și mai ales, structurile care sunt implicate în managementul securității:
 - Roluri și funcții ale managerilor de securitate în diferitele unități (funcție centrală, funcție locală, corespondenți de securitate locali, etc.).
 - Roluri și responsabilități ale managerilor de operațiuni și ierarhia lor.
 - Responsabilitatea individuală a fiecărui membru al personalului.
 - Structura consiliului de experți ai organizației (fie acesta formal sau nu) și modul în care este împărtășită expertiza.
- Elementele de bază ale unei culturi de securitate a întreprinderii:
 - Declararea unui număr de principii de bază care ar trebui să fie comune pentru toate departamentele. Printre aceste principii comune, următoarele ar putea fi exemple:
 - Nevoia de a acționa ca funcție a sensibilității informației și a bunurilor; și astfel nevoia de a defini o clasificare a acestora.

- Identificarea și rolul proprietarilor informației sau a bunurilor,
- Condițiile în care sunt acordate drepturile și privilegiile,
- Principiul după care poate fi auditată fiecare acțiune,
- Posibilitatea de a monitoriza munca fiecărui manager, și drepturile și obligațiile managementului lor în acest domeniu.

Această listă nu este exhaustivă și toate principiile care contribuie la asigurarea *consecvenței comportamentului* tuturor celor din cadrul organizației implicați în securitate constituie subiectul acestui capitol.

- Schema generală de clasificare comună folosită pentru toate părțile organizației: niveluri de clasificare, criteriile de clasificare, definiții generale ale nivelurilor de sensibilitate, etc.
- Obligația de a atrage atenția și de a educa personalul în elemente de securitate și elemente cheie care asigură faptul că un astfel de training împărtășește principii comune.
- Elemente federaționale care asigură consecvența soluțiilor care sunt implementate. În considerarea soluțiilor tehnice de securitate implementate, ar trebui luate în considerare în mod deosebit două puncte:
 - Securitatea acelor elemente care sunt, prin natura lor, comune, precum rețeaua globală a întreprinderii și anumite infrastructuri care trebuie împărtășite.
 - Alegerea elementelor de arhitectură a securității care împing organizația într-o anumită direcție pentru structurarea soluțiilor, și care prin natura lor au o influență strategică importantă asupra capacității viitoare de evoluție a sistemelor informaționale.
- Aceste două elemente reprezintă mize ridicate pentru fiecare dintre departamente și pentru întreaga organizație sau întreprindere. De aceea este foarte important să se definească în politica de securitate:
 - Modul în care acțiunile din acest domeniu sunt îndeplinite,
 - Cine ia inițiativa pentru ele, și cine asigură coordonarea,
 - Cine are ultimul cuvânt în deciziile care angajează organizația la o anumită direcție?

În afară de aceste două aspecte specifice, toate acele principii care contribuie la asigurarea *consecvenței deciziilor tehnice* privind securitatea globală a organizației fac obiectul acestui capitol.

- Moduri și mijloace pentru asigurarea managementului operațional al securității.
 - Alegerea metodelor de management al securității,
 - Uneltele de audit al securității, mijloace și structură în cadrul organizației,
 - Structura de monitorizare a securității și crearea sistemelor de măsurare la nivel de departament cât și de corporație.

6.1.1.2 Obiective de securitate și armonizarea parametrilor de măsurare a riscului

În managementul prin analiza riscului, decizia de a accepta sau refuza o situație de risc reprezintă o acțiune de management esențială. Scopurile de securitate sunt formate din criteriile care definesc dacă un risc este acceptabil sau nu.

MEHARI, fără îndoială cea mai avansată abordare pentru managementul riscului, sugerează folosirea unui tabel al acceptabilității (vezi gravitatea rezultantă a unei situații de risc). Un astfel de tabel ar trebui definit în acest stadiu al utilizării abordării.

În ceea ce privește măsurarea, crearea acestui tabel va permite conversia evaluării celor doi parametri, potențialitate și impact, într-o singură măsurare, și anume gravitatea unui risc.

În orice caz, pentru asigurarea consecvenței folosind procedurile automatizate MEHARI în diferite unități ale afacerii în timp, trebuie fixați anumiți parametri folosiți de către aceste proceduri. Acești parametri sunt descriși în „*Ghidul MEHARI de analiză a riscului*”.

6.1.1.3 Carta managementului

Carta managementului tratează aspecte ale politicii de securitate privind relația dintre organizație și angajații săi. Ea este separată de politica de securitate în sine, deseori, există aspecte care nu sunt pentru distribuția către întregul personal.

În general, ar trebui tratate drepturile și obligațiile personalului, dar și cele ale întreprinderii.

Sancțiunile, și modul în care acestea sunt clasificate, ar trebui definite clar.

Felul de puncte care ar trebui acoperite este:

- Capacitatea de urmărire a acțiunilor individuale, și capacitatea de a atribui acțiuni,
- Posibilitatea de a monitoriza activitatea în timp real,
- Posibilitățile pentru proceduri de audit și de control,
- Obligațiile și responsabilitățile personalului,
- Sancțiunile care sunt aplicabile atunci când există o încălcare a eticii companiei,
- Posibilitățile, și limitele investigațiilor în cazul anomaliilor sau incidentelor,
- Etc.

Este important, de la acest nivel strategic, ca regulile pe care întreprinderea sau organizația le va urma și aplica, să fie definite corespunzător pentru personal.

Anumite măsuri, mai ales cele care tratează disuasiunea, sunt eficiente doar dacă organizația are o politică clară și se asigură că aceasta este aplicată ferm, și astfel aplică sancțiunile în caz că se încalcă procedura. Dacă resursele umane sau managementul general nu sunt hotărâți să aplice o politică riguroasă, să urmeze investigațiile necesare atunci când au loc anomalii sau incidente, nu instigă în organizație procedurile de control și audit privind toate acțiunile făcute de personal, este mai bine să se știe imediat pentru a nu baza o strategie pe principii care nu vor fi urmate niciodată.

În orice caz, managerii care vor trebui să ia decizii privind managementul riscului vor trebui să știe ce să facă.

NOTĂ:

Acest tip de document poate fi greu de creat și sensibil la comunicare. Deci crearea sa formală nu reprezintă întotdeauna regula. Totuși, în spiritul MEHARI, acest pas, condus de către CISO sau un consultant pare esențial.

6.1.2 Crearea planurilor operaționale de securitate

La nivelul de plan operațional, abordarea este mai preocupată de specificațiile funcționale ale soluțiilor care ar trebui implementate, și de planificarea unor astfel de soluții.

Acest proces este derulat intern către o entitate cu putere de decizie și rezultate independente într-un plan, cunoscut în MEHARI ca „**plan operațional**”.

Scopurile sale sunt:

- Să ofere o analiză precisă a riscurilor implicate,
- Să ofere o specificație detaliată a soluțiilor și măsurilor de securitate care trebuiesc implementate,
- Să planifice îmbunătățirile necesare în timp.

Abordarea este în principal responsabilitatea CISO sau a managerilor de risc (care ar putea fi manageri de operațiuni), sau a ambilor.

Sunt cinci pași principali în crearea unui plan operațional:

- Analiza mizelor și clasificarea informațiilor și a bunurilor sistemului informațional,
- recenzie a vulnerabilității securității,
- Identificarea și evaluarea riscurilor potențiale pentru entitate,
- Exprimarea necesităților pentru îmbunătățirea securității,
- Crearea unui plan de acțiune pentru securitate.

6.1.2.1 Analiza mizelor și clasificarea

Abordarea MEHARI este descrisă în detaliu în „*Ghidul MEHARI de analiză și de clasificare a mizelor*” și face distincția între:

- Scara de valori a defecțiunilor,
- Clasificarea informației și a bunurilor sistemelor informaționale,
- Crearea tabelului impactului intrinsec folosit de baza de cunoștințe a scenariilor de risc.

Trebuie menționat că, pentru managementul pe bază de analiza riscului, scara de valori a defecțiunilor este obligatorie, în timp ce pasul clasificării formale este opțional. Este suficient să se folosească scara de valori pentru a evalua impactul intrinsec pentru fiecare scenariu de risc analizat. În practică, MEHARI sugerează ca evaluarea impactului intrinsec să fie sistematizată prin utilizarea tabelului impactului intrinsec. Acest lucru fiind folosit mai târziu de către procedurile automatizate oferite de MEHARI.

NOTĂ: Analiza mizelor poate fi considerată ca fiind parte din abordarea strategică, deoarece de obicei rămâne valabilă pentru o perioadă de timp mai lungă.

6.1.2.2 Recenzia vulnerabilității, sau auditul de securitate

Acesta este auditul de securitate care a fost descris în Evaluarea stării serviciilor de securitate. Termenul „audit de securitate” este folosit adesea, deși deseori el nu este mai mult decât o recenzie. Merită observată aici diferența dintre o recenzie care folosește chestionare și un audit adevărat care verifică dacă politicile și regulile sunt aplicate eficient.

6.1.2.3 Identificarea și evaluarea riscului

Acest lucru privește identificarea situațiilor de risc, așa cum se descrie în Identificarea situațiilor de risc, și evaluarea lor cantitativă, așa cum se descrie în Analizarea situațiilor de risc.

Acest pas rezultă într-un set de situații de risc care pot fi considerate inadmisibile, și care trebuie reduse la un nivel acceptabil printr-un plan de acțiune.

6.1.2.4 Exprimarea necesităților de îmbunătățire în securitate

Acest pas este specific acestui tip de management, deoarece privește efectiv analiza unui set de situații de risc care ar trebui tratate global.

Înainte de a crea un plan de acțiune real, există nevoia de a defini ce se cere de la serviciile de securitate care pot transforma situațiile de risc inadmisibile în unele tolerabile.

În cazul obișnuit, unde analiza riscului și recenzia vulnerabilității au fost realizate cu ajutorul unui profesionist în securitate, CISO sau consultantul extern, nu prea există nevoia unei metodologii adiționale

sau a uneltelor specifice pentru a exprima aceste nevoi:

- Analiza, pentru fiecare situație de risc, a tipurilor de măsuri care sunt deja folosite și o evaluare a eficacității lor va da o idee imediată asupra măsurilor adiționale necesare pentru a reduce nivelul de risc.
- Recenzia vulnerabilității sau auditul de securitate oferă adițional o idee clară asupra problemelor majore care trebuie rezolvate, independent de orice analiză a riscului.
- comparație a stării securității, așa cum a fost evaluată prin auditul de securitate, și politica de securitate va rezulta în identificarea nevoilor specifice.

MEHARI oferă, printre alte unelte, un algoritm pentru selectarea măsurilor de securitate. Acest lucru este descris în „*Ghidul MEHARI de analiză a riscului*”.

6.1.2.5 Luarea în considerare a măsurilor generale sau organizaționale

Capitolul Evaluarea stării serviciilor de securitate a pus în discuție măsuri generale care nu au nici un efect direct asupra scenariilor de risc.

Totuși, orice slăbiciune, detectată în măsurile generale, trebuie acoperită în timpul creării planurilor operaționale. Aceste măsuri, deși pot să nu aibă nici un efect direct asupra scenariilor de risc, pot fi indispensabile în motivarea personalului și în determinarea lor pentru a adopta scopurile de securitate ale organizației.

Cel mai adesea, acest lucru necesită doar bun simț. Asistența unui profesionist în securitate va fi de obicei destul pentru a se asigura că punctele cele mai importante sunt acoperite.

6.1.2.6 Crearea unui plan de securitate operațional

Așa cum spune în definiția nevoilor de securitate, rareori există nevoia pentru orice unelte specifice sau metodologie pentru a construi un plan de securitate din necesitățile exprimate.

Experiența ar recomanda, totuși, că este mai bine ca un prim pas să se grupeze măsurile în jurul proiectelor cu aceeași temă (securitatea logică, planificarea de rezervă, etc.), sau în sub-proiectele mai specifice (în planificarea de rezervă există „realizarea rezervelor”, „refacerea după rezerve”, „planificarea continuității misiunii”, etc.). Sub-proiectelor ar trebui atunci să li se aloce un nivel de prioritate, luând în considerare impactul lor asupra gravității scenariilor și potențiala dificultate de implementare (dat fiind că unele proiecte impun constrângeri asupra altora).

6.1.3 Consolidarea planurilor operaționale din diferite departamente independente

Această fază, care se desfășoară pe toată întreprinderea, asigură consolidarea și consecvența planurilor operaționale din diferitele departamente independente și oferă un cadru pentru arbitraj, dacă este necesar.

Acest lucru poate reprezenta și o ocazie de a re-echilibra diferite departamente, dacă grupul responsabil pentru consolidare are acest mandat.

Figura de mai jos ilustrează abordarea generală.

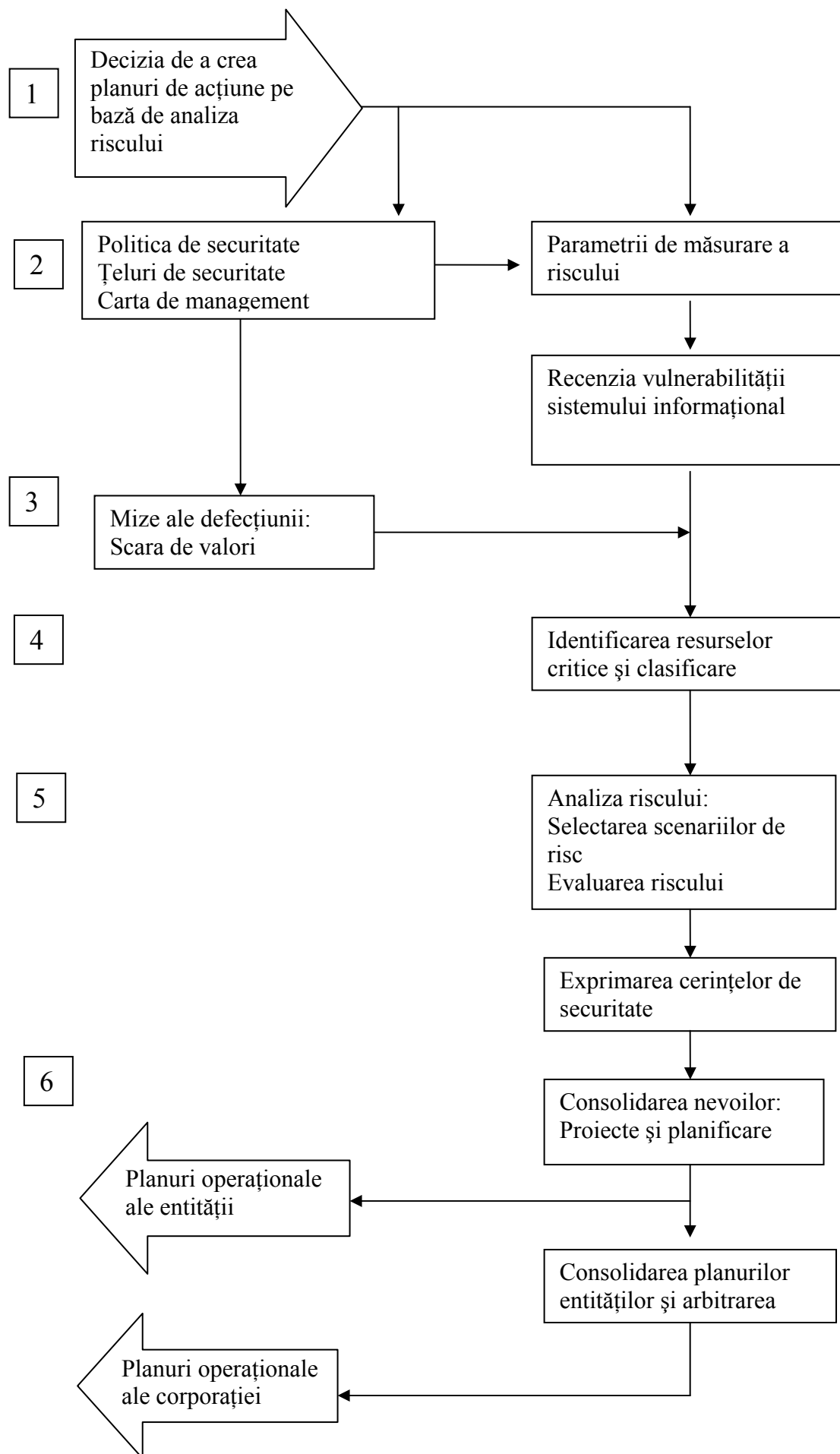


Figura 7: Crearea planurilor de securitate pe bază de analiza riscului

6.2 Planuri de securitate pe baza unui audit

O abordare relativ obișnuită este de a crea planuri de securitate direct ca rezultat al unui audit de securitate, sau după o recenzie a vulnerabilității.

Multe persoane, care au folosit în trecut metodologia Marion, au aplicat pur și simplu pasul 3 al acelei metodologii: un plan de acțiune pe baza unui audit.

În funcție de circumstanțe, această abordare poate fi practică, iar MEHARI oferă mijloacele pentru aceasta.

6.2.1 Procesul pentru crearea planurilor de securitate pe baza unui audit

Procesul pentru derularea unui audit este extrem de simplu: cuprinde o recenzie a vulnerabilității și planurile de acțiune care rezultă pentru îmbunătățirea acelor servicii care nu au un nivel al calității suficient de ridicat.

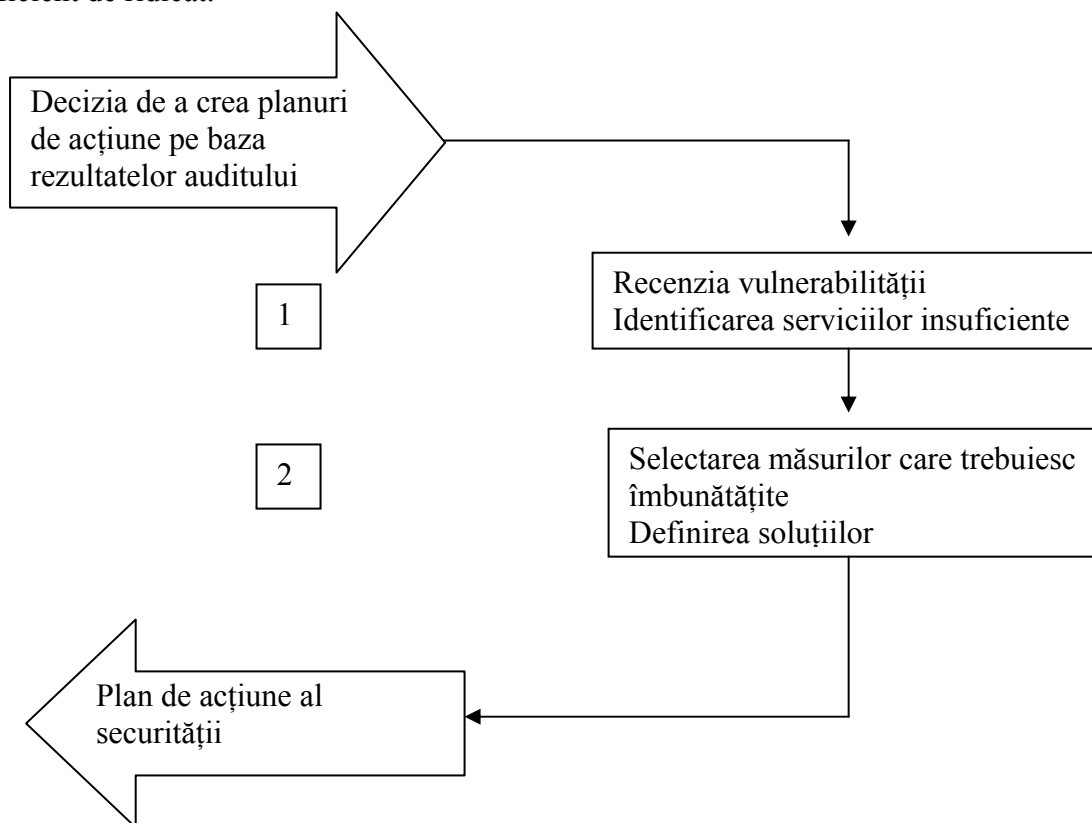


Figura 8: Administrarea securității printr-un audit

6.2.2 Chestionarul de audit și evaluarea întrebărilor

Trebuie puse în discuție două puncte privind chestionarul folosit în timpul unui audit:

- Poate un chestionar care este specific pentru această abordare să fie același cu cel folosit în timpul analizei riscului?
- Poate, și ar trebui, evaluarea răspunsurilor să fie la fel?

Nu există un răspuns universal la aceste întrebări, iar răspunsurile lor vor depinde de cât de matură este organizația în ceea ce privește securitatea.

Dacă organizația se află doar în stadiul de prime reflecții asupra securității sistemului informațional, o evaluare ușoară ar trebui să fie suficientă. Totuși, dacă a existat deja de ceva timp o abordare serioasă pentru securitatea sistemului informațional, un audit mai detaliat ar fi mai indicat. Primul caz va încerca să identifice cele mai evidente slăbiciuni și să le corecteze în timp ce mărește vigilența managementului și să accepte faptul că anumite slăbiciuni vor rămâne. În cel de-al doilea caz, totuși, se va crea un plan complet pentru a avea o acoperire omogenă care să ofere un nivel al securității satisfăcător.

6.2.2.1 Politicile de referință în securitate și notarea pentru un audit de evaluare ușoară

Termenul de „politici de referință în securitate” se referă în general la setul de reguli care vor fi verificate în timpul unui audit. În acest caz, include setul de întrebări care vor fi adresate.

Într-un audit de evaluare ușoară, nu se intenționează să se adreseze întrebări mai profunde, ci să se caute o evaluare generală a stării securității și principala sa slăbiciune.

Foarte des, doar funcțiile de bază vor fi analizate, fără a căuta să se verifice robustețea sau permanența soluțiilor care sunt implementate.

Evaluarea ușoară folosește un chestionar specific care caută să identifice care domenii de securitate sunt acoperite în prezent și care nu.

Cu acest lucru în minte, evaluarea întrebărilor este simplă și nu există nici un motiv pentru a introduce un sistem mai bun de evaluare precum cel folosit de recenzia MEHARI a vulnerabilității.

Întrebările vor fi notate doar de către un sistem de evaluare simplu.

6.2.2.2 Politicile de referință în securitate și notarea pentru un audit detaliat

Spre deosebire de evaluarea ușoară, un audit detaliat caută să verifice toate aspectele serviciilor de securitate (eficacitate, robustețe și permanență). Este deci aceeași abordare din punct de vedere global precum cea necesară pentru o analiză a riscului. Pot fi folosite aceleași chestionare și același sistem de evaluare ca pentru analiza riscului.

Totuși, deoarece auditul nu are aceeași poziție în cele două abordări generale, sunt necesare câteva puncte de clarificare.

Într-o analiză a riscului, după recenzia vulnerabilității, există un stadiu de analiză unde realitatea recenziei poate fi pusă sub semnul întrebării, fie de tehnicieni sau de utilizatori. Recenzia poate fi contrabalansată de către analiza riscului.

Auditul, într-o abordare de analiză a riscului, poate fi bazat pe răspunsuri la întrebări, fără nevoia de a verifica adevărul răspunsurilor date.

Cu o abordare a managementului bazată doar pe audit, lucrurile nu stau la fel. Nici un stadiu nu permite ca rezultatul să fie contestat. Răspunsurile trebuie deci să fie verificate, pentru a asigura un rezultat viabil. Acest lucru nu era important în cazul evaluării ușoare, dar este un element cheie pentru un plan de securitate pe bază de audit.

De aceea este important să se termine o recenzie a vulnerabilității de către un audit al practicilor reale

6.2.3 Pragul de acceptabilitate al calității serviciului de securitate

Tot așa cum trebuie luată o decizie privind riscurile inacceptabile în timpul analizei riscului, trebuie, în această abordare de management, luată o decizie privind pragul sub care calitatea serviciului de securitate este considerată inacceptabilă.

Deciderea asupra nivelului acestui prag va depinde, din nou, de maturitatea organizației.

În timpul unei evaluări ușoare, nu are nici un sens să fim deosebit de ambițioși. Scopul ei este doar să corecteze acele slăbiciuni care sunt cel mai evidente. Pragul calității serviciului poate deci să fie relativ scăzut (între 2 și 2.5).

Pentru un audit detaliat, și pentru administrarea securității pe bază de audit, ar părea mai bine și mai adecvat să se aleagă un prag mai ridicat (3, de exemplu).

6.2.4 Crearea planurilor de acțiune

Crearea planurilor de acțiune este deosebit de simplă cu această abordare, deoarece ea este un rezultat direct al recenziei înseși.

Simpla analizare a motivului pentru care un serviciu nu a avut o notă satisfăcătoare, cu alte cuvinte acele întrebări cu un răspuns negativ vor oferi o alegere a acțiunilor.

Așa cum s-a explicat deja pentru planurile de securitate de către entitate pe baza analizei riscului, este de cele mai multe ori mai bine să se grupeze diferitele măsuri asupra cărora s-a luat o hotărâre în proiecte consecutive (securitate logică, planuri de rezervă, și așa mai departe), sau chiar în sub-proiecte specifice. Apoi, pot fi alocate acestor proiecte prioritățile corespunzătoare, incluzând poate constrângerile implementării.

6.2.5 Luarea în considerare a mizelor

Este clar cu această abordare că procesul de bază nu prevede explicit includerea mizelor de securitate atunci când se iau decizii, ci doar valorile vulnerabilității.

În practică, mizele sunt deseori incluse informal în timpul creării planurilor de acțiune de către experții în securitate care participă la acest pas. Pertinența planurilor de acțiune va depinde de aprecierea de către ele a mizelor, sau de modul în care au fost capabile să le evalueze.

În mod clar, includerea unui pas pentru crearea scării de valori și clasificare poate îmbunătăți serios pertinența planurilor de acțiune de securitate pe bază de audit.

Abordarea corespunzătoare este rezumată în figura de mai jos:

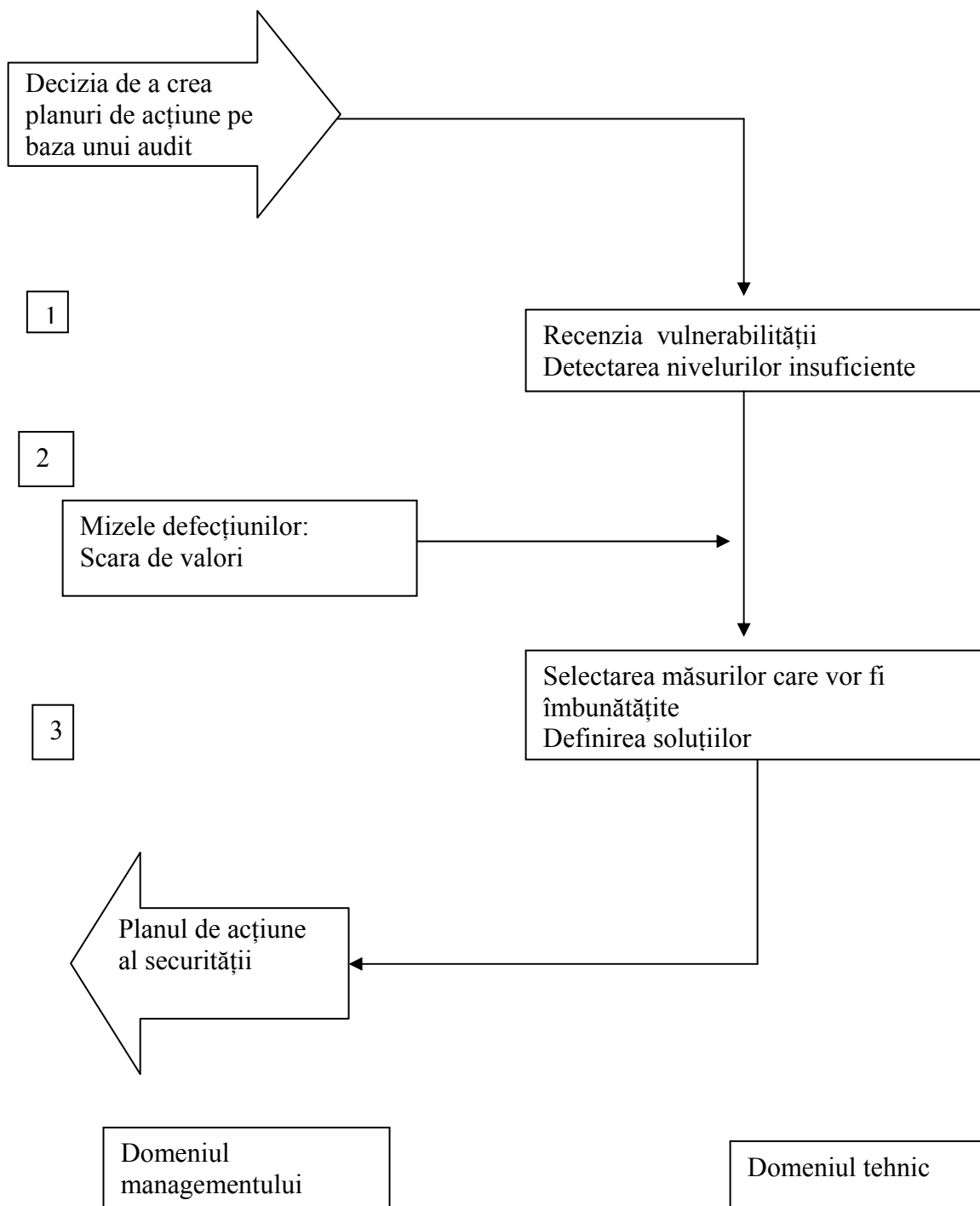


Figura 9: Managementul securității prin audit și mize

6.3 Securitatea proiectelor de dezvoltare

Până acum, acest document a discutat diferite metode de management care pot fi folosite pentru a crea planuri de acțiune generale.

Aici va fi discutată problema managementului securității într-un proiect specific, și nu un plan de securitate global (sau operațional).

Abordarea generală folosită pentru un plan pe bază de analiză a riscului va fi reutilizată, dar cu nevoi de adaptare evidente.

6.3.1 Abordarea managementului securității pe bază de proiect

O privire generală a abordării este ilustrată în figura de mai jos:

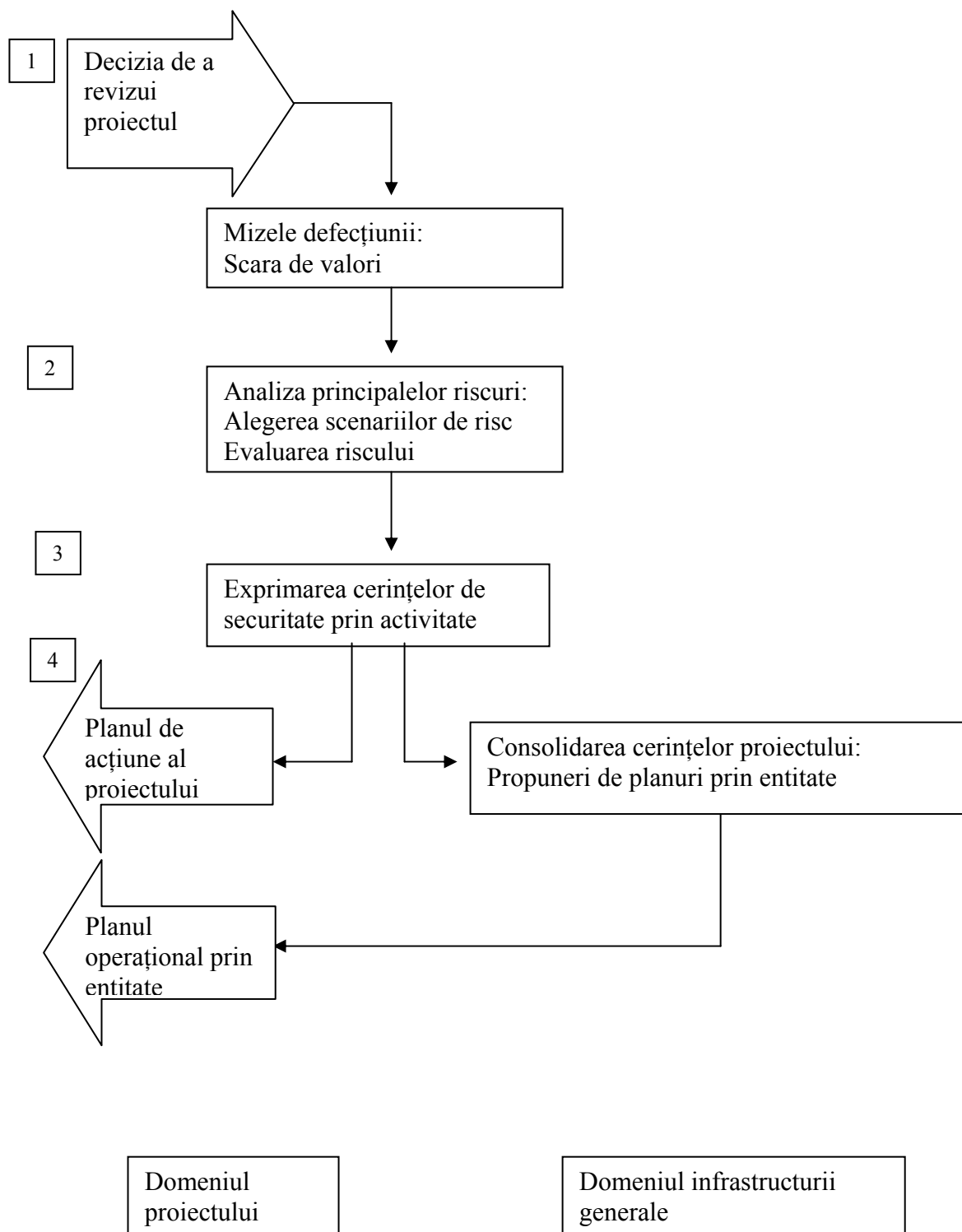


Figura 10: Managementul securității proiectului

6.3.2 Niveluri strategice și operaționale

Nu se face nici o distincție între aceste două niveluri.

Este evident de dorit ca elementele strategice să fie definite independent de orice proiect. Acest lucru nu poate decât să faciliteze sarcinile liderilor de proiect, dar acest pas nu face parte din managementul securității proiectului.

În plus, aceste elemente nu mai au același nivel al nevoii. Este posibil să se folosească o metodă de analiză a riscului într-un proiect fără ca elementele strategice să fie definite în prealabil. Acest lucru ar fi în detrimentul consecvenței dintre proiecte, dar ar putea fi considerat secundar în comparație cu provocarea de a se asigura că liderii de proiect își asumă o analiză a riscului pentru proiectele lor și hotărăsc, ca rezultat, planuri de acțiune pe care le vor integra în planurile lor de proiect.

6.3.3 Nivelul standard al serviciilor de securitate

Nivelul serviciului de securitate care va fi luat în considerare în timpul analizei riscului nu rezultă dintr-un audit formal al securității. Acest lucru se întâmplă din simplul motiv că proiectul nu este încă implementat și evident, la evaluarea inițială, multe puncte nu ar fi încă decise.

Foarte des, nivelurile standard ale serviciului de securitate, așa cum este definit de către politicile de referință ale securității, vor fi incluse în analiza riscului a proiectului.

În absența standardelor definite global, analiza ar considera nivelurile serviciului de calitate ca fiind foarte mici, cu presupunerea că nu trebuie decis nimic la început. În acest fel, abordarea va conduce la crearea unei descrieri a muncii care va fi efectuată pentru a răspunde planurilor de acțiune care rezultă din analiza riscului.

6.3.4 Analiza mizelor și scara de valori a defecțiunilor

Va fi folosit un proces de evaluare generală a mizelor și va fi creată o scară de valori a defecțiunilor specifică proiectului. Totuși, nu este neapărat obligatoriu să se deducă o clasificare.

6.3.5 Analiza riscurilor majore

Va fi aplicată o abordare de analiză a riscurilor unui set de scenarii de risc care sunt direct definite de către liderii de proiect, ca rezultat al scării de valori a defecțiunilor.

Va fi folosită o abordare directă, fără a folosi procedurile automatizate, și se va concentra asupra riscurilor majore.

6.3.6 Crearea planurilor de acțiune

Cerințele de securitate vor fi deduse în final din analiza precedentă a riscurilor. Acestea vor fi deci:

- Direct integrate în specificațiile proiectului, pentru partea specifică care poate fi decisă la acest nivel,
- Distribuite către managerii infrastructurii generale, pentru ca aceștia să le poată integra în planurile lor și în planurile entităților concentrate (sau prezentate pentru arbitrare).

6.3.7 Execuția globală a abordării

Global, abordarea este mult mai simplă decât cea care corespunde creării planurilor de securitate pentru o entitate sau activitate.

7 Recenzia principalelor îmbunătățiri în comparație cu versiunile anterioare ale mehari

MEHARI 2007 aduce îmbunătățiri în comparație cu versiunile anterioare în două domenii principale:

- Crearea tabelului impactului intrinsec,
- Asigurarea, după un audit MEHARI, unui raport asupra stării securității într-un format folosind punctele de control ISO/IEC 17799:2005.

În această nouă versiune a bazei de cunoștințe sunt incluse mai multe îmbunătățiri detaliate.

7.1 Crearea tabelului impactului intrinsec

Pentru a ajuta utilizatorii în crearea unui astfel de tabel, MEHARI 2007 include un proces extrem de detaliat

Acest proces include:

- Descrierea tabelelor care vor fi completate în timpul analizei mizelor de securitate și clasificării bunurilor,
- Indicații pentru a asista în mutarea de la aceste tabele la tabelul impactului intrinsec.

7.2 Măsurile de conformare ISO 17799 după un audit MEHARI

MEHARI și ISO 17799:2005 au scopuri diferite (vezi documentul “Privirea generală MEHARI”). Totuși, există o cerință pentru a obține măsurile de conformare de securitate ISO 17799 (cu punctele de control pentru entitate) ca rezultat al unui studiu MEHARI al vulnerabilității.

MEHARI oferă această măsurare prin chestionare exhaustive care permit cartografierea punctelor de control cerute de către Standard.

Tabelele de corespondență³, oferite în baza de cunoștințe, au fost rafinate pentru a lua în considerare cerințele ISO 17799:2005, repetate de ISO 27001. Anumite întrebări au fost introduse în mod special cu acest scop în chestionarele de audit MEHARI.

7.3 Amintirea îmbunătățirilor anterioare ale lui MEHARI

7.3.1 Evaluarea expunerii naturale

Cu MEHARI, expunerea naturală poate fi văzută ca o „potențialitate intrinsecă”, sau potențialitatea care ar fi obținută fără orice măsură disuasivă sau preventivă. Este cu siguranță un mod bun de a te gândi la expunere. Nu schimbă nimic în aparență, dar este o dimensiune mai ușor de înțeles și de estimat.

Având acest lucru în minte, este clar că, chiar și fără orice măsuri structurale, nu toate scenariile au aceeași potențialitate

- Potențialitatea intrinsecă a unui atac terorist poate fi considerată ca fiind mică pentru majoritatea organizațiilor.

³ RISCARE produce automat raporturi de audit
Concepte și mecanisme

- Cea a unei erori de introducere a datelor, totuși, este fără îndoială destul de mare.

Definiția expunerii naturale

Expunerea naturală este o măsurare a potențialității intrinsece în lipsa oricărei măsuri disuasive sau preventive.

În astfel de condiții, așa cum este explicat în „*Ghidul MEHARI de analiză a riscului*”, evaluarea expunerii naturale poate fi făcută prin evaluarea directă, fără chestionar, a potențialității intrinsece a unui anumit număr de evenimente caracteristice. Acest lucru permite calcularea directă a valorilor STATUS-EXPO pentru scenarii.

NOTĂ: Este important de reținut că expunerea naturală ar trebui (re)evaluată la fiecare audit (de ex.: luând în considerare vârsta și creșterea în număr de sisteme, schimbările la expunere – inundații mai frecvente etc.).

Evaluarea expunerii naturale:

Principiile metodei permit să se evalueze expunerea naturală ca potențialitate intrinsecă a unui anumit număr de evenimente caracteristice.

Un tabel ajutător pentru această evaluare este oferit în Anexa 1 al „*Ghidului MEHARI de analiză a riscului*”.

Acest tabel este completat, prin lipsă, cu valori mici care sunt valabile pentru majoritatea organizațiilor. În acest mod, dacă tabelul nu este reevaluat, valorile folosite pentru expunerea naturală vor fi mai mult sau mai puțin în conformitate cu situația standard a majorității organizațiilor.

7.3.2 Introducerea ideii impactului intrinsec pentru scenariile de risc și calculele corespunzătoare

7.3.2.1 Noțiunea de impact intrinsec

Modelul de risc MEHARI a făcut întotdeauna referință implicit la impactul maximal, deoarece un indicator de reducere a impactului (STATUS-RI) este evaluat. Totuși, evaluarea impactului intrinsec nu fusese inclusă în analiza riscului.

Impactul intrinsec în MEHARI

Impactul intrinsec al unui scenariu de risc reprezintă o evaluare maximală a consecințelor unui risc, fără nici o măsură de securitate.

Evaluarea impactului intrinsec poate fi dedusă din o scară de valori a defecțiunilor (care ar putea conduce la clasificare), sau obținută direct. Acesta este un pas formal în analiza riscului.

7.3.2.2 Referință la impactul intrinsec în bazele de cunoștințe

Atunci când bazele de cunoștințe sunt folosite pentru o căutare sistematică a situațiilor de risc, MEHARI necesită completarea unui tabel al impactului intrinsec. Acest tabel include diferitele tipuri de bunuri asupra cărora scenariile de risc pot avea impact, și diferitele tipuri de impact asupra acestor bunuri, cu alte cuvinte, prin lipsă, disponibilitatea, integritatea și confidențialitatea.

Deoarece scenariile se referă la bunurile asupra cărora are loc impactul, și tipul de impact, evaluarea impactului intrinsec este automată.

Observați că este posibil să se includă și alte criterii decât disponibilitatea, integritatea și confidențialitatea prin completarea tabelului impactului intrinsec și generarea tabelor de evaluare corespunzătoare prin crearea scenariilor ad hoc.

7.3.2.3 Personalizarea tabelului impactului intrinsec pentru anumite tipuri de bunuri

Așa cum s-a explicat deja, unii utilizatori vor să diferențieze între scenarii ca o funcție a tipului specific de bunuri asupra căruia are loc impactul (de exemplu: datele unui anumit departament sau ale unui anumit domeniu funcțional).

Faptul că scenariile fac referință explicit la tipurile de bunuri permite această diferențiere. Tot ceea ce se cere este crearea variațiilor de bunuri în tabelul impactului intrinsec (fie că este pentru date, servere, rețele, sau alte bunuri), și să se completeze tabelul pentru fiecare criteriu relevant.

Cu MEHARI, acest lucru se numește descompunere cartografică.

Cititorul ar trebui totuși să știe că variațiile de bunuri create astfel ar fi folosite pentru a genera variații de scenariu. Acest lucru poate duce la un număr foarte mare de scenarii, și această posibilitate ar trebui folosită cu grijă.

7.3.3 Introducerea scenariilor neevolutive și calculele corespunzătoare

Modul în care au fost prezentate măsurile de protecție în unele din versiunile anterioare poate fi confuz.

Ele au fost definite ca având obiectivul, fără a preveni deteriorarea sistemului, de a limita scopul său. Deși acest lucru este corect, în practică acestea erau confundate cu măsurile de detectare a deteriorării, acolo unde o astfel de detectare ar putea provoca o reacție, ceea ce nu se întâmplă întotdeauna.

De fapt, dacă reacția posibilă nu reduce gravitatea consecințelor scenariului, nu are nici un rost să fie inclusă.

Cu alte cuvinte, măsurile de protecție ar trebui luate în considerare doar dacă acestea reduc eficient impactul intrinsec al scenariului, așa cum a fost evaluat inițial.

Pentru a simplifica includerea acestei nuanțe, a fost creată noțiunea de scenariu „neevolutiv”.

Scenariul neevolutiv:

Dacă un scenariu nu evoluează și este fix în timp și spațiu, nici o măsură de protecție nu îi poate limita consecințele directe.

Anumite scenarii, care nu sunt fixe în timp și spațiu, pot fi de așa natură încât măsurile de protecție potențiale nu au nici un efect asupra impactului intrinsec. Acestea trebuie deci considerate ca fiind neevolutive, și tratate ca atare.

În mod deosebit, există cazuri pentru care efectul real al măsurilor de protecție poate fi decis doar în contextul global al organizației:

- Atunci când datele sunt modificate (caz de fraudă), sau programele sunt modificate (rea voință sau erori), impactul intrinsec poate (sau nu) fi redus prin detectarea timpurie în funcție de faptul dacă există un drept al erorii sau nu.

- Atunci când informația este dezvăluită necorespunzător, prevenirea repetării prin detectarea din timp poate reduce impactul intrinsec în funcție de context și de subiectul informației.

Evident, aceste exemple ale caracterului evolutiv (sau nu) al scenariului nu depind doar de baza de cunoștințe. Ele ar trebui să depindă și de alegerea și deciziile care trebuie luate de către utilizatori.

De la versiunea precedentă a MEHARI, managementul scenariului de către procedurile automatizate permit declararea unui scenariu ca fiind neevolutiv, deși a fost considerat inițial ca fiind evolutiv.

7.3.4 Abordări propuse de MEHARI

7.3.4.1 Un spectru larg de abordări

Modelul de risc al lui MEHARI și bazele de cunoștințe au permis din totdeauna multe abordări, dar setul de documentație precedent a accentuat o abordare specifică care a condus la formalizarea planurilor strategice și operaționale pentru organizație.

Pe de altă parte natura modulară și complementară a uneltelor setului de metodologii este acum accentuată. Aceasta este o parte esențială a MEHARI.

Pentru cei care au aplicat deja MEHARI, și au pregătit planuri strategice sau operaționale formale, nu există nici o revoluție – doar evoluție.

Pentru aceia care au considerat că MEHARI este prea formal în planificarea strategică, ei vor găsi ghiduri care permit evitarea anumitor constrângeri, pe care structurile mai mici nu trebuie să le înfrunte.

Cei care vor să folosească MEHARI doar pentru proiecte vor găsi și ei sfaturi corespunzătoare.

7.3.4.2 Unicitatea abordării de analiză a riscului

În MEHARI, abordarea analizei riscului este unică și noțiunile de abordare globală și abordare analitică sunt legate.

Există o abordare fundamentală care include evaluarea (a impactului intrinsec, expunerii naturale și factorii de reducere a riscului), raționamentul și judecata finală asupra potențialității și a impactului riscului și, în final, acceptabilitatea riscului.

Procedurile automate oferă asistență în procesul de bază și sunt un ajutor esențial în căutarea sistematică a situațiilor de risc, dar nu pot fi considerate niciodată o înlocuire pentru judecata umană.

7.3.4.3. Natura complementară a uneltelor MEHARI și principiile de proiectare

Natura complementară a uneltelor asociate cu metoda impune principii de proiectare stricte, care trebuie explicate.

Din acest motiv, chiar și în versiunile anterioare ale MEHARI, principiile de proiectare au fost explicate.

Există două principii principale și un număr de principii complementare. Principiile principale sunt:

- Procedurile automate ale metodei nu trebuie să conducă niciodată la subestimarea unui risc. Este întotdeauna preferabil ca un risc să fie supra-estimat inițial, cu posibilitatea de a fi redus de o analiză detaliată ulterioară, decât să fie subestimat și să nu fie selectat pentru o examinare amănunțită.
- În orice caz, procedurile automate ale metodei trebuie să permită explicarea și justificarea pentru rezultatele obținute.

7.3.5 Bazele de cunoștințe

7.3.5.1 Domeniul de aplicație

Cu MEHARI, domeniul de aplicație al bazelor de cunoștințe acoperă sistemul informațional în cel mai larg sens.

Ca un rezultat specific, dimensiunile mediului de lucru al utilizatorului sunt luate în considerare (documente, poștă, spațiu al biroului, etc.).

7.3.5.2 Baza de cunoștințe a serviciilor de securitate

Principiile de bază pentru bazele de cunoștințe și chestionare au fost descrise deja. Aplicarea lor a condus la o revizuire a bazei de cunoștințe a serviciilor de securitate. În plus, a fost creat un dosar descriptiv („manualul de referințe al serviciilor de securitate”).

7.3.5.3 Baza de cunoștințe a scenariilor

Principiile care au fost aplicate în definirea acestei baze au fost descrise clar.

7.3.5.4 Tabelele de evaluare a factorilor reducerii riscului

În timp ce tabelele de evaluare pot fi modificate de către utilizatori, este preferabil ca crearea lor să fie fundamentată pe niște principii clare. Principiile folosite pentru a crea tabelele sunt documentate.