MEHARI 2010

Overzicht

December 2010

Methods working group

Gelieve uw vragen en commentaren te posten op dit forum:
http://mehari.info/

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11, rue de Mogador, 75009 Paris (France)
Tel.: +33 1 53 25 08 80 – Fax: +33 1 53 25 08 88
clusif@clusif.asso.fr – http://www.clusif.asso.fr

MEHARI is een geregistreerd handelsmerk van CLUSIF.

De wet van 11 maart 1957, volgens de paragrafen 2 en 3 van het artikel 41, autoriseert enkel, enerzijds, "kopieën of reproducties strikt voorbehouden voor particulier gebruik van de kopieerder, en niet bestemd voor een collectief gebruik" en, anderzijds, analyses en korte citaten die tot doel hebben als voorbeeld en illustratie te dienen".
Elke volledige of gedeeltelijke reproductie, gemaakt zonder de toestemming van de auteur of de rechthebbende partijen of de juridische opvolgers is illegaal" (1ste paragraaf van het artikel 40).
Deze representatie of reproductie, met om het even wel proces, zal als een vervalsing bestraft worden door de artikelen 425 en volgende van het wetboek van Strafrecht.

ERKENNINGEN

CLUSIF wil speciaal Frederic PETITJEAN (departement communicatie van de Koninklijke Federatie van Belgische Notarissen), Philippe SIX, Luc GOLVERS en Charlotte MAERTENS van BELCLIV-CLUSIB (Belgische Club voor de Informaticaveiligheid) voor deze vertaling en de leden van de commissie Methoden die hebben deelgenomen aan de realisatie van dit document:

Jean-Philippe	Jouas	Verantwoordelijk voor Methoden Commissie Verantwoordelijk voor de Werkgroep Principes, Mechanismen en Kennisbronnen voor MEHARI
Jean-Louis	Roule	Verantwoordelijk voor de Werkgroep MEHARI Documentatie
Dominique	Buc	BUC S.A.
Olivier	Corbier	Docapost
Martine	Gagné	HydroQuébec
Moïse	Hazzan	Ministerie van Gouvernementele Diensten Québec
Gérard	Molines	Molines Consultants
Chantale	Pineault	AGRM
Luc	Poulin	CRIM
Pierre	Sasseville	Ministerie van Gouvernementele Diensten Québec
Claude	Taillon	Ministerie van Onderwijs, Vrije Tijd en Sport Québec
Marc	Touboul	BULL SA

1 INLEIDING

De MEHARI-methodiek werd oorspronkelijk ontworpen en voortdurend bijgewerkt om Chief Information Security Officers (CISO's) bij te staan in hun beheer van informatiebeveiligingstaken. Dit overzicht is voornamelijk gericht op hen, maar is ook bestemd voor accountants, CIO's of risico managers die grotendeels dezelfde of soortgelijke uitdagingen delen.

Het belangrijkste doel van dit document is om te beschrijven hoe MEHARI kan worden gebruikt. Een meer gedetailleerde beschrijving van de methodologie en de bijbehorende instrumenten is opgenomen in andere documenten beschikbaar bij Clusif, in het bijzonder:

- MEHARI: Concepten en functionele specificaties,
- MEHARI Handleidingen: voor
  - Inzetanalyse en classificatie,
  - evaluatie van de veiligheidsdiensten en
  - risicoanalyse,
- MEHARI Handleiding van de veiligheidsdiensten,
- MEHARI Kennisbronnen

MEHARI's eerste doelstelling is het verschaffen van een risicobeoordeling en -management methode, met name op het gebied van informatiebeveiliging, die voldoet aan de ISO / IEC 27005:2008-eisen en het verstrekken van een set van tools en elementen die nodig zijn voor de uitvoering ervan[1].

Bijkomende doelstellingen zijn:

Een directe en individuele analyse voorzien van risicovolle situaties, beschreven door scenario's.

Te zorgen voor een complete set van tools die specifiek ontworpen zijn voor security management op korte, middellange en lange termijn, en die aan te passen zijn aan de verschillende niveaus en de overwogen acties.

Inderdaad, MEHARI voorziet een consistente methodologie, met passende kennisdatabanken, om Chief Information Security Officers (CISO's), algemene managers en security managers, of andere mensen die betrokken zijn bij risicoreductie, in hun verschillende taken en acties te helpen.

MEHARI's relatie met ISO / IEC 27000-normen wordt beschreven op het einde van het document.

1 De tools en de bijbehorende middelen, geleverd door MEHARI in aanvulling op de standaard, worden beschreven en verantwoord in *MEHARI: Concepten en functionele specificaties*

2 GEBRUIK VAN MEHARI

MEHARI is vooral een methode voor risicobeoordeling en -beheer.

In de praktijk betekent dit dat MEHARI en de bijbehorende kennisbronnen zijn ontworpen voor een nauwkeurige analyse van risicovolle situaties beschreven in scenario's.

Over het algemeen is security management een functie of activiteit die evolueert in de tijd. Corrigerende maatregelen zijn verschillend afhankelijk van de vraag of de organisatie nog niets heeft gedaan in het domein, of - integendeel - aanzienlijke investeringen qua tijd en moeite heeft gedaan. In de eerste stappen naar een beveiliging, is het ongetwijfeld aan te raden om de balans op te maken van de toestand van de bestaande veiligheidsmaatregelen en het beleid van de organisatie, en om deze af te zetten tegen de *best practices*, om de in te vullen kloof te verduidelijken.

Volgend op deze statusbeoordeling en het besluit om organisatorische beveiligingsmaatregelen te implementeren, zal er over concrete acties besloten moeten worden. Dergelijke besluiten, die doorgaans worden ingedeeld in de plannen, bedrijfsregels, het beleid of een veiligheidsreferentiekader, dienen te worden gemaakt met behulp van een gestructureerde aanpak. Deze aanpak kan worden gebaseerd op risicoanalyse, zoals vereist door ISO / IEC 27001 als onderdeel van een ISMS (Information Security Management System). Ook andere middelen zijn voorhanden, zoals benchmarking, hetzij intern, professioneel of inter-professioneel.

In dit stadium moet, zonder uitdrukkelijk risicoanalyse te vermelden, beantwoord worden wat de inzet van de beveiliging is. Heel vaak, hoe de beslissing ook is genomen, zal de persoon die het definitieve besluit voor de toewijzing van de desbetreffende kredieten neemt, ongetwijfeld de vraag stellen "is dit echt nodig?". Vanwege het ontbreken van een voorlopige beoordeling van en een algemene overeenstemming over de betrokken inzet, worden veel veiligheidsprojecten verwaarloosd of vertraagd.

Vaak later, maar soms vanaf het begin van een veiligheidsaanpak, zal het reële risico dat de organisatie of onderneming loopt in vraag gesteld worden. Dit wordt vaak geformuleerd in soortgelijke bewoordingen als deze: "Zijn alle risico's waaraan de organisatie kan worden blootgesteld, geïdentificeerd en is er enige zekerheid dat de niveaus ervan aanvaardbaar zijn?". Deze vraag kan net zo goed worden gevraagd op bedrijfsniveau, of in verwijzing naar een specifiek project. Een methodiek die risicoanalyse omvat, is vereist.

MEHARI is gebaseerd op het principe dat de instrumenten die nodig zijn in elk stadium van de beveiligingsontwikkeling, consequent moeten zijn. Hierbij moet worden begrepen dat de eventuele resultaten gegenereerd in een bepaald stadium, herbruikbaar moeten zijn door andere tools later of elders in de organisatie.

De verschillende instrumenten en modules van de MEHARI-methode, ontworpen om een directe en individuele risicoanalyse te begeleiden, kunnen afzonderlijk worden gebruikt van elkaar in elke stap van de ontwikkeling van een beveiliging, met behulp van verschillende managementbenaderingen, en staan garant voor consistentie in de daaruit voortvloeiende besluiten.

Al deze tools en modules - hieronder kort beschreven - omvatten een consistente risicobeoordelingmethode met de vereiste ondersteunende tools en modules voor het analyseren van de inzet en de controle van de kwaliteit van de veiligheidsmaatregelen, enz.

2.1 Risicoanalyse of -beoordeling

Risicoanalyse wordt genoemd in bijna elke publicatie over veiligheid, als de drijvende kracht om de veiligheidseisen te uiten. Dit wordt ook onderschreven door ISO / IEC-normen.

Echter, de meeste laten na te bespreken welke methoden moeten worden gebruikt.

Al meer dan 15 jaar voorziet Mehari in een gestructureerde aanpak voor de evaluatie van risico's[2], gebaseerd op enkele eenvoudige principes.

Een risicosituatie kan worden gekenmerkt door verschillende factoren:

- Structurele (of organisatorische) factoren, die niet afhankelijk zijn van veiligheidsmaatregelen, maar van de kernactiviteit van de organisatie, haar omgeving, en zijn context.
- Risicobeperkende factoren die een directe functie zijn van geïmplementeerde beveiligingsmaatregelen.

De analyse van de veiligheidsinzet is nodig om de maximale ernst van de gevolgen van een risicosituatie vast te stellen. Dit is typisch een structurele factor, terwijl de beoordeling van de veiligheid zal worden gebruikt om factoren te evalueren die het risico verminderen.

MEHARI maakt een kwalitatieve en kwantitatieve evaluatie van deze factoren mogelijk en helpt bijgevolg bij het evalueren van de risiconiveaus. Aldus integreert MEHARI instrumenten (zoals de criteria voor de beoordeling, formules, enz.) en kennisbronnen (met name voor het diagnosticeren van beveiligingsmaatregelen), die een essentiële aanvulling vormen op het minimum kader voorgesteld door ISO / IEC 27005.

2.1.1 Systematische analyse van de risicovolle situaties

Om een antwoord te kunnen geven op de vraag ‘Wat zijn de risico’s die boven een organisatie hangen en zijn ze aanvaardbaar of niet?’ is een gestructureerde aanpak nodig om alle potentiële risicosituaties te identificeren, om de meest kritische van hen individueel te analyseren en vervolgens acties te identificeren om het risico te verminderen tot een aanvaardbaar niveau.

De aanpak van MEHARI is gebaseerd op een kennisdatabank rond risicosituaties en op geautomatiseerde procedures voor de evaluatie van de factoren die kenmerkend zijn voor elk risico en die toestaan het niveau ervan te beoordelen. Bovendien biedt de methode hulp bij de selectie van een passende aanpak.

Met het oog op risico-evaluatie, worden twee belangrijkste opties voorgesteld:

- Ofwel het gebruik van een reeks van functies van de kennisbasis (voor Microsoft Excel of Open Office), om de resultaten van MEHARI-modules (bijvoorbeeld classificatie van de activa volgens de inzet analyse, diagnostiek van veiligheid) te integreren. Vanuit deze functies is het mogelijk om het huidige niveau van de risico's te beoordelen en aanvullende maatregelen voor risicoreductie voor te stellen.
- Of een softwareapplicatie, (zoals RISICARE[3]), die een rijkere gebruikersinterface biedt en simulaties, visualisaties en verdere optimalisaties toelaat.

2 Een gedetailleerde beschrijving van het risicomodel staat in *MEHARI Fundamentele Principes en Functionele specificaties.*

3 Van BUC S.A. software editor

2.1.2 Spontane analyse van risicosituaties

Dezelfde set van tools kan worden gebruikt op elk moment in andere benaderingen van veiligheidsmanagement. In sommige takken van de sturing van de veiligheid, waar risicomanagement niet het belangrijkste doel is en waar de veiligheid wordt beheerd door middel van audits of veiligheidsreferentiekaders, zullen er vaak specifieke gevallen zijn waarin de regels niet kunnen worden toegepast. Spontane risicoanalyse kan worden gebruikt om te beslissen wat de beste manier is om verder te gaan.

2.1.3 Risicoanalyse in nieuwe projecten

Het model van risicoanalyse en de mechanismen kunnen worden gebruikt in projectmanagement, met als resultaat een plan tegen de risico's en een beslissing welke maatregelen moeten worden genomen.

2.2 Veiligheidsbeoordelingen

MEHARI integreert grondige diagnostische vragenlijsten van de bestaande veiligheidscontroles, met als doel de beoordeling van de kwaliteit van de mechanismen en oplossingen die gericht zijn op vermindering van het risico[4].

2.2.1 De kwetsbaarheidsreview, een element van risicoanalyse

MEHARI voorziet een gestructureerd risicomodel dat rekening houdt met "de risicoreducerende factoren", in de vorm van veiligheidsdiensten.

De daaruit voortvloeiende kwetsbaarheidevaluatie zal dan ook een belangrijke input vormen voor de risicoanalyse door ervoor te zorgen dat de veiligheidsdiensten hun rol daadwerkelijk vervullen - een essentieel punt voor de geloofwaardigheid en betrouwbaarheid van de risicoanalyse.

Een essentiële kracht van Mehari, is zijn vermogen om het huidige risiconiveau te beoordelen, evenals de toekomstige niveau(s) op basis van deskundige kennis in het evalueren van het kwaliteitsniveau van de veiligheidsmaatregelen, of ze nu al in voege zijn of er toe besloten werd.

2.2.2 Veiligheidsplannen op basis van de kwetsbaarheidreviews

Een mogelijke aanpak is om actieplannen op te bouwen als rechtstreeks gevolg van de beoordeling van de toestand van de veiligheidsdiensten.

Het proces van veiligheidsbeheer dat deze benadering volgt, is uiterst eenvoudig: voer een beoordeling uit en beslis om alle diensten die niet beschikken over een voldoende kwaliteitsniveau te verbeteren.

De diagnostische vragenlijsten van MEHARI kunnen gebruikt worden in deze aanpak.

Een eerste analyse van de zakelijke belangen moet ook worden voorzien, om zo een link naar deze module van MEHARI te voorzien. De inzetanalyse maakt het mogelijk om de vereiste kwaliteit vast te stellen voor de relevante veiligheidsdiensten en, bijgevolg, de anderen te negeren als onderdeel van de beoordeling.

4 Beveiligingscontroles, of maatregelen zijn gegroepeerd in sub-diensten, dan diensten en tot slot in veiligheidsdomeinen.

2.2.3 Ondersteuning door de kennisbronnen bij het creëren van een veiligheidsreferentiekader

MEHARI's unieke kennisbron kan direct gebruikt worden om een beveiligingreferentiekader (of beveiligingsmaatregelen) te creëren, die de set van de veiligheidsregels en -instructies die de onderneming of organisatie zal volgen, zal bevatten en beschrijven.

Deze aanpak wordt vaak gebruikt in organisaties of bedrijven met een aantal onafhankelijke opererende eenheden of sites. Dit zou normaal gesproken het geval zijn voor grote multinationals met verschillende filialen, maar is net zo gemakkelijk van toepassing op middelgrote bedrijven met een groot aantal regionale filialen of agentschappen. In dergelijke gevallen is het werkelijk moeilijk om tal van evaluaties of risicoanalyses uit te voeren.

De opbouw van het veiligheidsreferentiekader

De beoordelingsvragenlijsten van MEHARI zijn een goede basis voor veiligheidsmanagers om te beslissen wat er moet worden toegepast in hun organisatie.

Het beheer van uitzonderingen op de regels

De creatie van een set van regels, door middel van een beveiligingsreferentiekader, botst vaak op de plaatselijke moeilijkheden bij de uitvoering; er moeten dus vrijstellingen en uitzonderingen op de regels worden beheerd.

Een samenhangende kennisbron, met een consistente set van tools en een analytische methodologie, laat toe om lokale verschillen te beheren. Verzoeken om uitzonderingen kunnen worden gedekt door een specifieke risicoanalyse gericht op de vastgestelde moeilijkheden.

2.2.4 Domeinen van de module kwetsbaarheidsbeoordeling

Uit het oogpunt van een risicoanalyse, voor het identificeren van alle risicovolle situaties en de wens om alle onaanvaardbare risico's te dekken, beperkt MEHARI zich niet tot het IT-domein.

De beoordelingsmodule omvat, afgezien van het informatiesysteem, de algemene organisatie en de sitebescherming in het algemeen, alsook de werkomgeving en de wettelijke en regelgevende aspecten.

2.2.5 Overzicht van de beoordelingsmodule

Een zaak om in gedachten te houden over de module kwetsbaarheidsbeoordeling is dat het een breed en consistent beeld van beveiliging biedt. Dit kan worden gebruikt in verschillende benaderingen, evolutief in de diepte en de mate van detaillering van de analyse, en kan gebruikt worden in alle stadia van het veiligheidsbewustzijn en –organisatie van de onderneming.

2.3 Het analyseren van de inzet

Veiligheid gaat over de bescherming van activa. Ongeacht de oriëntatie van het veiligheidsbeleid, is er één principe waarover alle managers het eens zijn; dat er een goed evenwicht moet zijn tussen investeringen in de beveiliging en het belang van de relevante zakelijke inzet.

Dit betekent dat een goed begrip van de zakelijke belangen van fundamenteel belang is, en dat de analyse van de veiligheidsinzet een hoge prioriteit en een strikte en gestructureerde evaluatiemethode verdient.

Het doel van een analyse van de beveiligingsinzet is een antwoord op de dubbele vraag:

"Wat kan er gebeuren, en als er iets gebeurt, zou het ernstig zijn?"

Dit toont aan dat op het gebied van veiligheid, de inzet wordt gezien als het gevolg van gebeurtenissen die de beoogde activiteiten van een onderneming of organisatie verstoren.

MEHARI voorziet een module voor de analyse van de inzet, zoals beschreven in MEHARI*: Stakes analyse en classificatie*, welke twee soorten resultaten produceert:

- Een storingsschaal
- Een classificatie van informatie en van IT-activa

De storingsschaal

De identificatie van storingen of potentiële gebeurtenissen is een proces dat begint met de activiteiten van de onderneming en bestaat uit het identificeren van mogelijke storingen in de operationele processen. Het zal resulteren in:

- Een beschrijving van de mogelijke soorten storingen
- Een definitie van de parameters die de ernst van elke storing beïnvloed
- Een evaluatie van de kritische drempels van deze parameters die de ernst van de storing veranderen

Deze set van resultaten vormt een storingsschaal.

Classificatie van informatie en activa

Het is gebruikelijk in IT-systeembeveiliging om te spreken van de indeling van de informatie en de indeling van IT-activa.

Een dergelijke indeling bestaat uit het definiëren, voor elk type van informatie en voor elke IT-activa, en voor elk indelingscriterium (klassiek: beschikbaarheid, integriteit en vertrouwelijkheid, hoewel andere criteria kunnen worden gebruikt, zoals traceerbaarheid) van representatieve indicatoren van de ernst van het criterium dat beïnvloed wordt of verloren gaat voor deze informatie of activa.

De indeling van de informatie en activa, voor informatiesystemen, is de eerder gedefinieerde storingsschaal, vertaald in gevoeligheidsindicatoren in verband met de IT-activa.

Uitdrukkenvan de beveiligingsinzet

De storingsschaal en de indeling van de informatie en de activa zijn twee verschillende manieren om de beveiligingsinzet uit te drukken.

De eerste is meer gedetailleerd en biedt meer informatie voor CISO's. De laatste is meer globaal en nuttiger voor bewustmakingscampagnes en communicatie, maar is minder gedetailleerd.

2.3.1 Het analyseren van de inzet, de basis voor een risicoanalyse

Deze module is duidelijk de sleutel bij risicoanalyse. Zonder een gemeenschappelijk akkoord over de gevolgen van mogelijke storingen, zal een oordeel over risiconiveaus niet mogelijk

zijn. MEHARI biedt een rigoureuze methode voor de beoordeling van de inzet en de activaclassificatie, welke objectieve en rationele uitkomsten biedt.

2.3.2 De analyse van de beveiligingsinzet: de hoeksteen van elkstrategisch actieplan

Uiteraard is het analyseren van de inzet nodig voor de uitvoering van eender welk beveiligingsplan. Ongeacht de gebruikte benadering die wordt gebruikt, op een bepaald punt, zullen middelen moeten worden toegewezen om actieplannen uit te voeren, en onvermijdelijk zal de rechtvaardiging voor een dergelijke investering in discussie gesteld worden.

De middelen en de fondsen die zullen worden toegewezen aan de veiligheid zijn, zoals voor de verzekeringpolissen, in directe verhouding tot het risico. Als er geen overeenstemming is over de mogelijke storingen, dan is het zeer onwaarschijnlijk dat een budget zal worden toegewezen.

2.3.3 Indeling: een essentieel element van het veiligheidsbeleid

Beveiligingsreferentiekaders, veiligheidsbeleid, en de bijbehorende aanpak van veiligheidsmanagement zijn al genoemd in dit document.

In de praktijk zullen bedrijven die beveiliging beheren via een set van regels, verplicht zijn om te differentiëren, in de regels zelf, tussen de acties die worden uitgevoerd als een functie van de gevoeligheid van de informatie die verwerkt wordt. Het is gebruikelijk om te verwijzen naar een classificatie van informatie- en IT-systeem activa.

MEHARI's module voor de analyse van de veiligheidsinzet biedt de middelen om deze classificatie uit te voeren.

2.3.4 Analyse Veiligheidsinzet: de basis van het veiligheidsplan

Het hele proces van de veiligheidsinzetanalyse, dat uiteraard de bijdrage van de operationele managers vereist, leidt vaak tot de noodzaak voor directe actie.

De ervaring leert dat, wanneer het hoogste operationele management geïnterviewd is, ongeacht de grootte van de organisatie, en ze daarbij hun visie en inschatting van de ernstige storingen hebben uitgelegd, dat dit leidt tot veiligheidsbehoeften die zij voordien niet hadden overwogen en die snelle reacties vereisen.

Actieplannen kunnen dan onmiddellijk gecreëerd worden, met behulp van een lichte en directe benadering gebaseerd op de combinatie van soorten expertise: dat van de beroepsgroep zelf, door het operationele beheer, en dat van beveiligingsoplossingen, verstrekt door beveiligingsexperts.

2.4 Algemeen overzicht van het gebruik van MEHARI

Het is duidelijk dat de risicobeoordeling en -reductie, de belangrijkste oriëntatie van MEHARI is. De gebruikte kennisbronnen, de mechanismen en de instrumenten zijn gemaakt voor dat doel.

De behoefte aan een gestructureerde methode voor risicoanalyse en -reductie, kan, in de hoofden van de ontwerpers van de methodologie, de volgende zijn, afhankelijk van de organisatie:

- Een permanente werkwijze - richtlijnen voor een gespecialiseerde groep,
- Een werkmethode die parallel gebruikt wordt met andere praktijken voor veiligheidsbeheer,

- Een werkmethode af en toe gebruikt om reguliere praktijken aan te vullen.

Met dit in gedachten, biedt MEHARI een reeks benaderingen en instrumenten waarmee men een risicoanalyse kan maken wanneer nodig.

De MEHARI-methodologie, bestaande uit de kennisbronnen, de handleidingen en de gidsen die de verschillende modules beschrijven (belangen, risico's, kwetsbaarheden), is er om mensen te helpen die betrokken zijn bij security management (CISO's, risicomanagers, accountants, CIO's, ...), in hun verschillende taken en acties.

3 MEHARI EN ISO/IEC 27000 STANDAARDEN

Een vraag die vaak gesteld wordt is: hoe komt MEHARI overeen met de internationale normen - met name de ISO / IEC 27000-reeks.

De bedoeling is om hier uit te leggen hoe MEHARI past in de ISO 27001, 27002 en 27005 normen, in termen van compatibiliteit en doelen.

3.1 Derespectieve doelstellingen van ISO/IEC 27001, 27002, 27005 en MEHARI

3.1.1 Doelstellingen van de ISO/IEC 27002:2005-standaarden

Deze norm bepaalt dat een organisatie zijn veiligheidseisen moet identificeren met behulp van drie belangrijke bronnen:

- Risicoanalyse,
- Juridische, wettelijke, regelgevende of contractuele voorschriften,
- Het geheel van principes, doelen en eisen die gelden voor de verwerking van informatie die de organisatie heeft ontwikkeld om zijn operaties te ondersteunen.

Met dit als basis, kunnen controlepunten gekozen en geïmplementeerd worden met behulp van de lijst in de rubriek "gedragscode voor informatiebeveiliging" uit de standaard of die afkomstig zijn uit een andere reeks van controlepunten (§ 4.2).

NB: in het kader van 27002: 2005, is bepaald dat de norm "richtlijnen en algemene principes voor het initiëren, implementeren, onderhouden en verbeteren van het beheer van informatiebeveiliging" voorziet, wat betekent dat de ISO-norm kan worden gezien als een startpunt. Echter, ISO / IEC 27001 bepaalt (§ 1.2) dat elke uitsluiting moet worden gemotiveerd en dat het aanvaardbaar is om de controlepunten toe te voegen (Bijlage A - A.1).

De ISO 27002 norm voorziet een compilatie van richtlijnen, die een organisatie kan gebruiken. Hij wijst er echter op dat de lijst niet compleet is en dat aanvullende maatregelen nodig kunnen zijn. Echter, geen methodologie is aanbevolen voor de creatie van een compleet veiligheidsbeheerssysteem.

Aan de andere kant, elk deel van de gids met *best practices* bevat inleidingen en commentaren op de beoogde doelen, wat een zeer nuttige steun kan zijn.

NB: De ISO-norm bepaalt ook dat het kan worden gebruikt om "te helpen het vertrouwen in inter-organisatorische activiteiten op te bouwen". Dit is niet toevallig opgenomen en brengt een essentieel aspect naar boven dat ondersteuners van de standaard promoten, zijnde evaluatie (zelfs certificatie), uit een oogpunt van informatieveiligheid, van partners en leveranciers.

3.1.2 Doelstellingen van ISO/IEC 27001:2005

De duidelijke doelstelling van de ISO / IEC 27001 is om "een model te voorzien om een corporate **information security management systeem (ISMS)** te creëren en te beheren op bedrijfsniveau" en om "gebruikt te worden, hetzij intern of door derden, met inbegrip van certificatie-instanties."

Het beoordeling- en certificatiedoel legt een sterke nadruk op formele aspecten (documentatie en registratie van de besluiten, verklaring van toepasbaarheid, registers, enz.) en controle (reviews, audits, etc.).

Het is duidelijk dat de basis van de veiligheidsaanpak impliceert dat een risicoanalyse moet worden uitgevoerd, om de risico's waaraan de organisatie kan worden blootgesteld, te onderzoeken en om passende maatregelen te nemen om de risico's tot een aanvaardbaar niveau te brengen (paragraaf 4.2.1).

ISO / IEC 27001 bepaalt dat een methode voor risicoanalyse moet worden gebruikt, maar dit is geen onderdeel van de standaard en geen specifieke methode wordt voorgesteld, met uitzondering van de integratie van het recursieve proces PDCA (Plan, Do, Check, Act) van het model, zoals gedefinieerd voor de oprichting van de ISMS.

Ook zijn de aanbevelingen of *best practices* die kunnen worden gebruikt om risico's te verminderen "afgestemd op diegene die zijn opgenomen in ISO / IEC 27002:2005", terwijl een verbandhoudende lijst van controlepunten is opgenomen in de bijlagen.

Volgens ISO / IEC 27001 is de basis van de **evaluatie van het beveiligingssysteem** niet zozeer de kennis of de verificatie van de vraag of de beslissingen die zijn gemaakt, geschikt zijn en aangepast zijn aan de behoeften van de organisatie, maar veeleer om te controleren dat, zodra de besluiten zijn gemaakt, het managementsysteem zo is dat een auditeur of een certificeerder er zeker kan van zijn dat de beslissingen echt zijn geïmplementeerd.

3.1.3 Doelstellingen van ISO/IEC 27005:2008

De doelstellingen van deze norm zijn niet om een methode van risicomanagement te vormen, maar veeleer om een minimaal kader vast te stellen en vereisten beschrijven voor het risicobeoordelingsproces zelf, voor de identificatie van de bedreigingen en kwetsbaarheden die toelaat om de risico’s en hun niveau in te schatten en vervolgens om in een positie te zijn om een behandelingswijze, bijbehorende plannen en metingen gericht op de evaluatie en verbetering van de situatie, te selecteren.

De norm stelt dat een methode voor risicobeoordeling moet worden gekozen in overeenstemming met deze eisen, om het gebruik van inconsistente of simplistische methodes te vermijden, in vergelijking met de bedoeling van de opstellers van de standaard.

3.1.4 Doelstellingen van MEHARI

Mehari is een consistente set van tools en methodologische functies voor veiligheidsbeheer en de bijbehorende meting, op basis van een nauwkeurige risicoanalyse. De fundamentele aspecten van Mehari:

- het risico model (kwalitatief en kwantitatief),
- de overweging van de efficiëntie van de veiligheidsmaatregelen die geïmplementeerd of gepland zijn,
- de mogelijkheid tot het evalueren en simuleren van derestrisico’s als gevolg van aanvullende maatregelen,

zijn verplichte aanvullingen op de eisen van de ISO / IEC 27000-normen en in het bijzonder van ISO / IEC 27005.

3.1.5 Vergelijking van de doelen van Mehari en ISO / IEC 27001 en 27002 normen

De doelen van Mehari en de eerder genoemde ISO-normen zijn totaal verschillend.

- Mehari heeft tot doel instrumenten en methoden te voorzien die gebruikt kunnen worden om de meest passende beveiligingsmaatregelen te kiezen voor een bepaalde organisatie en om de restrisico's te beoordelen, zodra deze maatregelen van toepassing zijn. Dit is niet het primaire doel van de ISO-normen.
- De ISO-normen voorzien in een reeks van *best practices*, die zeker zeer nuttig zijn, maar niet noodzakelijkerwijs geschikt voor wat er op het spel staat in de organisatie, en nuttig zijn om de aspecten te dekken van de graad in beveiliging, informatiebeveiligingsplanning, onafhankelijke interne eenheden en partners.

De ***referentiehandleiding voor veiligheidsdiensten*** van Mehari biedt gedetailleerde elementen die kunnen worden gebruikt om een veiligheidskader op te bouwen en kan worden vergeleken met ISO / IEC 27002. Op dit punt is het duidelijk dat Mehari's dekking ruimer is dan die van ISO, en betrekking heeft op essentiële aspecten van de veiligheid buiten alleen dat van de informatiesystemen.

3.2 Compatibiliteit tussen deze benaderingen

De Mehari benadering is volledig verenigbaar met ISO 27002, omdat, hoewel ze niet dezelfde doelstellingen hebben, het relatief eenvoudig is om de resultaten van een Mehari-analyse voor te stellen in termen van ISO 27002-indicatoren.

Mehari beantwoordt aan de behoefte, uitgedrukt in zowel ISO 27001 en 27002 normen, voor een risicoanalyse om de maatregelen die moeten worden uitgevoerd, te definiëren.

3.2.1 Compatibiliteit met de ISO / IEC 27002:2005 norm

De standaardcontrolepunten of *best practices* van ISO zijn voornamelijk algemene, gedrags- of organisatorische maatregelen, terwijl Mehari daarenboven de noodzaak benadrukt van maatregelen waarvan de efficiëntie kan worden gegarandeerd.

Ondanks deze verschillen, voorziet de Mehari kwetsbaarheidsreview in correlatietabellen om indicatoren in lijn met de verdeling gebruikt in de ISO 27002:2005 norm te laten zien, deze zijn geschikt voor al degenen die behoefte hebben om hun overeenstemming met die norm te bewijzen.

Het is de moeite waard hier te vermelden dat de Mehari auditvragenlijsten werden ontworpen en samengesteld om het de operationele managers mogelijk te maken efficiënt de kwetsbaarheidsreviews te doorlopen en om van elke veiligheidsdienst de capaciteit om deze risico's te verminderen, af te leiden.

3.2.2 Compatibiliteit met de ISO / IEC 27001 standaard

Mehari kan gemakkelijk worden geïntegreerd in de PDCA (Plan - Do - Check - Act) processen zoals door ISO / IEC 27001 beschreven, en dan met name de 'Plan'-fase (§ 4.2.1). Mehari dekt volledig de beschrijving van de taken die de oprichting van de ISMS-basissen mogelijk maken.

Voor de 'DO-fase (§ 4.2.2), die streeft naar de uitvoering en het beheer van ISMS, biedt Mehari nuttige uitgangselementen zoals de bouw van de plannen voor het risicobeheer, met prioriteit die rechtstreeks verband houd met de risico-indeling en de voortgangsmetingen tijdens het gebruik ervan.

Voor de fase 'CHECK' (§ 4.2.3), voorziet Mehari elementen die de beoordeling van de restrisico's en verbeteringen gemaakt in de veiligheidsmaatregelen, mogelijk maken.

Daarnaast kunnen eventuele wijzigingen in de omgeving (zoals de inzet, bedreigingen, oplossingen en organisatie) eenvoudig opnieuw geëvalueerd worden door middel van gerichte audits, die de resultaten van de eerste Mehari-audit gebruiken. Zo kunnen de veiligheidsplannen worden herzien en in de tijd evolueren.

Voor de fase 'ACT' (§ 4.2.4), roept Mehari impliciet de controles en continue verbetering van de veiligheid in, om zodoende te garanderen dat de doelen voor risicoreductie zijn bereikt. Hoewel Mehari niet in het hart zit van de processen, draagt het in deze drie fasen sterk bij aan hun uitvoering en zorgt het voor hun efficiëntie.

3.2.3 Compatibiliteit met de ISO / IEC 27005:2008 norm

Het kader vastgesteld door deze nieuwe standaard is volledig van toepassing op de manier waarop Mehari het mogelijk maakt risico's te beheersen, bijvoorbeeld:

- De processen voor risicoanalyse, evaluatie en behandeling (overgenomen uit ISO 13335),
- De identificatie van de primaire en ondersteunende activa plus de indelingsniveaus ervan, volgend op de inzetsanalyse,
- De identificatie van bedreigingen met inbegrip van hun niveau (natuurlijke blootstelling), waarvoor Mehari nauwkeuriger is voor de beschrijving van de risicoscenario's,
- De identificatie en kwantificatie van de efficiëntie van de veiligheidsmaatregelen (of controles) in de vermindering van de kwetsbaarheden,
- De combinatie van deze elementen voor de beoordeling van het ernstniveau van risicoscenario's, op een schaal met 4 niveaus.
- De mogelijkheid om direct de veiligheidsmaatregelen te selecteren die nodig zijn voor de risicoreductieplannen.

Daarom is Mehari niet alleen eenvoudig te integreren in een ISMS-proces, zoals gepromoot door ISO 27001, maar voldoet volledig aan de ISO 27005-eisen voor risicomanagement.

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11, rue de Mogador
75009 Paris (France)
✆ +33 1 53 25 08 80
clusif@clusif.asso.fr

Download CLUSIF productions at:
www.clusif.asso.fr