MEHARI

Guide du diagnostic de l'état des services de sécurité

Mai 2017

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11, rue Mogador, 75009 PARIS

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

Web : http://www.clusif.fr

Remerciements

La mise à jour de ce document, initialement publié par le CLUSIF, a été réalisée par le CLUSIQ, Club de la Sécurité de l'Information du Québec.
Que les personnes qui ont rendu possible la réalisation de ce document, en soient remerciées, tout particulièrement :

Jean-Philippe	Jouas	Ancien président du CLUSIF Ancien Responsable de l'Espace Méthodes du CLUSIF Créateur de la méthode
Jean-René	Blanchet	CAA-Québec
Guirec	Duperrin	GDC-Conseil
Gilles	Gouin	MAX2G
Christophe	Jolivet	PR4GM4
Benoit	Laliberté	VICTRIX
Chantale	Pineault	VICTRIX
Jean-Louis	Roule	

Sommaire

1 Introduction

Les principes fondamentaux de MEHARI ont été présentés dans le document « *MEHARI – Principes fondamentaux et spécifications fonctionnelles* ».

Ces principes incluent la nécessité d'une base de connaissance de services de sécurité incluant :

- La définition des services de sécurité
- La définition de critères d'évaluation des niveaux de qualité : paramètres à prendre en compte et niveaux de qualité
- Des questionnaires permettant le diagnostic de la qualité des services de sécurité.
- La définition d'une base métrologique pour évaluer la qualité des services de sécurité

Nous revenons sur ces diverses définitions avant d'aborder le diagnostic proprement dit des services de sécurité

2 Définitions

2.1 Services de sécurité

Un **service de sécurité** est une réponse à un besoin de sécurité, exprimée en termes génériques et fonctionnels décrivant la finalité du service, généralement en référence à certains types de menaces.

Un service de sécurité décrit une fonction de sécurité.

Cette **fonction** est **indépendante des mécanismes et solutions concrètes** permettant la réalisation effective du service.

Exemple : le service « Contrôle d'accès », dont la finalité ou fonction, décrite implicitement par son titre, est de contrôler les accès, c'est à dire de ne laisser passer que les personnes autorisées.

2.1.1 Services et sous-services de sécurité

La fonction assurée par un service de sécurité peut, elle-même, nécessiter plusieurs éléments complémentaires, qui peuvent être considérés comme des « sous-fonctions ». Dans l'exemple ci-dessus, le contrôle d'accès nécessite la connaissance de ce qui est autorisé, ce qui fait appel à une fonction d'autorisation, la reconnaissance d'une personne, ce qui fait appel à une fonction d'authentification, et le filtrage des accès, ce qui fait appel à une troisième fonction de filtrage.

Un service de sécurité peut ainsi lui-même être constitué de plusieurs autres services de sécurité pour répondre à un besoin ou une finalité déterminée. ***Chacun des constituants est un sous-service de sécurité*** du service en question, tout en conservant, vis-à-vis d'une fonction qui lui est propre, les caractéristiques d'un service, telles que définies plus haut.

2.1.2 Mécanismes et solutions de sécurité

Un "**Mécanisme**" est une manière particulière d'assurer, totalement ou partiellement, la fonction du service ou du sous-service. Il peut s'agir de procédure spécifique, d'algorithme, de technologie, etc.

Pour le sous-service d'authentification abordé précédemment, les mécanismes possibles (pour l'authentification aux systèmes d'information) sont les mots de passe, les jetons, les processus reposant sur des algorithmes contenus dans des cartes à puce, les systèmes biométriques, etc.

Pour un sous-service donné, plusieurs mécanismes sont généralement possibles. Leur choix a très souvent un effet direct sur la qualité du sous-service concerné.

Une **solution de sécurité** est la réalisation concrète d'un mécanisme de sécurité et comprend les matériels et logiciels nécessaires à son déploiement, les procédures de déploiement et de support opérationnel ainsi que les structures organisationnelles nécessaires.

2.1.3 Typologie des services de sécurité

Certains services peuvent être considérés comme des mesures générales, d'autres comme des services techniques :

— Les mesures générales sont des mesures de sécurité reconnues comme utiles, voire nécessaires, à la sécurité des systèmes d'information, mais dont l'effet se situe davantage au plan de l'organisation, du pilotage de la sécurité ou de la sensibilisation, sans influence directe sur des situations de risques précises.

— Les mesures techniques ont un rôle précis, une finalité directe et ont un effet immédiat sur certaines situations de risque qu'il est possible de préciser.

2.2 Critères d'évaluation de la qualité des services de sécurité

Les services de sécurité peuvent avoir des niveaux de performance très différents selon les mécanismes employés. Ils seront plus ou moins efficaces (performants) dans leur fonction et plus ou moins robustes dans leur capacité à résister à une attaque directe.

2.2.1 Paramètres à prendre en compte

Pour mesurer la performance d'un service de sécurité, plusieurs paramètres doivent être pris en compte :

- L'efficacité du service
- Sa robustesse
- Les moyens de contrôle de son bon fonctionnement

Efficacité d'un service de sécurité

Pour les services dits techniques, l'efficacité mesure leur capacité à assurer effectivement la fonction demandée face à des acteurs ayant des compétences plus ou moins fortes ou face à des circonstances plus ou moins courantes.

Pour prendre l'exemple du sous-service "Gestion des autorisations d'accès au système d'information", qui concerne l'attribution des droits à des utilisateurs, la fonction du service est de faire en sorte que seules les personnes dûment habilitées par leur hiérarchie se voient effectivement attribuer des autorisations d'accès au système d'information. En pratique, l'efficacité du service dépendra de la rigueur du contrôle de l'authenticité de la demande et du contrôle de la position du demandeur vis-à-vis de l'utilisateur. S'il s'agit d'un simple courrier signé sans qu'il y ait dépôt de signature ni compte rendu à la hiérarchie, n'importe quelle personne connaissant un peu le circuit d'autorisation sera capable de se faire attribuer indûment des droits et la qualité du sous-service pourra être considérée comme faible.

L'efficacité d'un service contrôlant des actions humaines est ainsi la mesure des moyens et des compétences nécessaires pour qu'un acteur puisse passer au travers des contrôles mis en place ou pour les abuser.

Pour les services visant des événements naturels (tels que la détection incendie, l'extinction incendie, etc.), l'efficacité est la mesure de la « force » de l'événement pour lequel ils gardent leur effet.

S'il s'agit, par exemple, d'une digue destinée à empêcher une inondation due à la crue d'une rivière, l'efficacité sera directement liée à la hauteur de la crue (sa force) à laquelle la digue résiste. ***En pratique cette force sera souvent évaluée en fonction du caractère plus ou moins exceptionnel de l'événement.***

Les services qui sont des mesures générales ne peuvent pas, par principe, être évalués en fonction de leur finalité directe mais en fonction de leur rôle indirect.

L'efficacité des mesures générales mesure leur capacité à générer des plans d'action ou des changements significatifs de comportement

Robustesse d'un service de sécurité

La robustesse d'un service mesure sa capacité à résister à une action visant à le court-circuiter ou à l'inhiber.

La robustesse ne concerne que les services dits techniques.

Dans l'exemple précédent de gestion des autorisations, la robustesse du sous-service dépend, en particulier, des possibilités d'accès direct à la table des droits attribués aux utilisateurs et donc de se faire attribuer des droits sans passer par les processus normaux de contrôle mis en place.

Dans le cas de services visant des accidents ou des événements naturels (système de détection et d'extinction automatique d'incendie, par exemple), leur robustesse tiendra compte de leur capacité à résister à une mise hors circuit volontaire ou accidentelle.

Mise sous contrôle d'un service de sécurité

La qualité globale d'un service de sécurité doit enfin prendre en compte sa permanence dans le temps.

Pour cela, il convient que toute interruption de service soit détectée et que des mesures palliatives soient alors décidées. La qualité de ce paramètre dépend donc de la capacité et de la rapidité de détection et des moyens de réaction.

Pour les mesures générales, la mise sous contrôle représente d'une part, leur aptitude à être mesurées en termes de mise en œuvre ou d'effet et d'autre part la mise en place effective d'indicateurs et de systèmes de contrôle

2.2.2 Définition des niveaux de qualité des services de sécurité

La qualité d'un service de sécurité mesure ainsi son efficacité, sa robustesse et sa capacité d'autocontrôle. Globalement la qualité d'un service de sécurité est ainsi sa capacité de résistance à différents types d'attaque, en notant qu'aucune forteresse n'est inviolable.

La qualité d'un service de sécurité est notée sur une échelle allant de 0 à 4. Cette échelle reflète le niveau de force ou de compétence qu'il faut avoir pour violer le service, le court-circuiter et/ou inhiber ou rendre inefficace la détection de sa mise hors circuit.

Bien que cette échelle soit continue, il n'est pas inutile de donner quelques valeurs de référence pour la qualité de service.

Qualité de service évaluée à 1

Le service a une qualité minimale. Il peut ne pas être efficace (ou ne pas résister) à une personne quelconque, sans qualification particulière, ou tant soit peu initiée ou, dans le domaine des événements naturels, ne pas être efficace face à un événement relativement banal. Pour une mesure générale, elle aura très peu d'effet sur les comportements ou l'efficacité de l'organisation.

Qualité de service évaluée à 2

Le service reste efficace et résiste à un agresseur moyen, voire initié, mais pourrait être insuffisant contre un bon professionnel du domaine concerné (un informaticien professionnel pour un service de sécurité logique, un cambrioleur normalement équipé ou un "casseur" pour un service de sécurité physique des accès). Dans le domaine des événements naturels, un tel service pourrait être insuffisant pour des événements très sérieux, considérés comme rares. Pour les mesures générales, un tel service n'apportera une amélioration des comportements que dans des cas courants.

Qualité de service évaluée à 3

Le service reste efficace et résiste aux agresseurs et événements décrits ci-dessus, mais pourrait être insuffisant contre des spécialistes (hackers chevronnés et équipés, ingénieurs systèmes fortement spécialisés sur un domaine donné et dotés d'outils spéciaux qu'ils maîtrisent, espions professionnels, etc.) ou des événements exceptionnels (catastrophes naturelles). Une mesure générale de ce niveau aura un effet certain dans la très grande majorité des circonstances, mais peut-être pas dans des circonstances exceptionnelles.

Qualité de service évaluée à 4

Il s'agit du niveau le plus élevé et le service de sécurité reste efficace et résiste aux agresseurs et événements décrits ci-dessus. Il reste qu'il pourrait être mis en brèche par des circonstances exceptionnelles : meilleurs experts mondiaux dotés d'outils exceptionnels (moyens pouvant être mis en œuvre par des États importants) ou concours exceptionnels de circonstances elles-mêmes exceptionnelles.

Le processus d'évaluation de la qualité des services de sécurité prévu par MEHARI a été bâti pour fournir des évaluations de la qualité des services de sécurité répondant à ces définitions.

2.3 Bases de connaissances MEHARI des services de sécurité

MEHARI comprend plusieurs bases de connaissances, chacune incluant une base de services de sécurité comprenant des questionnaires de diagnostic organisés par domaines de responsabilité.

Cette organisation par domaine permet d'avoir des questionnaires séparés en fonction des interlocuteurs à rencontrer pour faire le diagnostic.

Les domaines sont différents, selon les bases de connaissances mais comprennent :

- Un domaine relatif à l'organisation de la sécurité
- Un ou deux domaines traitant de la sécurité physique
- Un ou plusieurs domaines relatifs à l'infrastructure informatique (systèmes et réseaux)
- Un ou plusieurs domaines relatifs à l'administration et l'exploitation de l'infrastructure
- Un ou plusieurs domaines relatifs à la sécurité applicative et aux développements
- Un domaine traitant des postes de travail utilisateurs
- Eventuellement des domaines relatifs aux processus de management

2.4 Système de mesure de la qualité des services de sécurité

Le système de mesure de la qualité des services de sécurité de MEHARI est basé sur un système de cotation des réponses aux questions, **questions auxquelles il est demandé de répondre par oui ou par non**, avec des conventions de cotation et de pondération que nous étudierons plus loin.

Nous donnons ci-dessous un extrait du questionnaire relatif au contrôle d'accès aux systèmes et applications et plus particulièrement à la gestion des autorisations et privilèges.

Questionnaire d'audit : Domaine des Systèmes (07)	
Service : A. Contrôle d'accès aux systèmes et applications **Sous-service : A02. Gestion des autorisations d'accès et privilèges (attribution, délégation, retrait)**	
N° Question	**Libellé de la question**
07A02-01	La procédure d'attribution des autorisations d'accès nécessite-t-elle l'accord formel de la hiérarchie (à un niveau suffisant) ?
07A02-02	Les autorisations sont-elles attribuées nominativement en fonction du seul profil des utilisateurs ?
07A02-03	Le processus d'attribution (ou modification ou retrait) effectif d'autorisations à un individu (directement ou par le biais de profils) est-il strictement contrôlé ? *Un contrôle strict requiert une identification formelle du demandeur (reconnaissance de sa signature, signature électronique, etc.), que la matérialisation des profils attribués aux utilisateurs (par exemple sous forme de tables) soit strictement sécurisée lors de leur transmission et de leur stockage et qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que ces modifications soient journalisées et auditées.*
07A02-04	Y a-t-il un processus de remise à jour systématique de la table des autorisations d'accès lors de départs de personnel interne ou externe à l'entreprise ou de changements de fonctions ?

07A02-05	Y a-t-il un processus strictement contrôlé (voir ci-dessus) permettant de déléguer ses propres autorisations, en tout ou en partie, à une personne de son choix, pour une période déterminée (en cas d'absence) ? *Dans ce cas les autorisations déléguées ne doivent plus être autorisées à la personne qui les a déléguées. Cette dernière doit cependant avoir la possibilité de les reprendre, en annulant ou en suspendant la délégation.*
07A02-06	Peut-on contrôler à tout moment, pour tous les utilisateurs, les habilitations, autorisations et privilèges en cours ?
07A02-07	Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des profils ou des autorisations attribués aux utilisateurs et des procédures de gestion des profils attribués ?

Les questionnaires comprennent à la fois des questions axées sur l'efficacité des mesures de sécurité (par exemple : fréquence des sauvegardes, type de contrôle d'accès physique : lecteur de carte, digicode, etc., existence d'un système de détection d'incendie, etc.), des questions axées sur la robustesse des mesures de sécurité (par exemple : localisation et protection d'accès au lieu de stockage des sauvegardes, existence d'un sas d'entrée ou solidité de la porte, protection du système de détection incendie, etc.) et, généralement, une ou deux questions sur le contrôle ou l'audit des fonctionnalités attendues du service.

Système de pondération des questions

Les questions à se poser au sujet d'un service de sécurité sont relatives à des mesures de sécurité utiles ou nécessaires au service. Or, ces mesures ne jouent pas toutes le même rôle, et les mesures contributives, les mesures majeures ou suffisantes et les mesures indispensables seront à distinguer.

2.4.1 Mesures contributives

Certaines questions ont trait à des mesures qui ont un certain rôle, au sens où elles contribuent à la qualité de service sans, pour autant, que leur mise en œuvre soit indispensable.

En termes quantitatifs, une pondération classique de ces mesures reflète bien cette notion de contribution. Dans ce cas, certaines mesures, plus importantes que d'autres, ont des poids différents. Les bases de connaissances MEHARI indiquent les poids attribués à chaque question.

Le tableau ci-dessous est un extrait d'une des bases MEHARI, dans lequel une colonne est utilisée pour la réponse aux questions (1 pour Oui et 0 pour Non), avant la colonne indiquant le poids de chaque question.

Questionnaire d'audit : Domaine des Systèmes (07)

Service : A. Contrôle d'accès aux systèmes et applications
Sous-service : A02. Gestion des autorisations d'accès et privilèges (attribution, délégation, retrait)

N° Question	Libellé de la question	R-V1	P
07A02-01	La procédure d'attribution des autorisations d'accès nécessite-t-elle l'accord formel de la hiérarchie (à un niveau suffisant) ?	0	4
07A02-02	Les autorisations sont-elles attribuées nominativement en fonction du seul profil des utilisateurs ?	1	2
07A02-03	Le processus d'attribution (ou modification ou retrait) effectif d'autorisations à un individu (directement ou par le biais de profils) est-il strictement contrôlé ? *Un contrôle strict requiert une identification formelle du demandeur (reconnaissance de sa signature, signature électronique, etc.), que la matérialisation des profils attribués aux utilisateurs (par exemple sous forme de tables) soit strictement sécurisée lors de leur transmission et de leur stockage et qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que ces modifications soient journalisées et auditées.*	1	4
07A02-04	Y a-t-il un processus de remise à jour systématique de la table des autorisations d'accès lors de départs de personnel interne ou externe à l'entreprise ou de changements de fonctions ?	0	2
07A02-05	Y a-t-il un processus strictement contrôlé (voir ci-dessus) permettant de déléguer ses propres autorisations, en tout ou en partie, à une personne de son choix, pour une période déterminée (en cas d'absence) ? *Dans ce cas les autorisations déléguées ne doivent plus être autorisées à la personne qui les a déléguées. Cette dernière doit cependant avoir la possibilité de les reprendre, en annulant ou en suspendant la délégation.*	0	4
07A02-06	Peut-on contrôler à tout moment, pour tous les utilisateurs, les habilitations, autorisations et privilèges en cours ?	1	1
07A02-07	Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des profils ou des autorisations attribués aux utilisateurs et des procédures de gestion des profils attribués ?	0	1

La moyenne pondérée est alors un simple cumul des poids des mesures actives (pour lesquelles il a été répondu affirmativement), ramené à la somme des poids possibles et normé sur l'échelle 0 à 4.

Soit en notant R_i la réponse à la question i, P_i le poids de la question i et Mp la moyenne pondérée :

$Mp = 4 \times \Sigma R_i.P_i / \Sigma P_i$

Dans l'exemple de réponses donné dans le tableau ci-dessus la moyenne pondérée serait ainsi :

$Mp = 4 \times 7/18 = 1,6$

et la qualité de service $Q = Mp = 1,6$

2.4.2 Mesures majeures ou « suffisantes »

D'autres mesures peuvent être jugées suffisantes pour atteindre un certain niveau de qualité. Ainsi, l'existence d'un système de détection incendie peut être considérée comme suffisante pour atteindre le niveau 2 pour le sous-service correspondant.

Il a donc été introduit un seuil minimum, qui est le minimum atteint, pour la qualité de service, si une mesure est active.

La colonne "Seuil min" indique que s'il est répondu oui à une question pour laquelle un seuil min a été fixé, alors le sous-service atteint au moins ce palier.

Un deuxième extrait de la même base, avec la colonne Min est présenté ci-dessous :

Questionnaire d'audit : Domaine des Systèmes (07)				
Service : A. Contrôle d'accès aux systèmes et applications **Sous-service : A02. Gestion des autorisations d'accès et privilèges (attribution, délégation, retrait)**				
N° Quest.	**Libellé de la question**	**R-V1**	**P**	**Min**
07A02-01	La procédure d'attribution des autorisations d'accès nécessite-t-elle l'accord formel de la hiérarchie (à un niveau suffisant) ?	0	4	
07A02-02	Les autorisations sont-elles attribuées nominativement en fonction du seul profil des utilisateurs ?	1	2	
07A02-03	Le processus d'attribution (ou modification ou retrait) effectif d'autorisations à un individu (directement ou par le biais de profils) est-il strictement contrôlé ? …	1	4	3
07A02-04	Y a-t-il un processus de remise à jour systématique de la table des autorisations d'accès lors de départs de personnel interne ou externe à l'entreprise ou de changements de fonctions ?	0	2	
07A02-05	Y a-t-il un processus strictement contrôlé (voir ci-dessus) permettant de déléguer ses propres autorisations, en tout ou en partie, à une personne de son choix, pour une période déterminée (en cas d'absence) ? …	0	4	
07A02-06	Peut-on contrôler à tout moment, pour tous les utilisateurs, les habilitations, autorisations et privilèges en cours ?	1	1	
07A02-07	Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des profils ou des autorisations attribués aux utilisateurs et des procédures de gestion des profils attribués ?	0	1	

Dans l'exemple donné, le fait que le processus d'attribution, modification ou retrait de droits (question 3) soit strictement contrôlé a été jugé suffisant pour augmenter la cotation de la qualité du service au palier minimum de 3.

2.4.3 Mesures indispensables

Par contre, d'autres mesures peuvent être jugées indispensables pour atteindre un certain degré de qualité de service. A ces mesures indispensables pour obtenir un certain niveau de qualité, et donc aux questions correspondantes, MEHARI associe donc un seuil de qualité pour aller au-delà duquel la mesure est indispensable.

En d'autres termes, le seuil indiqué dans la colonne "Max" est la limite maximum de niveau de qualité que peut atteindre le sous-service si la mesure n'est pas mise en œuvre.

En cas de conflit entre un seuil min et un seuil max, le seuil max prévaut.

Le tableau précédent devient alors le tableau final suivant :

Questionnaire d'audit : Domaine des Systèmes (07)					
Service : A. Contrôle d'accès aux systèmes et applications **Sous-service : A02. Gestion des autorisations d'accès et privilèges (attribution, délégation, retrait)**					
N° Quest.	**Libellé de la question**	**R-V1**	**P**	**Max**	**Min**
07A02-01	La procédure d'attribution des autorisations d'accès nécessite-t-elle l'accord formel de la hiérarchie (à un niveau suffisant) ?	0	4	2	
07A02-02	Les autorisations sont-elles attribuées nominativement en fonction du seul profil des utilisateurs ?	1	2		
07A02-03	Le processus d'attribution (ou modification ou retrait) effectif d'autorisations à un individu (directement ou par le biais de profils) est-il strictement contrôlé ? …	1	4	2	3
07A02-04	Y a-t-il un processus de remise à jour systématique de la table des autorisations d'accès lors de départs de personnel interne ou externe à l'entreprise ou de changements de fonctions ?	0	2		
07A02-05	Y a-t-il un processus strictement contrôlé (voir ci-dessus) permettant de déléguer ses propres autorisations, en tout ou en partie, à une personne de son choix, pour une période déterminée (en cas d'absence) ? …	0	4		
07A02-06	Peut-on contrôler à tout moment, pour tous les utilisateurs, les habilitations, autorisations et privilèges en cours ?	1	1		
07A02-07	Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des profils ou des autorisations attribués aux utilisateurs et des procédures de gestion des profils attribués ?	0	1	2	

Dans l'exemple ci-dessus, l'opinion d'experts est que les réponses négatives aux questions 1 et 7 font que le niveau de qualité de service ne peut excéder le niveau 2. Cette limitation prévaut sur le niveau 3 évalué précédemment.

Ce triple système de mesure de la qualité de service évite le risque de voir une série de mesures faiblement efficaces surévaluer un niveau de qualité si les mesures essentielles ne sont pas actives ou, au contraire, une série de mesures de poids faible sous-évaluer la qualité de service, alors qu'une mesure essentielle est effectivement en place. Cette approche est une valeur distinctive de MEHARI et s'appuie sur l'expertise des personnes qui tiennent à jour les bases de connaissance.

2.4.4 Questions sans objet

Certaines questions peuvent être « sans objet » pour certaines unités. Dans ce cas, le fait de remplir « X » dans la colonne réponse suffit à faire que la question ne soit pas prise en compte.

Il conviendra de faire très attention cependant à ce qu'une question sans objet doit le rester quelles que soient les évolutions prévisibles du système d'information et des services de sécurité.

3 Processus de diagnostic

Avant de décrire le processus de diagnostic proprement dit, il est nécessaire d'aborder une question préliminaire qui a trait aux services à diagnostiquer. Il peut, en effet, exister plusieurs variantes du même service et il peut être nécessaire d'en tenir compte

3.1 Le schéma d'audit

Les services de sécurité tels que décrits dans MEHARI sont des fonctions de sécurité et ces fonctions sont assurées par des **solutions** effectivement mises en place dans l'entreprise ou l'organisme.

Le diagnostic de l'état de la sécurité consiste, en pratique, à analyser ou auditer les solutions ainsi que les procédures mises en place pour assurer les fonctions de sécurité.

Cependant, il existe généralement, dans la même entreprise, plusieurs solutions pour assurer la même fonction générale.

Par exemple, le contrôle d'accès aux locaux est certainement assuré par des mécanismes différents et avec des solutions différentes pour l'accès aux salles informatiques, l'accès aux baies de répartition des lignes téléphoniques, l'accès aux salles de conférence et l'accès aux salles techniques contenant les gros équipements d'alimentation électrique.

Il est clair également que les fonctions de contrôle d'accès logique aux systèmes et applications sont assurées de manière différente par des systèmes d'exploitation différents, z/OS, UNIX, Windows, etc.

Avant même d'engager le processus d'analyse et d'évaluation des services de sécurité, la première question à poser est celle d'identifier les solutions distinctes à analyser ou auditer.

C'est le but de ce que MEHARI appelle le **« plan d'audit »** ou **« schéma d'audit ».**

3.1.1 Pourquoi un schéma d'audit ?

Dans l'absolu, il faudrait raisonner au niveau de chaque service de sécurité et identifier toutes les solutions différentes qui existent dans l'entreprise ou l'organisme pour assurer chaque service, afin de les auditer une par une.

Cela conduirait à une charge de travail vraisemblablement insupportable pour une précision de résultat en grande partie superflue. Il est donc nécessaire de simplifier et de regrouper les services à analyser en ensembles homogènes.

Pour autant, il n'est généralement pas possible de considérer toutes les solutions implantées dans l'entreprise comme équivalentes. Cela reviendrait à considérer que tous les locaux sont protégés de la même manière, que toutes les parties de l'infrastructure informatique font l'objet de plans de secours équivalents, que toutes les données sont sauvegardées avec le même soin, et ainsi de suite, ce qui est très certainement faux.

Il est bien sûr toujours possible de regrouper des objets différents au sein d'un ensemble considéré comme homogène, mais un principe de précaution, essentiel pour un diagnostic de sécurité, devrait alors faire retenir pour tous les éléments de l'ensemble l'évaluation la plus pessimiste, ce qui risque alors de donner une image très négative de l'ensemble.

Il est donc nécessaire de trouver un compromis et de distinguer des domaines de solutions à auditer séparément et à l'intérieur desquels les solutions de sécurité seront considérées comme homogènes. La définition de ces domaines est traduite par le « schéma d'audit ».

3.1.2 Élaboration du schéma d'audit

L'approche de MEHARI est de considérer que les services de sécurité sont définis et mis en œuvre par des équipes en nombre limité, ayant une politique de sécurité, explicitement exprimée ou non, qui leur fera prendre des décisions homogènes et cohérentes, même en présence de contraintes techniques imposant des solutions de détail différentes.

Partant de ce principe, la démarche de MEHARI est de :

- Distinguer des domaines de responsabilité pour lesquels il est possible de définir des **responsables de domaine ayant une politique de sécurité cohérente**
- Analyser, à l'intérieur de ces domaines, s'il existe des responsables différents pouvant avoir des politiques différentes et de distinguer alors des sous-domaines de responsabilités (par exemple des responsables de sites différents pouvant avoir, pour la sécurité de leur site, des politiques différentes)
- Analyser dans chaque domaine ou sous-domaine les **sous-ensembles pouvant faire l'objet d'une politique différenciée, pour des raisons techniques ou pour toute autre raison**

3.1.3 Les domaines de responsabilités de MEHARI

MEHARI a défini des domaines de responsabilité, qui ont été cités au paragraphe 2.3 plus haut.

Le schéma d'audit devant finir par se traduire par des audits spécifiques associés à chaque domaine, les questionnaires d'audit de MEHARI sont eux-mêmes découpés selon cette organisation et c'est pour cette seule raison qu'ils ont été organisés comme ils le sont.

Le premier niveau de structuration du schéma d'audit est donc fait selon cette décomposition, puis l'auditeur doit déterminer, pour chaque domaine à couvrir, combien de variantes devraient être définies :

- Combien d'organisations différentes méritent d'être auditées séparément pour les fonctions de sécurité dépendant des organisations ?
- Combien de responsables de sites peuvent avoir une politique de sécurité propre, nécessitant de faire des diagnostics séparés ?
- Combien de responsables de locaux peuvent avoir une politique de sécurité propre, nécessitant de faire des diagnostics séparés ?
- Y a-t-il plusieurs responsables de réseaux locaux à interroger séparément ?
- Etc.

Chaque fois que la réponse à ces questions ira dans le sens d'une distinction nécessaire pour des raisons d'autonomie ou de politiques pouvant ne pas être cohérentes, le domaine sera éclaté en « variantes », ce qui se traduit par des réponses différenciées qui seront reportées dans des colonnes différentes (R-V1 à R-V4)[1] dans le questionnaire du domaine concerné.

Un exemple de schéma d'audit est donné ci-dessous.

Domaine	**Variantes**
Organisation	L'entreprise
Locaux	Les salles informatiques Les locaux techniques Les zones de bureaux
Infrastructure informatique	Systèmes et réseau du siège Systèmes et réseaux des sites de production

[1] Les bases de connaissances standard contiennent 4 colonnes correspondant à 4 possibilités de variantes ce qui est très généralement suffisant, mais il est bien sûr possible de définir plus de 4 variantes

Domaine	Variantes
L'administration de l'infrastructure informatique	L'administration de l'infrastructure du siège L'administration de l'infrastructure des sites de production
Les développements informatiques	Les développements faits par la Direction Informatique Les développements faits par les utilisateurs
Les postes de travail utilisateurs	Les postes Windows Les appareils mobiles personnels (BYOD)

Un tel schéma d'audit permet de définir dans le détail, l'organisation du diagnostic de sécurité, en prévoyant de faire un diagnostic spécifique pour chaque variante identifiée.

3.2 Le processus de diagnostic

3.2.1 Le processus de diagnostic proprement dit

Puisque les questionnaires d'audit des services de sécurité sont précisément organisés en fonction des domaines de responsabilité, il suffira, une fois défini le schéma d'audit, de collecter les réponses correspondant à chaque variante auprès de la personne ou du groupe de personnes le mieux placé pour cela.

Il peut arriver que certains sous-services apparaissent, lors de l'audit, sans objet pour l'entité concernée. Il convient alors de les supprimer des questionnaires et d'en documenter la raison.

Par ailleurs, en ce qui concerne l'usage des questionnaires, les réponses par oui ou par non peuvent, dans certains cas, poser des difficultés, les réponses naturelles pouvant être :

- "Oui en général mais avec des exceptions"
- "Oui en théorie, mais, en pratique, ce n'est pas certain ou pas appliqué partout"
- "Oui partiellement, à X %"
- "Oui, en cours de déploiement"
- "Oui, c'est prévu mais non encore appliqué"
- etc.

Les recommandations suivantes peuvent être faites :

- Il faut impérativement noter les explications accompagnant les réponses et en garder la trace. C'est ainsi que dans les questionnaires papiers qui servent de support aux réunions d'audit, il importe de garder une colonne "Commentaires" dans laquelle la réponse précise sera notée.
- La cotation demandant une réponse "oui" ou "non", il faut prendre un parti. La position "sécuritaire" consisterait à répondre "non" à toutes les questions précédentes pour que les décisions qui découleront de l'audit n'occultent pas l'imperfection constatée.
- Il faut être conscient, néanmoins, que cela peut démotiver les utilisateurs et décrédibiliser l'audit si trop d'insistance est mise sur un point mineur en cours de correction et maîtrisé.
- La solution raisonnable semble ainsi être de répondre "Oui" chaque fois que le processus de correction et de réaction aux manquements ou de déploiement est sous contrôle et maîtrisé et de répondre "Non" dans le cas contraire.

A noter que pour que de telles réponses puissent être saisies, il est absolument nécessaire que l'audit ait lieu lors d'une rencontre entre l'auditeur et le responsable du domaine audité et que les questionnaires soient remplis lors de cette réunion. Les questionnaires remplis par la personne auditée en

dehors de la présence de l'auditeur masquent totalement cet aspect des réponses et peuvent introduire des biais sérieux dans la qualité de l'audit.

3.2.2 Cotations et corrections des cotations

Pour les cotations obtenues par questionnaires, une fois ceux-ci remplis, la cotation des services de sécurité peut être entreprise, selon ce qui a été expliqué plus haut, en fonction du système de pondération proposé par MEHARI.

Le système de pondération a été mis au point par les experts du CLUSIF, mais il se peut toujours qu'il fasse apparaître des imperfections locales. Il ne saurait, en effet, tenir compte de tous les contextes particuliers qui peuvent être rencontrés dans un audit, ni être parfaitement adapté à toutes les organisations.

L'auditeur devra donc, avant de tirer ses conclusions et d'établir une synthèse de l'audit, vérifier qu'il est d'accord avec la cotation retenue pour chaque service et sous-service de sécurité, en se référant aux définitions du niveau de qualité atteint.

De ce point de vue, l'auditeur doit obligatoirement être un professionnel de la sécurité expérimenté.

4 Livrables

Les résultats bruts sont constitués des questionnaires remplis, avec les commentaires comme expliqué plus haut.

4.1 La synthèse par services de sécurité

La synthèse de la qualité des services de sécurité se trouve dans la feuille « Services » de chaque base de connaissances.

Au cas où des variantes ont été définies, le résultat qui apparait dans cette présentation est le minimum des variantes.

A partir de là, le diagnostic final peut être présenté sous diverses formes de graphique : ces présentations sont laissées à l'initiative des utilisateurs.

4.2 Fournitures d'indicateurs relatifs à la norme ISO/IEC 27002:2013

Ainsi qu'il a été indiqué dans le document « *MEHARI Principes fondamentaux et spécifications fonctionnelles* », le diagnostic de sécurité peut servir également à exprimer le niveau de maturité de l'organisation considérée vis à vis des bonnes pratiques de la norme ISO/IEC 27002:2013.

En effet, chaque question de l'audit MEHARI peut être vue comme un point de contrôle élémentaire destiné à vérifier les solutions et les processus de sécurité mis en œuvre par l'entité.

Comme l'organisation de l'audit MEHARI permet d'obtenir, auprès de chaque responsable opérationnel concerné, la capacité de l'entité à réduire les risques, la structure des services ne se plie pas directement à la structure « descriptive » de la norme.

De plus, les questionnaires de MEHARI comportent plusieurs services et contrôles allant au-delà des recommandations de la norme, il a été nécessaire de réaliser une extraction et un transcodage parmi les questions de l'audit MEHARI vers les pratiques de la norme ISO.

Les questionnaires d'audit de MEHARI permettent ce transcodage et une table de correspondance (avec les formules nécessaires) est fournie dans les bases de connaissances.

Ainsi, il est possible de visualiser le niveau de maturité de l'entité (avec un score de 0 à 10, par exemple) pour chaque point de contrôle de la norme. Il ne s'agit pas de l'objectif primaire de MEHARI mais cela peut constituer une information utile lors d'un processus de certification ou d'une comparaison entre plusieurs organisations.

5 Conseils pratiques

5.1 Points importants dans l'élaboration du schéma d'audit

Le schéma d'audit apparaît parfois comme quelque chose de compliqué. Pourtant, ce n'est rien d'autre que la prise en compte de solutions différentes ou de contextes différents.

Un système d'exploitation de gros ordinateur (z/OS par exemple) est différent d'un système Unix et les solutions de sécurité, comme les procédures d'exploitation, sont différentes par essence. Il peut alors être décidé de prendre en compte ces différences ou non. S'il est décidé de les prendre en compte, il faudra dupliquer les questionnaires et poser plusieurs fois la même question. Dans le cas contraire, il n'y a rien à faire et chaque question ne sera posée qu'une fois. ***Mais ceci est totalement indépendant de la méthode d'audit.***

Le schéma d'audit n'est qu'un moyen simple permettant de différencier, dans le processus d'audit, des domaines de solutions différents.

La distinction des domaines de solutions est donc une question de choix. Une bonne manière globale de prendre le problème est sans doute de se demander combien d'interlocuteurs différents devraient être rencontrés, pour le même domaine.

Au fond, la problématique à laquelle il faut répondre est la suivante : « dans chaque domaine de responsabilité, combien d'interlocuteurs pouvant avoir des réponses sensiblement différentes, devrait-on rencontrer ? ». On admettra, en corollaire de cette prise de position, que si deux interlocuteurs doivent avoir des réponses sensiblement identiques, il est inutile de les rencontrer séparément.

5.2 Points importants dans le processus d'audit

Comme nous l'avons déjà précisé, il est important que les questionnaires soient remplis en présence de l'auditeur, pour que tous les attendus ou commentaires puissent être pris en compte et notés.

Par ailleurs, et nous l'avons déjà évoqué, si les réponses ne sont pas totalement « oui » ou « non », il vaut mieux prendre en compte pour la pondération et l'évaluation des services, une approche sécuritaire (généralement en répondant non) quitte à reporter, dans les commentaires que la réponse était partiellement affirmative.

Les bases de connaissances de MEHARI, et, en particulier les questionnaires d'audit, ont été bâties en adoptant un principe de précaution qui est le suivant :

Les automatismes de la méthode ne doivent jamais conduire à sous-évaluer un risque. Il est toujours préférable qu'un risque soit surévalué au départ quitte à être revu à la baisse lors d'une analyse détaillée plutôt que sous-évalué et non sélectionné pour une analyse plus fine.

C'est un principe de précaution qui consiste à prendre les mesures nécessaires pour éviter que les automatismes de calcul ne considèrent un scénario de risque comme peu grave et l'éliminent d'une sélection, alors qu'il est d'un niveau de gravité élevé. Il peut y avoir plusieurs raisons qui fassent que les automatismes sous-évaluent la gravité d'un scénario … dont la surévaluation de la qualité des services de sécurité.

De par le principe exposé ci-dessus, les résultats de l'audit de sécurité pouvant être utilisés pour une analyse des risques encourus par l'entreprise, la cotation des services de sécurité est « prudente ».

Les résultats chiffrés des évaluations peuvent donc apparaître comme sévères, si une comparaison est faite avec les résultats d'autres méthodes d'audit. Le lecteur devra alors avoir à l'esprit que MEHARI est exigeant en termes de robustesse des services et de mise sous contrôle, et que la note finale tient compte d'une « assurance sécurité », ce qui n'est pas souvent le cas des autres méthodes ou questionnaires.

Téléchargez les bases de connaissances et la documentation de Méhari sur

www.meharipedia.org