MEHARI 2010

Ghid de Evaluare pentru Serviciile de Securitate

Noiembrie 2010

Comisia Metodelor

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11, rue de Mogador, 75009 PARIS (France)

Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88 – e-mail : clusif@clusif.asso.fr

Web : http://www.clusif.asso.fr

MULTUMIRI

Clusif ar dori să mulTumească în special lui Jean-Philippe Jouas pentru contributia sa, lui Jean-Louis Roule pentru traducere cât si membrilor comisiei Metodelor care au participat la realizarea acestui document.

Traducerea în limba română a fost realizată de **Lazareanu Elena-Luiza**, **Hrincescu Raluca**, **Cînipariu Petronela, Florentina Mariutei** si **Grigoras Anca-Laura** studenti ai Facultătii de Economie si Administrarea Afacerilor din cadrul Universitătii Alexandru Ioan Cuza din Iasi.

Proiectul a fost coordonat de **dr. Valentin-Petru Măzăreanu**, cercetător postdoc si cadru didactic asociat în institutia mai sus mentionată.

Contact:
www.managementul-riscurilor.ro
www.feaa.uaic.ro
vali.mazareanu@feaa.uaic.ro

CUPRINS

1. Introducere

Documentul "*MEHARI: Concepte fundamentale si specificatii functionale*", care prezinta principiul fundamental al MEHARI 2010, expune cerintele pentru folosirea adecvata a cunostintelor de baza a serviciilor de securitate, inclusiv:

- Definitia serviciilor de securitate,
- Definitia criteriului pentru evaluarea nivelelor de calitate: parametri de avut in vedere si definitia nivelelor de calitate,
- Constituirea cunostintelor de baza, inclusiv a listei serviciilor de securitate si chestionarelor permitand evaluarea nivelului de calitate ale acestora
- Definitia unei metrologii pentru evaluarea calitatii serviciilor de securitate.

Incepem prin explicarea definitiilor de mai sus inainte de a examina evaluarea serviciilor de securitate in sine.

2. Definitii

2.1 .Servicii de securitate

Un serviciu de securitate este un raspunsul unei nevoi de securitate, exprimata in termeni generali si functionali, care descriu scopul serviciului, si care se refera de obicei la anumite tipuri de amenintari.

Un serviciu de securitate asigura o functie de securitate.

Aceasta functie este **independenta de mecanismele si solutiile actuale** utilizate pentru a oferi in mod eficient serviciul.

Exemplu: serviciul de "Control al accesului", al carui scop sau functie, dupa cum sugereaza si numele, este de a controla accesul; cu alte cuvinte, permite accesul doar persoanelor autorizate.

2.1.1 Servicii si sub-servicii de securitate

Functia unui servicu de securitate poate solicita mai multe componente, care pot fi considerate "sub-servicii". In exemplul de mai sus, controlul accesului necesita cunoasterea celui autorizat, ceea ce implica o functie de autorizare, recunoasterea unei persoane, care la randul ei implica o functie de autentificare si o filtrare a accesului, care apoi implica o a treia functie de filtrare.

Un serviciu de securitate poate fi alcatuit din mai multe servicii de securitate pentru a satisface o nevoie specifica sau un scop. Fiecare componenta este un sub-serviciu de securitate a serviciului in cauza, desi cu privire la o functie individuală, acesta își păstrează caracteristicile unui serviciu asa cum sunt definite mai sus.

2.1.2 Mecanisme de securitate si solutii

Un „**mecanism**" este un mijloc special prin care se asigura, total sau partial, o functie pentru un serviciu sau sub-serviciu. Acesta ar putea consta intr-o anumita procedura, algoritm, tehnologie, etc.

Pentru autentificarea utilizatorului sub-serviciului (de exemplu la un sistem de operare) mai sus mentionat, mecanisme posibile ar putea fi parole, simboluri, carduri inteligente, sisteme biometrice, etc.

Pentru un anumit sub-serviciu, cateva mecanisme sunt general posibile; a caror selectie au adesea o consecinta directa asupra calitatii pe care sub-serviciul o va dobandi.

O **solutie de securitate** este realizarea concreta a unui mecanism de securitatea si ar putea fi alcatuit din hardware, software, proceduri si operatiuni de sprijin, impreuna cu structurile organizatorice necesare cerute.

2.1.3 tipologia serviciilor de securitate

Unele servicii ar putea fi considerate drept „masuri generale" iar altele servicii tehnice:

- Masurile generale sunt cu siguranta utile, chiar mandatorii, pentru securitatea sistemelor informatice, desi beneficiul acestora este mai eficient la nivel de organizare, managementul securitatii sau constientizarii decat a situatiilor de risc insasi.
- Masurile tehnice au un rol clar, un scop direct si un efect direct asupra catorva situatii de risc ce ar putea fi specificate.

2.2 Criterii pentru evaluarea calitatii serviciilor de securitate

Serviciile de securitate pot varia la nivel de performante. Ele vor fi mai mult sau mai putin eficiente in functia lor, si mai mult sau mai putin puternice in capacitatea lor de a rezista atacurilor directe, depinzand de mecanismele utilizate si de aspectele organizationale.

2.2.1 Parametri obligatorii

Pentru a masura performanta serviciului de securitate, trebuie luati in considerare mai multi parametri:

- Eficienta,
- Vigurozitatea,
- Performanta.

Eficienta serviciilor de securitate

Pentru serviciile de natura tehnica, eficienta este o măsură a capacitătii lor de a asigura eficient functia necesară atunci când se confruntă cu un personal mai mult sau mai putin competent sau cu circumstante mai mult sau mai putin obisnuite.

Sa luam , de exemplu, sub-serviciul „Managementul accesului autorizat la sistemul informatic", care implica atribuirea drepturilor de acces ale utilizatorilor. Functia acestui serviciu este de a asigura ca doar acele persoane care au autorizatia conducerii primesc de fapt informatia corespunzatoare accesului in sistem. În practică, eficienta serviciului depinde de strictetea controalelor, de autenticitatea cererii, si de corelarea relatiei ierarhice dintre petitionar si noul utilizator. Dacă tot ce se cere este o simplă trimitere postală, fără semnătură sau certificat, oricine cunoaste câte ceva despre procesul de autorizare ar putea să îsi aloce singuri fără permisiune drepturi de acces, si calitatea sub-serviciului ar fi considerată ca fiind slabă.

Eficienta unui serviciu care administrează actiunile umane reprezintă astfel măsura competentei necesare pentru a permite unor persoane să treacă de controalele în vigoare, sau chiar să abuzeze de ele.

Pentru acele servicii care tratează evenimentele naturale (*precum detectarea incendiilor, stingerea incendiilor*), eficienta reprezintă o măsură a "puterii" evenimentului pentru care interventia lor rămâne eficientă.

Dacă acest lucru priveste, de exemplu, un baraj care trebuie să împiedice un râu să se reverse din cauza ploilor abundente, eficienta este direct legată de debitul apei (puterea inundatiei) căreia i se opune. **În practică, puterea va fi deseori măsurată ca o functie a caracterului exceptional al evenimentului.**

Serviciile care oferă acoperire generală nu pot, în principiu, să fie evaluate pe baza efectului lor direct, ci doar pe baza rolului lor indirect.

Eficienta măsurilor generale reprezintă rezultatul capacitătii lor de a crea planuri de actiune sau schimbări de comportament semnificative.

Cât de robust este un serviciu de securitate?

Robustetea unui serviciu de securitate măsoară capacitatea sa de a rezista unei actiuni care este menită să scurt-circuiteze serviciul sau să-i restrictioneze eficienta.

Robustetea priveste doar acele servicii care sunt considerate tehnice.

În exemplul precedent (managementul accesului), robustetea sub-serviciului depinde, în mod deosebit, de cât de usor este să se acceseze direct tabelul cu drepturile de acces ale utilizatorilor, si astfel să se permită cuiva să îsi atribuie drepturi de acces fără necesitatea de a urma procesele de control obisnuite.

Atunci când avem de-a face cu servicii pentru managementul accidentelor sau al evenimentelor naturale (precum detectarea incendiilor, stingerea automată a incendiilor, si asa mai departe), robustetea lor va acoperi si capacitatea de a evita să fie scurt-circuitate sau evitate (fie accidental, sau intentionat).

Permanenta

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

Pentru aceasta, orice întrerupere a serviciului trebuie detectată si trebuie aplicate măsuri paliative. De aceea totul depinde de viteza detectării si de capacitatea de a reactiona.

Pentru măsurile generale, supravegherea solutiilor este importantă pentru a arăta că acestea pot fi măsurate cu adevărat, în ceea ce priveste implementarea si eficacitatea, dar si că există indicatori ai calitătii efective a serviciului si puncte de control implementate.

Definitia calitătii nivelelor serviciului de securitate

Calitatea unui serviciu de securitatea măsoară eficienta sa, cât de robust este, si existenta controalelor obisnuite. Global, calitatea unui serviciu de securitate reprezintă capacitatea sa de a rezista oricărui atac asupra măsurilor sale de apărare - desi nici un castel nu poate fi considerat protejat in totalitate.

Calitatea serviciului de securitate este notată pe o scară de la 0 la 4. Această scară reflectă competenta sau hotărârea care este necesară pentru a trece de apărare, pentru a o scurt-circuita, sau pentru a împiedica sau face inutilă detectarea neutralizării serviciului.

Desi această scară de valori permite valori fractionale, credem că este util să se ofere niste indicatii privind valorile întregi pentru un serviciu de securitate.

Calitatea serviciului evaluat de nivelul 1

Acest serviciu are un nivel minim. Ar putea fi total ineficient (sau nu rezistă) când se confruntă cu un utilizator obisnuit, fără calificări deosebite, sau putin educat . În evenimentele naturale, este probabil să nu fie de nici un folos în problemele de zi cu zi. În general, va avea un efect mic sau deloc asupra comportamentului sau eficientei organizatiei.

Calitatea serviciului evaluat de nivelul 2

Serviciul este de obicei eficient si rezistă unui hacker mediu sau putin competent. Totusi, el este cu sigurantă insuficient atunci când se confruntă cu un profesionist cu experientă în acel domeniu (acesta ar putea fi un profesionist IT, un hot bine echipat, sau un expert în spargeri fizice). În ceea ce priveste fenomenele naturale, este rareori suficient pentru a acoperi evenimente grave - desi acestea sunt rare. În general, astfel de servicii ar îmbunătăti doar situatiile de zi ci zi.

Calitatea serviciului evaluat de nivelul 3

Serviciul este mai eficient si rezistă la atacurile si evenimentele descrise mai sus, dar ar putea fi insuficient împotriva atacurilor specializate (hackeri bine echipati si cu experientă, ingineri de sistem specializati, mai ales dacă acestia au unelte sau expertiză aplicată pe domeniu, spioni profesionisti, si asa mai departe), sau a dezastrelor naturale cu adevărat exceptionale. O solutie generalizată ar avea un oarecare efect asupra unui număr mare de circumstante. Totusi, ea nu ar oferi cu sigurantă nici o garantie pentru probleme sau atacuri foarte grave.

Calitatea serviciului evaluat de nivelul 4

Acesta este cel mai ridicat nivel si serviciul de securitate va rămâne activ si eficient în fata tuturor agresiunilor descrise mai sus. Ar putea totusi fi spart în circumstante exceptionale: cei mai buni spărgători de coduri din lume cu cele mai bune unelte de spart coduri (ceea ce este posibil dacă unele tări vor ca acest lucru să se întâmple) sau o combinatie exceptională de circumstante exceptionale.

Procesul de evaluare a calitătii serviciului de securitate folosit de MEHARI a fost construit pentru a oferi evaluări de calitate corespunzătoare pentru definitiile de mai sus.

2.3. Baza de cunostinte MEHARI a serviciilor de securitate

Mehari cuprinde o baza de cunostinte a serviciilor de securitate format din chestionare, organizata pe domenii de responsabilitate, pentru revizuirea vulnerabilitatii.

Aceasta organizarea permite limitarea intrebarilor puse fiecarui interlocutor intalnit in timpul fazei de reexaminare.

Domeniile Mehari 2010 de responsabilitate acopera:

- Organizarea
- Securitatea site-ului
- Securitatea spatiilor
- Arhitectura si continuitatea serviciului retelelor extinse de inter-site-uri
- Arhitectura si continuitatea serviciului retelelor locale

- Activitatea retelei
- Sisteme de arhitectura si securitatea logica
- Activitatea sistemelor IT
- Aplicabilitatea securitatii
- Proiecte IT si dezvoltarea securitatii
- Gestionarea statiilor de lucru ale utilizatorilor
- Aplicabilitatea telecomunicatiilor
- Procese de management
- Informatii despre managementul securitatii

2.4. Evaluarea calitatii serviciilor de securitate

Evaluarea calitatii sistemului cuprinde un set de intrebari pentru care un raspuns cu da/nu este necesar, cu un sistem de asociere a scorului si evaluarii pe care il vom examina mai tarziu in acest document.

Mai jos este un exemplu, extras din chestionar, ce arata intrebari privitoare la domeniul “arhitecturii sistemului”.

Chestionar de audit : Controlul accesului la sisteme si aplicatii Managementul autorizatiilor si privilegiilor de acces (oferire, delegare, revocare)	
Intr. nr.	Intrebarea
07A02-01	Necesită procedura de acordare a autorizării accesului aprobarea oficială a managementului de linie (la un nivel suficient de înalt)?
07A02-02	Autorizatiile sunt acordate către indivizii numiti doar ca o functie a profilului lor?
07A02-03	Este procedura de acordare (sau schimbare sau revocare) a autorizatiei către o persoană (fie direct sau prin profilul său) strict controlată?
07A02-04	Există un proces sistematic de actualizare a tabelului de autorizatii la momentul plecării personalului sau la finalul contractului pentru personalul extern sau la schimbarea functiei?
07A02-05	Există un proces strict controlat (precum cel de sus) care permite delegarea autorizatiei proprie, în parte sau în întregime, unei persoane la alegere pentru o perioadă de timp determinată (în cazul absentei)?
07A02-06	Este posibil să se controleze în orice moment, pentru toti utilizatorii, drepturile, autorizatiile si privilegiile în vigoare?
07A02-07	Există un audit regulat, cel putin o dată pe an, al profilurilor si autorizatiilor acordate tuturor utilizatorilor si al procedurilor pentru managementul profilurilor atribuite?

Chestionarele cuprind întrebări de diferite feluri. Acestea ar putea fi întrebări orientate către eficacitatea măsurilor de securitate (ex.: frecventă back-up-ului, tipul controlului accesului fizic: cititor de carduri, digicod, etc., existenta detectoarelor de incendiu, etc.), întrebări orientate către robustetea măsurilor de securitate (ex.: acolo unde sunt depozitate rezervele, si cum este protejat accesul, dacă există o usă dublă, si cât de bine sunt construite usile, cum este protejat sistemul de detectare a incendiilor, etc.). În general, sunt si una sau două întrebări despre monitorizarea, controlul si auditul functiilor asteptate de la serviciu.

Sistemul de evaluare

Întrebările privind un serviciu de securitate depind de măsurile de securitate utile sau necesare ale acelui serviciu. Totusi, nu toate măsurile au acelasi rol de jucat, si trebuie făcută o distinctie între măsuri contributive, măsuri majore sau suficiente, si măsuri esentiale.

2.4.1 Masuri contibutive

Anumite întrebări au legătură cu măsuri care au un anumit rol în contributia la calitatea serviciului, fără ca implementarea lor totală să fie neapărat necesară.

În termeni cantitativi, o evaluare clasică aplicată la aceste măsuri reflectă ideea de contributie. În acest caz, anumite măsuri - mai importante decât altele - ar avea o valoare diferită. Baza de cunostinte MEHARI arată evaluarea aplicată fiecărei întrebări.

Tabelul de mai jos dezvolta extrasul de mai devreme. În el, coloana V1[1] este rezervată pentru răspunsurile la întrebări (1 pentru da, 0 pentru nu): coloana următoare arată valoarea aplicată răspunsurilor.

Chestionar de audit: Controlul accesului la sisteme si aplicatii Managementul autorizatiilor si privilegiilor de acces (oferire, delegare, revocare)			
Intr. nr.	Intrebarea	V1	W
07A02-01	Necesită procedura de acordare a autorizării accesului aprobarea oficială a managementului de linie (la un nivel suficient de înalt)?	0	4
07A02-02	Autorizatiile sunt acordate către indivizii numiti doar ca o functie a profilului lor?	1	2
07A02-03	Este procedura de acordare (sau schimbare sau revocare) a autorizatiei către o persoană (fie direct sau prin profilul său) strict controlată?	1	4
07A02-04	Există un proces sistematic de actualizare a tabelului de autorizatii la momentul plecării personalului sau la finalul contractului pentru personalul extern sau la schimbarea functiei?	0	2
07A02-05	Există un proces strict controlat (precum cel de sus) care permite delegarea autorizatiei proprie, în parte sau în întregime, unei persoane la alegere pentru o perioadă de timp determinată (în cazul absentei)?	0	4
07A02-06	Este posibil să se controleze în orice moment, pentru toti utilizatorii, drepturile, autorizatiile si privilegiile în vigoare?	1	1
07A02-07	Există un audit regulat, cel putin o dată pe an, al profilurilor si autorizatiilor acordate tuturor utilizatorilor si al procedurilor pentru managementul profilurilor atribuite?	0	1

Valorarea medie evaluată este pur si simplu suma măsurilor active evaluate (cele ale căror răspuns este ”1” pentru “da”), plus suma valorii posibile, rezultatul fiind normalizat pe o scară de la 0 la 4.

Deci, dacă V□□ contine răspunsul la întrebarea i, Wi este valoarea lui i si Mw valoarea medie:

Mw = 4 * ∑R; W; / ∑W;

Deci, pentru răspunsurile arătate în chestionarul de exemplu de mai sus, valoarea medie este:

Mw = 4*7/18= 1,6

Iar calitatea serviciului, Q = Mw = 1,6

2.4.2 Măsuri majore sau “suficiente”

Unele măsuri ar putea fi considerate suficiente pentru a asigura un anumit nivel de calitate al serviciului. De exemplu, un sistem de detectarea a incendiilor poate fi considerat suficient în oferirea nivelului 2 pentru sub-serviciul corespondent.

De aceea am adăugat un prag minim, care reprezintă nota minimă pentru calitatea serviciului dacă măsura este activă.

---

1 □ La acest nivel este luat in calcul o singura varianta pentru acest domeniu, exprimat prin valoarea 1 in capul de coloana V1

Coloana “Min” arată că dacă este dat un răspuns pozitiv la o întrebare pentru care a fost fixat un prag minim, atunci acel prag a fost atins sau întrecut de către sub-serviciu.

Mai jos este prezentată o altă privire asupra tabelului de mai devreme, de această dată cu coloana pentru “min” adăugată.

Chestionar de audit: Domeniu: Securitatea arhitecturii sistemelor (07) **A - Controlul accesului la sisteme si aplicatii**				
A02: Managementul autorizatilor de acces si privilegiile (de acordare, delegare, revocare)		**1**		
Nr. Întrebare	**Întrebare**	**V1**	**W**	**Min**
07A02-01	Procedura de acordare a autorizatiei de acces necesită aprobarea oficială a managementului de linie (la un nivel suficient de înalt)?	0	4	
07A02-02	Sunt autorizatiile acordate persoanelor fizice numite doar o functie a profilul lor?	1	2	
07A02-03	Este procedura de acordare (sau schimbare sau revocare) a autorizatiei unei persoane (fie direct sau prin profilul său) strict controlată?	1	4	3
07A02-04	Există un proces sistematic de actualizare a tabelului de autorizatii în momentul de plecare a personalului sau la sfârsitul contractului pentru personalul extern sau schimbarea functiei?	0	2	
07A02-05	Există un proces strict controlat (ca mai sus), care permite delegarea autorizatiilor lui / ei , în parte sau în totalitate, la o persoană de alegere pentru o perioadă determinată (în cazul absentei)?	0	4	
07A02-06	Este posibil să se controleze în orice moment, pentru toti utilizatorii, drepturile, autorizatiile si privilegiile în vigoare?	1	1	
07A02-07	Există un audit periodic, cel putin o dată pe an, al profilurilor si autorizatiilor acordate tuturor utilizatorilor si a procedurilor de gestionare a profilurilor atribuite?	0	1	

În exemplu, faptul că procesul de alocare, modificarea sau eliminarea drepturilor (întrebarea - 03) gestionat strict a fost considerat suficient pentru cresterea calitatatii serviciilor scorul la pragul minim de 3.

2.4.3 Măsuri esentiale

Pe de altă parte, anumite măsuri pot fi considerate obligatorii în asigurarea unui anumit nivel de calitate a serviciului.

MEHARI asociază cu întrebările privind acele măsuri considerate obligatorii în asigurarea unui anumit nivel de calitate, un prag de calitate. În cazul în care acest prag este depăsit, punerea în aplicare a măsurii este obligatorie.

Cu alte cuvinte, pragul se arată în coloana "Max" este nivelul de calitate maximă pe care un sub-serviciu il poate obtine în cazul în care măsura nu este pusă în aplicare. Atunci când există conflict între pragurile minime si maxime, valoarea maximă are prioritate.

Cu acest plus fată de tabelul anterior aducem in vedere următoarele:

	Chestionar de audit: Domeniu: Securitatea arhitecturii sistemelor (07) A - Controlul accesului la sisteme si aplicatii				
A02: Managementul autorizatilor de acces si privilegiile (de acordare, delegare, revocare)		**1**			
Nr. Întrebare	**Întrebare**	**V1**	**W**	**Max**	**Min**
07A02-01	Procedura de acordare a autorizatiei de acces necesită aprobarea oficială a managementului de linie (la un nivel suficient de înalt)?	0	4	2	
07A02-02	Sunt autorizatiile acordate persoanelor fizice numite doar o functie a profilul lor?	1	2		
07A02-03	Este procedura de acordare (sau schimbare sau revocare) a autorizatiei unei persoane (fie direct sau prin profilul său) strict controlată?	1	4	2	3
07A02-04	Există un proces sistematic de actualizare a tabelului de autorizatii în momentul de plecare a personalului sau la sfârsitul contractului pentru personalul extern sau schimbarea functiei?	0	2		
07A02-05	Există un proces strict controlat (ca mai sus), care permite delegarea autorizatiilor lui / ei , în parte sau în totalitate, la o persoană de alegere pentru o perioadă determinată (în cazul absentei)?	0	4		
07A02-06	Este posibil să se controleze în orice moment, pentru toti utilizatorii, drepturile, autorizatiile si privilegiile în vigoare?	1	1		
07A02-07	Există un audit periodic, cel putin o dată pe an, al profilurilor si autorizatiilor acordate tuturor utilizatorilor si a procedurilor de gestionare a profilurilor atribuite?	0	1	2	

În exemplul de mai sus, opinia expertilor spune că răspunsurile negative la întrebările 1 si 7 înseamnă că nivelul de calitate a serviciilor nu poate fi mai mare de 2. Această limită are prioritate peste nivelul 3 valoarea propusa mai devreme.

Acest sistem triplu de calitate a serviciului de măsurare evită riscul de a vedea o serie de măsuri ineficiente de a primi o supra-evaluare a nivelului calitatii măsurile esentiale nu sunt active sau, dimpotrivă, o serie de măsuri slab ponderate sub-evaluarea calitatii serviciilor atunci când o măsură esentială este pusă în aplicare. Această abordare este una dintre caracteristicile distinctive MEHARI, oferind o reală valoare bazata pe expertiza oamenilor care întretin bazele de cunostinte.

2.4.4 Întrebări inaplicabile

Anumite întrebări pot fi considerate inaplicabile pentru anumite organizatii. În acest caz, introducand un "X" în coloana răspunsului intrabarile nu sunt luate în considerare în procesul de evaluare.

Atentie deosebită trebuie acordată pentru a se asigura că o întrebare inaplicabilă rămâne asa, indiferent de evolutia planificată a sistemului IT si serviciile de securitate.

3. Procesul de evaluare

Înainte de a descrie procesul efectiv de evaluare, trebuie adresată o întrebare preliminară privind serviciile care necesită actiune. Pot exista mai multe variante ale aceluiasi serviciu si acestea ar putea avea nevoie să fie retinute.

3.1 Schema de audit

Serviciile de securitate, asa cum sunt definite de MEHARI, sunt functii de securitate care sunt furnizate de solutii implementate în întreprindere sau organizatie.

Controlul vulnerabilitătii implică, în practică, analiza si auditul solutiilor si procedurilor implementate pentru a asigura functiile de securitate.

Cu toate acestea, există în general o serie de solutii care să asigure un anumit tip de protectie.

De exemplu, controlul accesului fizic în sedii este în mod sigur oferit de diferite mecanisme si solutii - si acestea vor fi diferite pentru accesul în sălile de calculatoare,sau alte centre tehnice, precum instalatiile PABX, săli de conferinTe si instalatii electrice majore.

Este de asemenea evident că controlul accesului logic la diferite sisteme (mainframe-uri, UNIX, NT, etc) vor fi gestionate în diferite moduri în functie de tipul si nivelul de sensibilitate al sistemului.

Înainte chiar de a gândi la un proces de analiză si evaluare a serviciilor de securitate, CISO si auditorul de securitate ar trebui sa identifice întâi ce solutii specifice ar trebui să fie analizate si verificate.

În MEHARI acest lucru este numit ”plan de audit” sau ”schemă de audit”.

3.1.1 Scopul unei scheme de audit

Într-o lume ideală, fiecare serviciu de securitate în parte ar trebui să fie examinat, si toate solutiile care furnizează aceste sevicii în organizatie ar trebui sa fie identificate, asa încât acestea să poată fi verificate individual.

Acest lucru ar conduce la un volum de muncă incredibil de grea pentru un rezultat al cărui nivel de detaliu ar fi în mare măsura de prisos. Este recomandată, asadar, o simplificare prin gruparea de servicii similare astfel încât acestea să poată fi analizate ca seturi omogene.

Cu toate acestea, nu este în general posibil să se considere ca fiind echivalente toate solutiile implementate în cadrul întreprinderii. Ar fi acelasi lucru ca si cum s-ar considera că toate clădirile si încăperile sunt protejate în acelassi mod, că toate partile infrastructurii IT au aceleasi planuri de back-up, sau ca toate datele sunt stocate si păstrate în acelasi mod. Evident, nu este cazul.

Este, desigur, posibil întotdeauna să se grupeze diferite obiecte într-un singur set, care apoi ar fi considerat ca un întreg omogen. Dar ar trebui specificat faptul că un control precaut al vulnerabilitătii ar putea pune în aplicare cea mai pesimistă evaluare pentru toate obiectele dintr-un set dat. Acest lucru ar oferi o perceptie generală foarte săracă a întregului set.

Trebuie, prin urmare, să găsim o cale de mijloc. Aceasta ne-ar permite sa diferentiem diferite solutii ale domeniilor care ar trebui controlate separat, si în interiorul cărora solutiile de securitate pot fi considerate omogene. Definitia acestor domenii este reprezentată de ”schema de audit”.

3.1.2 Construirea unei scheme de audit

Abordarea MEHARI ia în considerare faptul că serviciile de securitate sunt definite si implementate de echipe de dimensiune limitată, cu o politică de securitate (fie documentată în mod explicit sau nu) care îi va determina să ia decizii omogene si consecvente, chiar si atunci când constrângerile tehnice necesită solutii care diferă în detaliu.

Pe această bază principiile MEHARI sunt de a:

- Face distinctie între domeniile de responsabilitate unde o persoană poate fi definită în mod clar ca având responsabilitate pentru un domeniu care are o politică de securitate coerentă.
- Analiza, în cadrul acestor domenii, dacă există diferite persoane care sa aibă diferite politici de securitate, si astfel, sa definească sub-domenii de responsabilitate separate. De exemplu, administratorii de site pot avea, pentru securitatea site-ului lor, politici care sunt diferite de cele ale unui alt site.
- Analiza, în cadrul fiecărui domeniu sau sub-domeniu, sub-seturile care ar putea avea politici diferite din oricare motiv (tehnic sau de altă natură).

3.1.3 Domeniile de responsabilitate ale MEHARI

Finalitatea schemei de audit este de a defini controale specifice pentru fiecare domeniu. Chestionarele de audit MEHARI sunt ele însele grupate. Acestea sunt organizate în acest mod pentru a optimiza procesul de audit.

Primul nivel structural al schemei de audit va reflecta, asadar, această descompunere. Apoi auditorul va trebui să decidă, pentru fiecare domeniu de acoperit, cât de multe variatii ar trebui definite:

- Câte organizatii diferite ar trebui verificate separat pentru functiile de securitate care depinde de organizatie?

- Câti administratori de site pot avea o politică de securitate specifică, necesitând recenzii separate ale vulnerabilitătii?
- Câti manageri locali ai sediilor pot avea o politică de securitate specifică, necesitând recenzii separate ale vulnerabilitătii?
- Există un număr de manageri ai zonelor de retele locale care ar trebui intervievati separat?

si asa mai departe

De fiecare dată când este nevoie să se facă distinctie între entităti sau responsabilităti (din motive de autonomie, sau imposibilitatea de a pune în aplicare politici coerente), ar trebui create sub-domenii, si chestionarele reproduse pentru fiecare din ele.

Observatie: în sens invers, în entitătile mici, una si aceeasi persoană poate gestiona diferite doemnii de responsabilitate sau servicii de securitate. Este rational apoi pentru auditor să le grupeze în ideea de a simplifica auditul.

3.1.4 tipuri de subseturi care ar trebui personalizate pentru controalele de securitate

Cel de-al doilea nivel al descompunerii schemei de audit are de-a face cu strategii tehnice, sau alte motive care necesită diferentieri, îm cadrul fiecărui domeniu, între subansambluri care ar putea cere politici de securitate specifice. tipul de întrebari care ar trebui puse la acest nivel sunt:

- Câte tipuri diferite de organizatii necesită să fie verificate separat pentru functiile de securitate care depind de organizatie?
- Câte tipuri diferite de site-uri au o politică de securitate specifică, necesitând recenzii ale vulnerabilităti specifice (uzine chimice, site-uri cu acorduri de apărare specifice, care se ocupă cu detaliile personale, sociale, fiscale si asa mai departe)?
- Câte tipuri de sedii ar trebui să fie diferentiate în planul de securitate (birouri, săli de calculatoare, centre tehnice, si asa mai departe)?
- Câte inter-site-uri extinse si retele externe (intranet, de exemplu)?
- Câte tipuri de retele locale?

Etc

Pentru fiecare domeniu, va trebui să se identifice câte variatii diferite au nevoie să fie identificate si verificate în mod individual.

3.1.5 Crearea unei scheme de audit detaliată

Schema de audit este rezultatul acestor doua componente structurale: domeniile de responsabilitate pe de o parte, si variatiile personalizate pe de altă parte.

O schema de audit corporativă la nivel mondial care este rezultatul acestei abordări ar putea să dea în mod tipic un tabel de tipul celui de mai jos:

Domeniu	**Sub-domenii (exemple)**	**tipuri de subdomenii**
Organizatie	Nici unul (nicio descompunere)	Întreaga întreprindere
Site-uri	HQ si agentii de vânzări Site-uri de productie (gestionate de către departamentul de productie industrială)	HQ Agentii de vânzări Site-uri de productie
Sedii	Birouri si alte sedii conduse de departamentul de lucrări centrale Zone IT, tehnice si de telecomunicatii	Zone conduse de terte părti (ex: conexiunea de energie electrică) Săli de calculatoare Alte zone tehnice
Arhitectura retelelor extinse	Nici unul (nicio descompunere)	Retea inter-site extinsă
Arhitectura retelelor locale	Retelele IT Retelele procesului de productie (gestionate de către departamentul de	Retelele IT Retelele procesului de productie

	productie industrială)	
Retea de exploatare	Retele IT Retelele procesului de productie (gestionate de către departamentul de productie industrială)	Retelele IT Retelele procesului de productie
Sisteme	Sisteme IT Sieteme ale procesului de productie (gestionate de către departamentul de productie industrială)	Mainframe(-uri) Sisteme deschise (Unix & NT) Sisteme de management al procesurilor Sisteme de management al securitătii proceselor
Operarea sistemelor IT	Sisteme IT Sieteme ale procesului de productie (gestionate de către departamentul de productie industrială)	Mainframe(-uri) Sisteme deschise (Unix & NT) Sisteme de management al procesurilor
Securitatea aplicatiilor	Nici unul (nicio desompunere)	Aplicatii mainframe Aplicatii open system
Dezvoltare IT	Dezvoltare condusă de departamentul IT Dezvoltare specifică realizată de utilizatori	Dezvoltare condusă de departamentul IT Dezvoltare specifică realizată de utilizatori
Managementul statiilor de lucru ale utilizatorilor	Aplicatii pentru birou Aplicatii specifice	HQ Puncte de vânzare Site-uri de productie
Managementul telecomunicatiilor	Nici unul (nicio descompunere)	
Procese de management	Nici unul (nicio descompunere)	
Managementul Securitătii Informatiei (ISM)	Nici unul (nicio descompunere)	

O astfel de schemă de audit permite definirea unei organizări detaliate pentru verificarea vulnerabilitătii si să identifice necesitatea unei verificări specifice a vulnerabilitătii pentru fiecare din elementele enumerate în coloana din dreapta. Auditorul de securitate poate, prin urmare, sa aplice chestionarele (dacă sunt folosite chestionare) în atâtea copii câte linii sunt în domeniul sorespunzător.

3.1.6 Construirea unor scheme de audit specifice

Este, desigur, posibil să se construiască scheme de audit specifice care să corespundă nevoilor specifice si care nu acoperă toate domeniile.

Este posibil, de exemplu, să se construiască o schemă de audit specifică unui departament sau proiect (din mediul de lucru al utilizatorului prin intermediul sistemului si aplicatiilor utilizate). Acest lucru s-ar realiza prin selectarea domeniilor în cauză si care leagă subseturile corespunzătoare cu zonele în cauză.

Ar trebui specificat, oricum, că dacă procesul de diagnosticare trebuie urmat de o analiză a riscului, componentele neverificate ar putea cauza probleme în timpul analizei riscului.

3.2 Procesul de audit

3.2.1 Procesul de revizuire în sine

Din cauza faptului că chestionarele de audit ale serviciilor de securitate sunt organizate după domenii de responsabilitate, odată ce schema de audit este definită, acestea pot fi duplicate pentru a acoperi orice variatii ale domeniului de analizat. La întrebări ar trebui să răspundă persoanele potrivite sau cei mai calificati oameni în acel domeniu. Aceeasi abordare generală poate fi utilizată pentru evaluarea directă a calitătii serviciilor de securitate.

Poate fi faptul că, în timpul auditului, anumite sub-servicii nu par a fi aplicabile pentru organizatia respectivă. Chestionarele corespondente pot fi apoi sterse.

Raspunzând doar cu da sau nu la chestionare se pot crea uneori dificultăti.

Răspunsurile pot fi:

-"In general, DA, dar există exceptii"
- "În teorie, DA, dar în practică, nu sunt sigur că poate fi aplicat universal"
- "DA, partial (X%)"
- "DA, este în curs de desfăsurare chiar acum"
- "Da, este planificat, dar nu este încă aplicat"
-Etc.

Sfatul nostru în asemenea situatii este:

-Notati întotdeauna orice explicatii care însotesc răspunsurile, si păstrati-le. Pe foile cu chestionarele care sunt folosite în timpul reuniunilor de audit, ar trebui sa adăugati o coloană numită "Comentarii" pentru astfel de explicatii.

-Deoarece sistemul de notare necesită un răspuns de tipul "da" sau "nu" , auditorul de securitate va trebui să ia o decizie. Calea „sigură” ar fi să răspundă "nu" la toate întrebările care ridică îndoieli (cum ar fi răspunsurile de mai sus). Oricare ar fi alegerea, este important ca răspunsurile să nu influenteze în mod necorespunzător deciziile care rezultă în urma auditului. În special, ele nu ar trebui să ascundă imperfectiunile.

- Ar trebui să se aibă în vedere, totusi, că a introduce un răspuns "nu" pentru acele zone care sunt în mod evident corectate si sub control, mai ales dacă acestea sunt minore, ar putea duce la demotivarea personalului si ar afecta credibilitatea auditului.

- O abordare rezonabilă pare a fi răspuns "da" de fiecare dată când procesul de corectie si de reactie la lipsa de măsuri de implementare este sub control, si "nu" în caz contrar. Retineti că, pentru ca aceste răspunsuri să fie admisibile, auditul trebuie să aibă loc printr-o întâlnire fată-în-fată între auditor si persoana responsabilă pentru domeniul auditat, iar chestionarele trebuie completate în timpul sedintei. Chestionarelor completate de către persoana auditată fără prezenta auditorului pot masca total realitatea si introduce erori grave în audit si a calitătii sale generale.

3.2.2 Notarea si corectarea acesteia

O dată ce punctajele obtinute prin chestionare sunt finalizate, ar trebui să se obtină un punctaj si pentru serviciul de securitate. Acest lucru se va face folosind sistemul de ponderare MEHARI, după cum s-a explicat mai devreme.

Acest sistem de ponderare a fost proiectat si definitivat de către experti CLUSIF.

Cu toate acestea, este posibil ca anumite imperfectiuni să apară la nivel local. Sistemul nu poate, efectiv, să ia în considerare fiecare caz local sau specific ce ar putea fi întâlnit în timpul unui audit, nici nu poate fi adaptat la specificul la fiecărei organizatii. Auditorul trebuie, prin urmare, înainte de a trage concluziile sale si de a prezenta concluziile auditului, să verifice dacă sistemul de notare utilizat pentru fiecare serviciu si sub-serviciu este cel potrivit, făcând trimitere la informatiile definitorii obtinute în nivelele de calitate.
Este, prin urmare, obligatoriu ca auditorul ar trebui să fie un profesionist cu experientă în sistemul de securitate.

4. Evaluări personalizabile

Chestionarele MEHARI au fost concepute pentru a fi cât mai „experte” posibil si pentru a fi utilizate pentru procese de managementul riscului individuale.

Acest lucru conduce la o abordare „precaută” în care calitatea serviciilor de securitate poate fi oarecum subestimată pentru a preveni subestimarea un risc ce ar putea fi critic.

În timp ce această atitudine este precaută îndeajuns, poate fi deprimant cazul în care nu este utilizată pentru gestionarea riscurilor, ci pentru formarea unei opinii cu privire la nivelul de securitate.

În plus, pentru entitătile care sunt în etapele de început la capitolul securitate, chestionarea ca un întreg poate fi disproportionată luând în considerare stadiul de securitate deja atins.

Din acest motiv, chestionarele pot fi limitate la mai multe sau mai putine întrebări cheie.

În acest scop, fiecărei întrebări din chestionarele MEHARI i se atribuie un coeficient care reflectă atât tipul de întrebare cât si nivelul dobândit de securitate alocat întrebării.

Prima parte a coeficientului este o literă: E, R sau C:

- E indică o întrebare legată de eficacitatea serviciului,
- R indică o întrebare legată de robustetea de serviciu,
- C indică o întrebare legată de plasarea acesteia sub control (permanenta).

A doua parte a coeficientului este un număr referitor la nivelul de maturitate al entitătii pe baza cărora întrebarea este pertinentă: 1, 2 sau 3 (3 este folosit doar pentru întrebări legate de eficacitatea serviciului):

- 1 indică o întrebare de bază la care trebuie să se răspundă, indiferent de gradul de maturitate al entitătii,
- 2 indică nivelul mediu de maturitate (o companie sau organizatie cu un nivel avansat al securitătii, dar care încă trebuie să facă progrese),
- 3 indică întrebări care se aplică numai la entitäti mature în totalitate.

Acest lucru face posibil să se excludă din chestionare orice întrebări legate de control sau întrebări care sunt de un nivel prea ridicat pentru o analiză sumară.

5. Rezultatele

Rezultatele brute sunt fie chestionarele completate, cu comentariile care le însotesc, asa cum a fost descris mai devreme, fie evaluarea directă a calitătii serviciului de securitate.

În general, rezultatele sunt prezentate printr-o serie de elemente grafice sintetice.

5.1 Graficul sintetic al serviciul de securitate

Recenzia finală a vulnerabilitătii este de obicei reprezentată grafic sub forma unei "diagrame păianjen", cu un anumit număr de dimensiuni:

- Prin serviciul de securitate (arătând diferitele sub-servicii si punctajul lor),
- Prin domeniu de responsabilitate (arătând diferitele servicii care alcătuiesc domeniul si punctajul lor, obtinut prin intermediul mediei de notare a componentei sub-servicii)
- La nivel global (arătând diferite domenii si punctajul lor).

5.2 Graficul „tematic" sintetic

Anumite servicii de securitate, desi apar în diferite domenii de audit, sunt complementare în atingerea unui obiectiv de securitate global. Prin urmare, pentru a avea o idee generală a calitătii planurilor anterioare, va trebui să se combine rezultatele planurilor de securitate ale retelei si IT, planurilor de continuitate, planurilor de securitate electrică, si asa mai departe.

CLUSIF a definit 16 "teme", care reprezintă domenii majore de securitate si care poate fi folosite pentru a se construi grafice. Acesti indicatori, pentru care calculele sunt disponibile în cunostintele MEHARI, sunt:

- Organizarea securitătii (roluri si structuri);
- Constientizarea si instruirea privind securitatea;
- Site-ul de securitate fizică (acces controlat, instalare);
- Accesul controlat în zonele sensibile;
- Protectia împotriva diferitelor riscuri (incendiu, inundatii, etc);
- Arhitectura de securitate a retelei (acces controlat, sub-retele logice, firewall, nivelurile de serviciu, etc);
- Comunicatii confidentiale si gestionarea integrătii;
- Accesul logic controlat (sisteme, aplicatii si date);
- Securitatea datelor;
- Proceduri operationale;
- IT de gestionare a mass-media;
- Gestionarea crizelor si planuri de back-up;
- Back-up-uri, planificarea lor, si planurile de restaurare a serviciilor;
- Întretinere;
- Proiecte de IT si dezvoltarea securitătii;
- Gestionarea incidentelor.

Este demn de remarcat faptul că în timpul unui audit partial care acoperă o temă sau un anumit număr de teme (de exemplu întretinerea sau securitatea proiectelor de dezvoltare), este mai facilă concentrarea asupra serviciilor de securitate care contribuie la temele selectate.

5.3 Respectarea măsurilor incluse în standardul ISO / IEC 27002: 2005

După cum s-a explicat în documentul "MEHARI: Concepte fundamentale si specificatii functionale", o revizuire a securitătii poate la fel de bine să servească drept un mijloc de a documenta nivelul de bună practică recomandat de standardul ISO / IEC 27002:2005.

Efectiv, fiecare întrebare din procesul de audit MEHARI poate fi văzută ca un punct de control elementar, ce este menită să valideze solutiile si procesul de securitate implementate de către entitatea organizatională.

Pentru ca organizarea auditului MEHARI să scoată la lumină capacitatea de a reduce riscul, la fiecare nivel operational si cu contributia managerilor operationali, structura de servicii nu este perfect aliniată cu „structura descriptivă” standard.

În plus, chestionarele MEHARI contin un anumit număr de servicii si controale care merg dincolo de recomandările standardului. Astfel, a fost realizată o cartografiere a întrebărilor MEHARI pe practicile standardului ISO.

Chestionarele de audit MEHARI 2007 facilitează cartografierea si furnizează un tabel de corespondente (cu formulele adecvate) în baza de date a cunostintelor.

Astfel, este posibil să se vizualizeze[2] nivelul operational de maturitate al entității pentru fiecare punct de control al standardului (cu scorul de 0-4, de exemplu). Acest lucru nu este obiectivul principal MEHARI, dar poate furniza informatii utile în timpul procesului de certificare sau atunci când se compară diferite organizatii.

6. Sfaturi practice

6.1 Puncte importante de inclus în scheme de audit

Uneori o schemă de audit este percepută ca fiind complicată. Nu există nici un motiv pentru acesta -este doar un instantaneu al stării diferitelor solutii si situatii.

Un mainframe si sistem UNIX sunt diferite, precum si sistemele lor de securitate si operatiunile lor, sunt în mod inevitabil diferite. Aceste diferente pot fi ignorate sau luate în considerare, în functie de circumstante. În cazul în care diferentele sunt luate în calcul, chestionarele ar trebui să fie copiate în mod corespunzător si întrebările similare puse unor grupuri diferite. Dacă preferati să se ignore aceste diferente, întrebările vor fi postate doar o dată la nivel global, dar acest lucru se realizează independent de metodologia auditului.

Schemă de audit reprezintă doar un mijloc facil de a diferentia domeniile diferite de solutii în timpul procesului de audit.

Distinctia între domeniile de solutii este doar o chestiune de alegere. O abordare în general bună a problemei este să se ia în considerare cât de multi oameni diferiti vor trebui să fie intervievati pentru acelasi domeniu.

Practic, întrebarea este "cât de multe persoane diferite pot avea atât de multe puncte de vedere diferite asupra aceleiasi situatii?". Fiecare punct de vedere diferit necesită un interviu specific, însă două puncte de vedere similare nu ar justifica risipa de timp si energie pentru interviuri separate.

6.2 Puncte importante care trebuie atinse în procesul de audit

Am insistat déjà asupra necesitătii de a completa chestionarele în timpul interviurilor fată-în-fată, astfel încât comentariile si restul s poata fi incluse.

Am sugerat de asemenea că, în cazul în care răspunsurile nu sunt în mod clar "da" sau "nu", este mai adecvată o viziune pesimistă, în timp ce adăugarea explicatiilor ca si comentarii arată o latură mai pozitivă.

Bazele de cunostinte MEHARI si, în special, chestionarele de audit, au fost proiectate folosind următorul principiu de precautie:

Procedurile automate de abordare nu trebuie vreodată să permită ca un risc să fie sub-evaluat. Întotdeauna este preferabil să se aibă un risc initial supra-evaluat, atunci când acesta poate fi redus mai târziu, decât să-l aibă sub-evaluat si să nu se regăsească într-o analiză mai detaliată.

---

2 Instrumentul RISICARE permite acest nivel de vizualizare

Unul dintre principiile de bază este să se încerce evitarea cazurilor în care procedurile automate ar elimina un scenariu de risc scăzut, atunci când de fapt riscul ar putea fi ridicat.La sub-evaluarea gravitătii unui scenariu contribuie o serie de factori, printre care se numară supra-evaluarea anumitor servicii de securitate.

Conform acestui principiu, ca rezultatele unui audit de securitate să poată fi folosite pentru analizarea riscurilor unei organizatii în general, sistemul de notare aplicat serviciilor de securitate trebuie să fie unul prudent.

Punctajul final poate părea uneori sever, în comparatie cu alte sisteme de audit. Cititorul ar trebui să aibă în vedere faptul că MEHARI insistă asupra faptului că serviciile de securitate trebuie să fie eficiente, robuste si permanente, ceea ce reprezintă obiectul unui control regulat. Sfatul nostru final este să se garanteze asigurarea securitătii prin această abordare. Acest lucru nu este întotdeauna valabil cu alte abordări.

In spiritul diseminarii

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11, rue de Mogador
75009 Paris France
✆ 01 53 25 08 80
clusif@clusif.asso.fr