METHODES

MEHARI 2010

Guide de développement d'une base de connaissances d'analyse de risque MEHARI

Mars 2012

Espace Méthodes

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11, rue de Mogador – 75009 PARIS
Tel : 01 53 25 08 80 – Fax : 01 53 08 81
clusif@clusif.asso.fr - http://www.clusif.asso.fr

Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

Jean-Philippe **JOUAS**

Les contributeurs

Dominique	**BUC**	BUC SA
Olivier	**CORBIER**	Docapost
Martine	**GAGNE**	HydroQuébec
Chantale	**PINEAULT**	AGRM
Jean-Louis	**ROULE**	
Claude	**TAILLON**	Ministère de l'Éducation, du Loisir et du Sport du Québec
Marc	**TOUBOUL**	BULL SA
Annabelle	**TRAVERS-VIAUD**	BULL SA

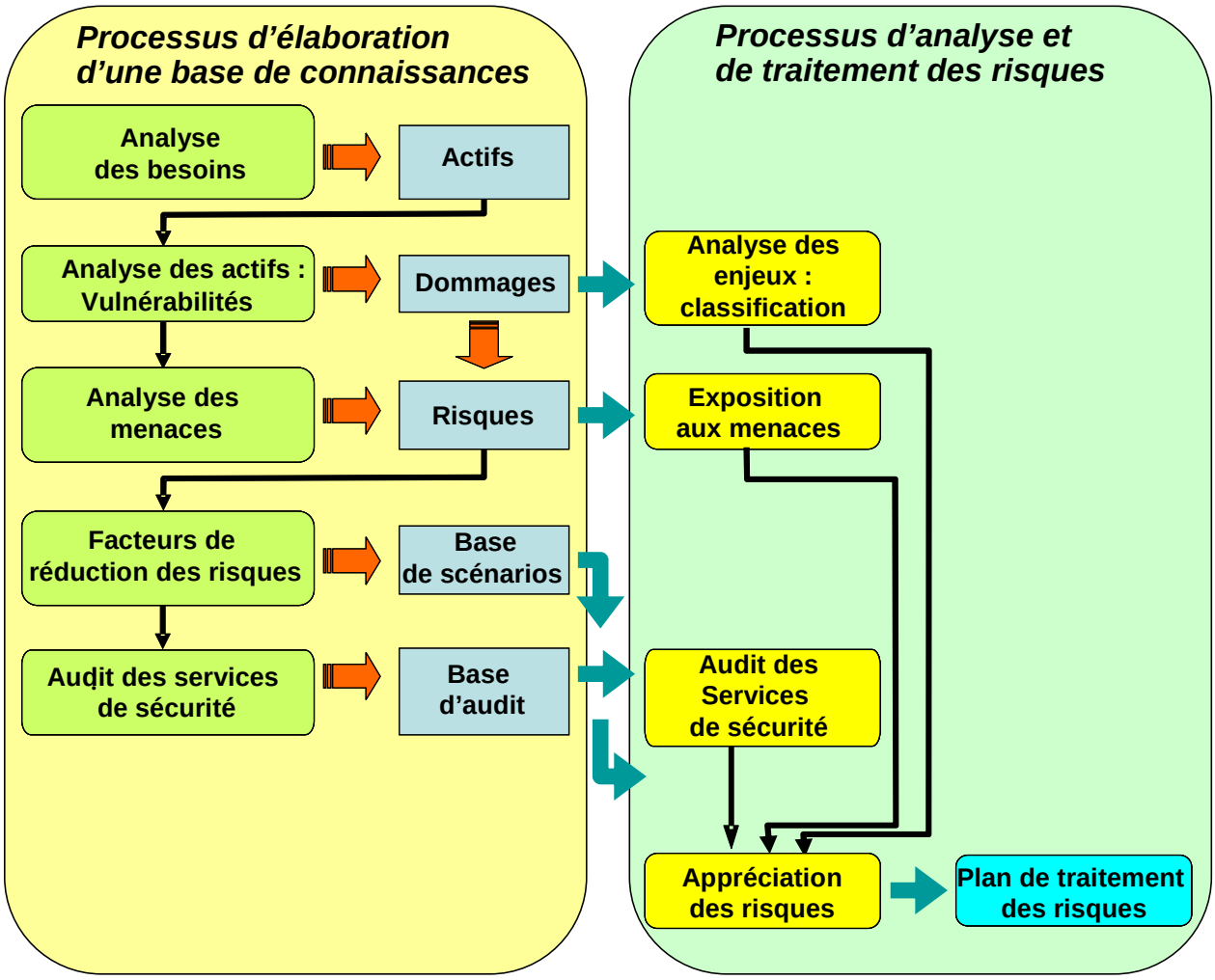
Ainsi que les membres du comité de relecture.

Sommaire

Introduction

Les principes fondamentaux d'une méthode d'analyse et de traitement des risques et ses spécifications fonctionnelles ont été développés dans un document du Clusif relatif à la méthode MEHARI (« MEHARI 2010 - Principes fondamentaux et spécifications fonctionnelles ») et ce document met en avant la nécessité d'une base de connaissances en support de la méthode.

Le schéma général qui ressort des principes de traitement est repris ci-dessous.



Ce schéma met en évidence que le processus d'identification, d'analyse et de traitement des risques comprend une série de phases qui peuvent être réalisées au profit d'entités diverses et partagées sous la forme d'une base de connaissances.

C'est sur ce principe qu'a été développée la base de connaissances de MEHARI, et, particulièrement, la base MEHARI 2010.

Ceci étant, d'autres bases peuvent être développées pour être adaptées à des environnements ou des contextes particuliers tel que le traitement de risques liés à des informatiques de conduite de processus industriels (conduite d'opérations industrielles, surveillances de processus dangereux, etc.), à des entreprises présentant des particularités telles que des PME, voire des TPE (très petites entreprises), à des secteurs d'activités spécifiques ou à des technologies opérationnelles comme les SCADA (Supervisory Control And Data Acquisition).

1. Objectif de ce document

Ce document est établi à l'usage des organisations qui souhaitent développer de nouvelles bases de connaissances ou adapter les bases du Clusif à des contextes ou environnements particuliers.

Les raisons d'un tel développement ou d'une telle adaptation peuvent être nombreuses. Citons, par exemple, l'utilisation de la méthode pour l'analyse et la gestion d'autres risques que ceux liés au système d'information, son utilisation pour des systèmes informatiques spécifiques tels que la conduite de processus industriels, l'existence de menaces particulières, etc.

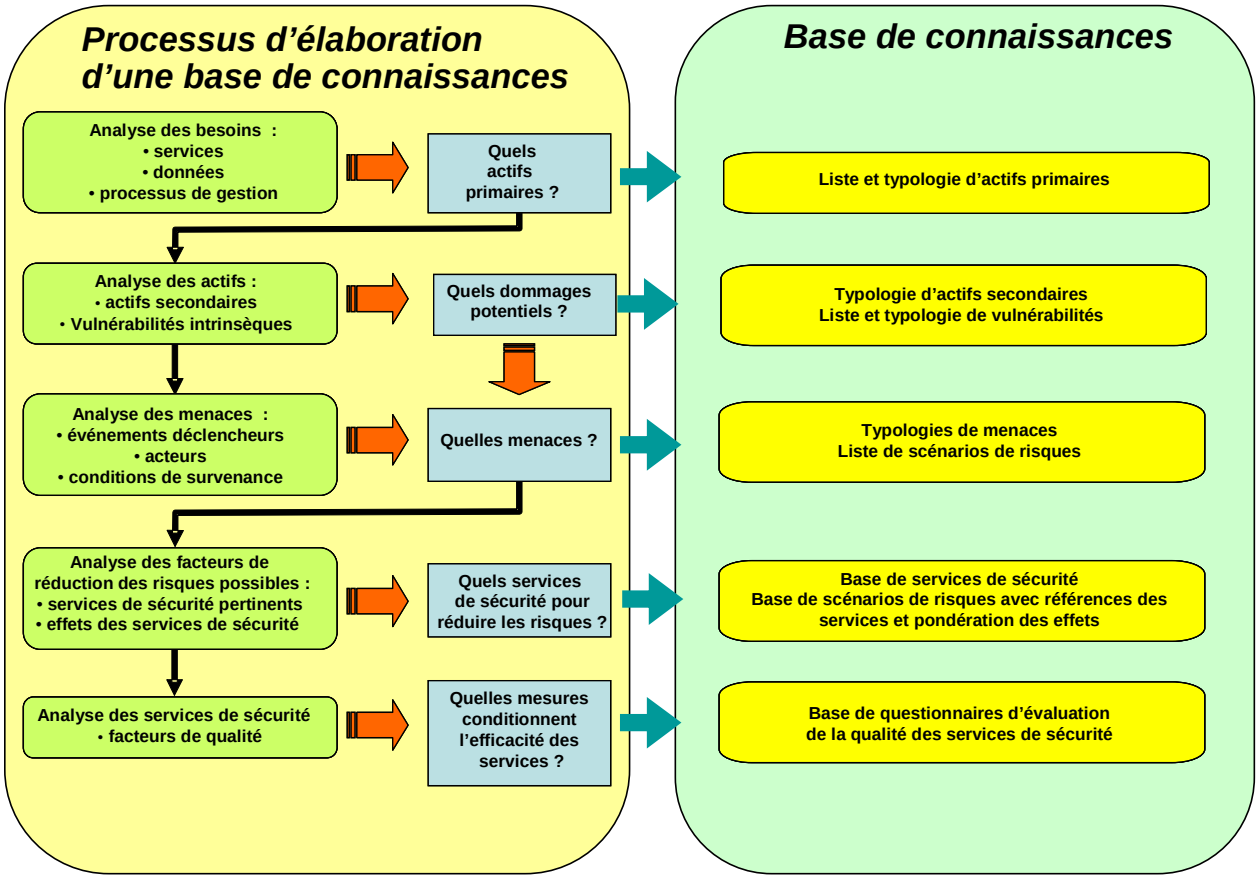
A qui s'adresse ce document ?

Le développement d'une base de connaissance Méhari, qui est le sujet de ce document, ne peut être abordé sans une très solide connaissance de la méthode. Ce document s'adresse à des experts de la méthode ou, à tout le moins, à des utilisateurs très confirmés.

Une très bonne connaissance des principes de la méthode ainsi que de l'utilisation de la base de connaissance fournie par le CLUSIF est supposée acquise.

Plan du document

Le plan d'ensemble et les différents aspects abordés sont représentés schématiquement ci-dessous.



Nous aborderons donc successivement :

- Quels actifs ?
- Quelles vulnérabilités ?
- Quelles menaces ?
- Quels scénarios ?
- Quels services de sécurité ?
- L'évaluation de la qualité des services de sécurité et l'élaboration des questionnaires de diagnostic
- L'élaboration de la base de connaissance des scénarios
- La finalisation de la base de connaissance globale

2. Principes fondamentaux

Deux principes fondamentaux doivent être rappelés en priorité avant tout développement d'une base de connaissance.

Principe de précaution

Mehari est essentiellement une méthode de gestion de la sécurité par l'analyse des risques, même si, au sein de MEHARI, certains modules peuvent être utilisés dans d'autres buts que l'analyse de risque. Il s'ensuit que l'objectif fondamental de l'ensemble des modules ou versions de MEHARI est de gérer les risques les plus importants.

Le principe de précaution qui en découle est le suivant :

Principe n° 1

Les automatismes ou aides contenus dans les bases de connaissance 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 des 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 :

- L'appel abusif, dans les formules des scénarios, à des services de sécurité qui, en fait, ne jouent qu'un rôle marginal pour le scénario.
- La surévaluation de la qualité des services de sécurité, en général ou plus particulièrement pour un scénario donné.
- Des grilles de décision mal conçues, mal validées ou inadaptées au contexte

Principe de justification

A contrario, une méthode qui surévaluerait systématiquement le niveau de gravité des scénarios de risque et dont le résultat ne saurait être expliqué, voire justifié, serait d'une utilité bien faible.

Il découle de cette nécessité que les automatismes de la méthode doivent produire, dans la majorité des cas, une évaluation explicable et justifiable du niveau de risque.

En ce qui concerne **l'impact**, la base de l'évaluation est la classification des ressources touchées par le scénario et c'est donc un élément raisonné et évalué très rigoureusement et en connaissance de cause, par les utilisateurs eux-mêmes. Partant de là, il faut et il suffit que tous les éléments de réduction d'impact soient pris en compte, sous réserve que l'on puisse garantir leur efficacité dans la situation considérée (principe de précaution).

En ce qui concerne **la potentialité**, il y a un risque de la surévaluer, en particulier en l'absence de services efficaces, et de décréter un scénario de risque comme très probable alors que chacun sait, en particulier les utilisateurs, que ce risque ne s'est jamais ou que très rarement concrétisé.

Le principe de justification qui découle de ce constat est le suivant :

Principe n° 2

Les automatismes de la méthode doivent, dans tous les cas, permettre d'expliquer et de justifier les résultats obtenus

Ces deux principes servent de fil directeur dans les chapitres suivants.

3. Définir la typologie des actifs

Introduction

Nous rappelons, ci-dessous, ce qui a été dit des actifs dans le document « Principes fondamentaux et spécifications fonctionnelles de MEHARI ».

Les actifs sont le sujet principal du risque : ce sont eux qui vont subir un dommage et le risque naît bien du fait qu'une certaine forme d'actif est susceptible de subir un dommage.

Il est bien clair, dès lors, que les conséquences et que la gravité de la survenance du risque dépendent de la nature de ces actifs et donc que cette nature (voir ci-dessous) doit faire partie de la caractérisation du risque.

Mode de description des actifs

a. Les actifs primaires

La description des actifs devant servir à évaluer les conséquences des risques auxquels ils sont exposés, les éléments clés doivent se référer aux **besoins** des organisations que l'on peut, dans un premier temps, classer dans trois catégories :

- Les services (fonctionnels),
- Les données,
- Les processus de management.

Cette décomposition parait la plus apte à mettre en évidence les besoins essentiels d'une organisation dont le fonctionnement est essentiellement basé sur la réalisation de services qui, eux-mêmes ont besoin de données et tout ceci tout en respectant un ensemble de règles, écrites ou non, concrétisées par des processus de management.

Cette décomposition, née de l'expérience, est fortement recommandée mais ne saurait constituer une contrainte.

Dans chaque catégorie, des types d'actifs primaires peuvent être distingués, en fonction :

- De la nature des besoins,
- De la nature des prestataires de service.

Et éventuellement :

- Du domaine d'activité et de domaines de responsabilité différents,
- De la technologie employée,
- Des utilisateurs concernés.

Ces typologies doivent correspondre à des types de besoins et être décrites au niveau fonctionnel.

Remarque : Les actifs primaires correspondent aux besoins des organisations et c'est donc à ce niveau qu'il conviendra d'évaluer l'importance de ce besoin, importance dont il sera tenu compte pour juger du niveau de risque, par l'intermédiaire d'une classification des actifs (représentée dans la base de connaissances par le « tableau d'impact intrinsèque »).

b. Les actifs secondaires ou actifs de support

Les actifs ont des vulnérabilités et ce sont elles dont l'exploitation conduit au risque.

Pour rechercher ces vulnérabilités, il est essentiel de distinguer, pour chaque actif primaire :

- les diverses formes qu'il peut revêtir,
- les diverses contingences dont il peut dépendre.

Ces formes et contingences peuvent être regroupées sous l'appellation **d'actifs secondaires** ou **d'actifs de support**.

Autant les actifs primaires correspondent à des besoins fonctionnels, autant les actifs secondaires correspondent à un niveau matériel et concret et aux moyens nécessaires à la réalisation des besoins fonctionnels.

Paramètres clés pour la définition des typologies d'actifs

Il ressort des définitions et considérations ci-dessus qu'un point essentiel dans le développement d'une base de connaissances réside dans la définition des types d'actifs primaires que l'on souhaite distinguer et dans l'expression des actifs secondaires et des vulnérabilités associées.

Typologies d'actifs primaires

En ce qui concerne les actifs primaires, le choix principal réside dans le degré de détail avec lequel on souhaite les préciser ou les distinguer.

A titre d'exemple, on peut se contenter de considérer les services informatiques, au sens large, ou souhaiter distinguer les services applicatifs, les services bureautiques, les services systèmes communs, etc. De même on peut se contenter de considérer les données informatiques ou distinguer les données applicatives, les données bureautiques, les archives informatiques, etc.

La question est alors : « quelles sont les raisons qui pourraient inciter à distinguer des types d'actifs primaires les uns des autres ou au contraire les regrouper dans une même catégorie ? ».

Les raisons possibles sont les suivantes :

- Distinguer des actifs pouvant avoir des sensibilités notablement différentes (et donc conduire à des scénarios de risque de gravités différentes).
- Distinguer des actifs primaires ayant des actifs secondaires différents (en fonction de formes possibles de ces actifs ou de contingences possibles), donc des vulnérabilités différentes et conduisant à des scénarios différents.
- Distinguer des actifs protégés par des services de sécurité différents.

Nous allons revenir sur chacun de ces points.

Distinguer des actifs de sensibilités différentes

Cela peut sembler une bonne idée que de distinguer des actifs primaires ayant des sensibilités notablement différentes. C'est pour traiter ce point d'ailleurs qu'avait été introduite la décomposition cartographique en 2007.

Cela permet, il est vrai, d'avoir des scénarios bien représentatifs de types d'activité et donc bien adaptés à une communication dédiée par secteur d'activité.

Il reste que cela revient à créer des variantes de scénarios ne différant que par le degré de sensibilité des actifs et que cela va créer une surcharge de travail au niveau de l'analyse des scénarios, charge qui aurait pu être reportée au niveau du déploiement des mesures de sécurité, ce qui est sans doute plus efficace. En effet, c'est au niveau du déploiement que l'on pourra faire des

choix économiques valables en choisissant de ne déployer les mesures décidées que pour les actifs les plus sensibles ou, au contraire, de généraliser ces mesures.

Distinguer des actifs en fonction de leur sensibilité est ainsi, peut-être, un choix de communication, mais n'est pas une nécessité pour l'analyse des risques. Dans l'optique d'une simplification des tâches d'analyse de risques, cette option ne devrait pas être retenue.

Distinguer des actifs primaires ayant des actifs secondaires différents

Les données bureautiques, par exemple, peuvent être matérialisées sous des formes (actifs secondaires) différentes des données applicatives (PDA, clés USB, etc. pour les données bureautiques, disques ou bandes pour les données applicatives).

Distinguer des actifs primaires ayant des actifs secondaires différents permettra effectivement d'être plus précis dans la description des actifs secondaires, donc dans la description de leurs vulnérabilités et donc dans l'identification et la description des risques

La contrepartie qu'il est bon d'avoir en tête est que cela n'a d'intérêt que si l'on est capable de mettre en face de ces vulnérabilités spécifiques des services de sécurité adaptés.

On notera ainsi, à ce stade, que la multiplication des actifs primaires et secondaires peut conduire à une multiplication des services de sécurité[1].

Distinguer des actifs primaires ayant des actifs secondaires et donc des vulnérabilités différents permet de mieux mettre en lumière des scénarios de risques différenciés mais nécessite, en contrepartie, de créer des services de sécurité eux-mêmes différenciés.

Distinguer des actifs primaires protégés par des services de sécurité différents

Si les services de sécurité sont déjà définis, parce que la base de connaissance des services existe et que l'on ne souhaite pas en changer, pour des raisons de cohérence des diagnostics ou pour toute autre raison, la question se pose de savoir si la définition et la typologie des actifs doivent être alignées sur la typologie des services de sécurité (si on a défini des services de sécurité spécifiques pour le réseau étendu intersites et pour le réseau local, faut-il distinguer le service du réseau étendu de celui du réseau local ?).

Cela est certainement plus cohérent, mais ce n'est pas obligatoire.

En effet, les formules qui serviront à apprécier les scénarios de risque sont telles qu'il est toujours possible d'évaluer simultanément plusieurs alternatives ou variantes en ne retenant au final, pour le calcul, que le résultat le plus pessimiste. Par exemple pour un scénario d'indisponibilité de réseau, si on sépare en tant qu'actifs le réseau étendu et le réseau local, on évaluera distinctement les scénarios d'indisponibilité pour chaque type de réseau, chacun avec ses services spécifiques, mais dans le cas où ces actifs sont confondus il faudra prendre soin d'évaluer chaque facteur de réduction de risque pour chaque type de réseau et on prendra systématiquement le minimum de chaque facteur.

Si on considère un scénario d'indisponibilité de réseau dû à un incendie :

---

[1] Par exemple, le fait de distinguer les fichiers courants des fichiers d'archive conduira à définir des services de sécurité différents pour la protection des documents courants et la protection des archives. De même le fait de distinguer les réseaux locaux des réseaux étendus conduit à différencier les services de sécurité correspondants.

- dans le cas où les types d'actifs sont distincts on évaluera 2 scénarios : un scénario d'indisponibilité du réseau étendu dû à un incendie et un scénario d'indisponibilité du réseau local dû à un incendie et, pour les mesures palliatives, on considèrera, pour le premier, le PRA du réseau étendu et pour le second le PRA du réseau local.
- Dans le cas ou les deux types de réseau sont considérés comme un seul type d'actif, on n'évaluera qu'un scénario : indisponibilité du réseau dû à un incendie et on considèrera, au titre des mesures palliatives, le minimum entre le PRA du réseau étendu et celui du réseau local.

Les calculs seront donc possibles que l'on ait distingué les types de réseau ou non.

Par contre, il peut y avoir une difficulté ou un jugement trop pessimiste si les types d'actifs se révèlent avoir des sensibilités différentes. Si le type d'actif le moins sensible a des services de sécurité d'un niveau de qualité moindre que le type d'actif le plus sensible, cela peut conduire, en regroupant les types d'actifs, à un jugement plus sévère que la stricte réalité, parce que l'on retiendra le niveau le plus bas de service avec le niveau le plus haut de sensibilité.

Distinguer des actifs protégés par des services de sécurité différents produira un jugement sur la gravité des scénarios plus précis et, dans certains cas, moins pessimiste, mais cette distinction n'est pas indispensable à une évaluation des risques.

En résumé, plus la typologie des actifs primaires sera fine, plus on pourra être précis et exhaustif dans l'identification et l'appréciation des risques, avec comme corollaire qu'il faudra distinguer davantage de services de sécurité, en cohérence avec la typologie des actifs.

Plus les services de sécurité seront détaillés, plus il sera souhaitable, pour une appréciation des risques, de détailler les actifs en conséquence, mais sans que cela soit indispensable[2].

Typologie d'actifs secondaires

Indépendamment des considérations précédentes relatives à la finesse de définition des types d'actifs primaires, il convient ensuite de définir les actifs secondaires qui seront à l'origine de vulnérabilités. En effet, autant les actifs primaires correspondent à des besoins fonctionnels, autant les actifs secondaires consistent en des objets concrets utilisés par les processus pour réaliser les services demandés.

Il n'y a pas de démarche imposée pour rechercher les actifs secondaires pertinents pour chaque actif primaire, mais on peut faire les recommandations suivantes, en fonction du type général d'actif primaire :

Pour les actifs de type « services (fonctionnels) » :

Distinguer :

- Les équipements nécessaires à la réalisation du service.
- Les moyens de servitude éventuellement nécessaires à ces équipements (électricité, fluides, etc.).

[2] La distinction d'actifs différenciés apportera une plus grande précision dans l'analyse de risques (en particulier dans l'évaluation des impacts, au prix d'un surcroît de travail lors de l'analyse des risques.

- Les éléments immatériels ayant une influence directe sur le déroulement des processus supports du service (logiciel, automatisme, paramétrage de processus, procédures, etc.).
- Les éléments matériels supports des éléments immatériels décrits ci-dessus.
- Les éléments logistiques nécessaires aux opérations effectuées par du personnel (locaux, climatisation, restauration, transport, etc.).
- Le personnel interne chargé d'assurer les services.
- Les services extérieurs nécessaires et non distingués au niveau des actifs primaires.

Pour les actifs de type « données » :

Distinguer :

- Les entités logiques rassemblant les données (fichiers, bases de données, répertoire, etc.).
- Les données isolées.
- Les données transitoires (messages, contenus d'écrans, etc.).
- Les supports matériels des entités ci-dessus (media magnétiques ou optiques, supports papiers, etc.).

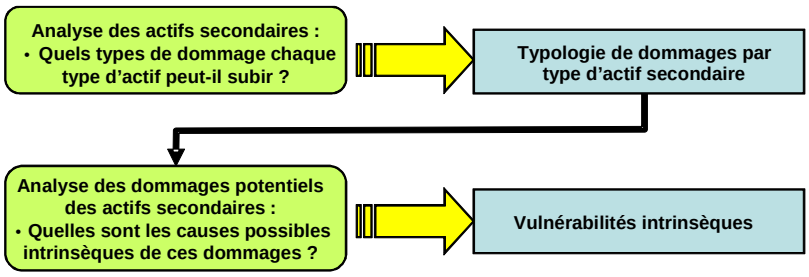
Pour les actifs de type « processus de management » :

- Pour ces actifs, il n'y a pas, à proprement parler, d'actifs secondaires à distinguer. Par contre ils seront précisés en fonction des domaines de préoccupation possibles (protection de la vie privée, normes comptables, exigences contractuelles, etc.).

4. Définir la typologie des vulnérabilités

Les vulnérabilités qu'il convient de rechercher sont les « vulnérabilités intrinsèques » des actifs secondaires.

La démarche recommandée pour rechercher les vulnérabilités intrinsèques pertinentes pour chaque actif secondaire ressemble beaucoup à celle employée dans l'analyse des modes de défaillance et consiste à systématiser une recherche correspondant au diagramme ci-dessous :



Ainsi, on doit rechercher, pour les trois critères de base, Disponibilité, Intégrité et Confidentialité, quels sont les types de dommages possibles, ce qui permettra in fine de définir la typologie des vulnérabilités intrinsèques.

Cette recherche peut se faire avec un degré de détails plus ou moins grand et dépend de la finesse de description des actifs secondaires.

Il faut noter, en effet, qu'il y a souvent des possibilités de transfert entre types d'actifs secondaires et types de vulnérabilités. On peut, par exemple, pour une configuration logicielle définie comme actif secondaire, mettre en évidence, comme vulnérabilité, l'inopérabilité due à une absence de licence, mais on peut aussi détailler davantage en définissant comme actif secondaire la licence nécessaire au fonctionnement de la configuration logicielle et comme vulnérabilité de cette licence son effacement, sa disparition, etc. Dans un autre domaine, on peut considérer, comme vulnérabilité d'un serveur, qu'il dépend de la mise à disposition d'énergie par des organes de servitude ou, au contraire, définir les moyens de servitude comme actifs secondaires et rechercher les vulnérabilités détaillées de ces moyens.

Il faut noter que le degré de finesse avec lequel le tableau des vulnérabilités types est décrit est un facteur clé, au même titre que la finesse de description des actifs, facteur qui influe directement sur la précision, et corrélativement sur la charge, de l'analyse de risques.

Pour établir ce tableau, il est recommandé de commencer par établir un tableau d'analyse préliminaire décrivant par grand type d'actif secondaire (sans détail à ce niveau d'analyse) et par type de conséquence (DIC) les types de dommages possibles avant de remplir le tableau des vulnérabilités intrinsèques.

Nous donnons ci-dessous, deux tableaux ainsi élaborés, à titre d'exemple :

- Un premier tableau d'analyse ne considérant que les aspects matériels, immatériels ou de services et cherchant à mettre en évidence les types de dommages possibles.
- Un deuxième tableau construit à partir d'une typologie d'actifs secondaires et reprenant les résultats du tableau d'analyse précédent

Tableau d'analyse préliminaire des dommages (exemple) :

Tableau d'analyse préliminaire des dommages			
Type d'actif secondaire	***Type de conséquence***	***Type de dommage***	***Commentaire***
Élément matériel : Équipement fonctionnel, câblage, dispositifs de sécurité, etc. Media matériel support de logiciel, d'automatisme, de paramètres de processus ou de données	Indisponibilité	Endommagement physique	L'élément est bien là, mais a été endommagé ou détruit
		Inopérabilité	L'élément est bien là, mais on ne peut y accéder ou le faire fonctionner (absence de clé d'accès ou de démarrage, de personnel qualifié, d'équipement de lecture pour un media, etc.)
		Inexploitabilité	Les résultats ou actions de l'élément ou de sa mise en œuvre ne sont pas conformes ou totalement absents (panne, blocage, résultats visiblement altérés, etc.)
		Disparition	L'élément n'est plus là
	Défaut d'intégrité	Altération de l'élément	L'élément a été modifié (accidentellement ou volontairement)
		Échange de l'élément	L'élément matériel a été échangé avec un autre qui a été modifié
	Divulgation	Duplication de l'élément	L'élément a été dupliqué
		Acquisition par un tiers de l'élément	L'élément matériel a été acquis par un tiers (vol, perte, envoi)
Élément immatériel : Logiciel, automatisme, paramétrage de processus, procédure, etc. Données (fichiers constitués, données fugitives, etc.)	Indisponibilité	Endommagement logique	L'élément est bien là, mais a été pollué ou visiblement altéré
		Inopérabilité	L'élément est bien là, mais on ne peut y accéder ou le faire fonctionner (absence de clé d'accès ou d'autorisation : licence, jeton, etc.)
		Inexploitabilité	Les résultats ou actions de l'élément ou de sa mise œuvre ne sont pas conformes ou totalement absents (bug, blocage, incompatibilité de formats, résultats visiblement altérés, etc.)
		Disparition	L'élément a été effacé
	Défaut d'intégrité	Altération de l'élément	L'élément a été modifié (accidentellement ou volontairement)
	Divulgation	Copie de l'élément	L'élément a été copié
		Acquisition par un tiers de l'élément	L'élément immatériel a été acquis par un tiers (envoi direct erroné ou volontairement faussé)
Service extérieur nécessaire au fonctionnement des services internes ou à l'exploitation des données	Indisponibilité	Inopérabilité	Le service est bien présent, mais on ne peut y accéder ou le faire fonctionner (absence de moyen de communication, service volontairement inactif, absence de contrat ou de support administratif, mise en oeuvre du service impossible pour des raisons internes ou externes, etc.)
		Inexploitabilité	Les résultats ou actions de la mise œuvre du service ne sont pas conformes ou totalement absents (incapacité technique, incompatibilité de délais, résultats visiblement incomplets, etc.)
		Disparition	Le service n'existe plus ou n'est définitivement plus assuré.

Tableau des vulnérabilités intrinsèques :

Tableau des vulnérabilités intrinsèques génériques				
	Type d'actif secondaire	***Type de conséq. DIC***	***Type de dommage***	***Type de vulnérabilité***
Catégorie : Service				
	Élément matériel : Équipement fonctionnel, câblage, dispositifs de sécurité, etc. Media matériel support de logiciel, d'automatisme ou de paramètres de processus	D	Endommagement	Possibilité d'endommagement ou de destruction d'un équipement
		D	Inopérabilité	Possibilité d'incapacité à mettre ou maintenir l'équipement en service
		D	Inexploitabilité	Possibilité de non fonctionnement ou de fonctionnement incorrect d'un équipement
		D	Disparition	Possibilité de disparition d'un équipement
		I	Altération	Possibilité de modification matérielle d'un équipement
		I	Échange	Possibilité qu'un équipement soit échangé avec un équipement modifié
	Locaux	D	Endommagement	Possibilité d'endommagement général ou de destruction totale des locaux nécessaires au service
		D	Inopérabilité	Possibilité qu'il soit impossible ou interdit d'accéder aux locaux
	Moyens de servitude : Alimentation en énergie, fluides et climatisation, etc.	D	Endommagement	Possibilité d'endommagement général ou de destruction totale des moyens de servitude nécessaires au service
		D	Inopérabilité	Possibilité d'incapacité à mettre ou maintenir en service les moyens de servitude
	Éléments immatériels (support d'un processus) : Logiciel, automatisme, paramétrage de processus, procédure, etc.	D	Endommagement logique	Possibilité d'endommagement de configurations immatérielles
		D	Inopérabilité	Possibilité de blocage d'un processus par défaut d'autorisation
		D	Inexploitabilité	Possibilité de non fonctionnement intrinsèque d'un logiciel, d'un automatisme ou d'un processus (bug, dysfonctionnement majeur, erreurs récurrentes, etc.)
		D	Disparition	Possibilité d'effacement de configurations immatérielles
		I	Altération	Possibilité d'altération des configurations immatérielles supports de processus
		C	Divulgation	Possibilité de diffusion de configuration
	Compte ou moyen d'accès au service	D	Blocage	Possibilité de blocage des comptes utilisateurs
		D	Disparition	Possibilité de perte des moyens nécessaires à la connexion au service
	Media support de logiciel	D	Endommagement physique	Possibilité de destruction ou d'endommagement de media support de logiciel
		D	Inopértabilité	Possibilité d'incapacité à mettre le media en service (format de lecteur, incompatibilité de format de lecture, etc.)
		D et C	Disparition	Possibilité de disparition de media support de logiciel
		I	Echange	Possibilité d'échange de media support de logiciel par un media modifié
		C	Duplication	Possibilité de duplication de media support de logiciel
	Service extérieur nécessaire au fonctionnement des services internes ou à l'exploitation des données	D	Inopérabilité	Possibilité d'incapacité à mettre en œuvre le service extérieur
		D	Inexploitabilité	Possibilité de non fonctionnement du service extérieur
		D	Disparition	Possibilité de disparition du prestataire du service extérieur
Catégorie : données				
	Media support de données	D	Endommagement physique	Possibilité d'endommagement ou de destruction de media support de données
		D	Inopértabilité	Possibilité d'incapacité à lire le media (format de lecteur, incompatibilité de format de lecture, etc.)
		D et C	Disparition	Possibilité de disparition de media support de données
		I	Echange	Possibilité d'échange de media support de données avec un media contenant des données modifiées
		C	Duplication	Possible duplication de media support de données
	Fichier support de données	D	Endommagement logique	Possibilité d'endommagement logique du fichier de données
		D	Inexploitabilité	Possibilité d'altération massive ou d'inexploitabiité du fichier support de données
		D	Disparition	Possibilité d'effacement du fichier de données
		I	Altération	Possibilité d'altération du fichier support de données
		C	Divulgation	Possibilité de duplication ou diffusion (et divulgation) de fichier support de données
	Moyen d'accès aux données	D	Disparition	Possibilité de disparition d'un moyen nécessaire pour l'accès aux données (clés logiques ou physiques)
	Données en transit, messages, écrans	I	Altération	Possibilité d'altération de données en transit ou messages
		C	Divulgation	Possibilité de duplication (et divulgation) de données en transit, messages, écrans
		D et C	Perte	Possibilité de perte de données en transit ou messages
Catégorie : processus de fonctionnement				
	Procédures et directives	E	Inefficience	Possibilité que les procédures appliquées soient inefficientes (vis-à-vis des obligations légales, réglementaires ou contractuelles)

5. Définir la typologie des menaces

Il n'y a pas de risque s'il n'y a pas une cause, qui fait que la vulnérabilité intrinsèque de l'actif est effectivement exploitée.

Il est cependant nécessaire d'inclure dans la menace d'autres aspects que la simple cause.

En effet, il est nécessaire de préciser tout ce qui peut avoir une influence sur la probabilité d'occurrence du risque et donc tout paramètre descriptif de la manière dont le dommage pourrait survenir qui aurait ou pourrait avoir une influence sur cette probabilité.

C'est ainsi qu'il peut être nécessaire de décrire :

- L'événement déclenchant l'occurrence du risque (si les variantes d'événements n'ont pas la même probabilité).
- Le caractère volontaire ou accidentel de cet événement.
- L'acteur déclenchant cet événement, et en particulier les acteurs ayant des droits particuliers qui pourront plus (ou moins) facilement agir.
- Les circonstances dans lesquelles survient cet événement

Il est clair, en effet, que chacun de ces paramètres peut influer sur la probabilité d'occurrence du risque.

Ici encore, le niveau de détail avec lequel est décrit chacun de ces points est un élément clé dans la détermination du nombre de menaces différentes et donc, in fine, du nombre de risques différents qu'il faudra analyser et évaluer.

Ceci étant, deux éléments sont à prendre en compte pour le choix du niveau de détail, quel que soit l'élément analysé :

- Un niveau de détail supplémentaire conduit-il à distinguer des menaces ayant des probabilités intrinsèques différentes ?
- Existe-t-il des mesures de sécurité (dissuasives ou préventives) différentes qui rendent nécessaires de distinguer des éléments auxquels peuvent s'appliquer des mesures différentes ?

Nous allons revenir ci-dessous sur chacun des éléments constituant les menaces.

Typologie d'événements déclencheurs

La recherche des événements déclencheurs doit être organisée avec l'objectif d'être aussi exhaustive que possible.

Un tableau, comme le tableau d'analyse préliminaire des dommages utilisé pour les vulnérabilités peut être construit. Un tel tableau directement issu du tableau précédent est donné ci-dessous, à titre d'exemple (tableau en 2 parties).

Il complète simplement les dommages par leurs causes possibles en termes d'événements déclencheurs.

Tableau d'analyse préliminaire des menaces (causes des dommages)			
Type d'actif secondaire	***Type de conséquence***	***Type de dommage***	***Evénements déclencheurs possibles***
Élément matériel : Équipement fonctionnel, câblage, dispositifs de sécurité, etc. Media matériel support de logiciel, d'automatisme, de paramètres de processus ou de données	Indisponibilité	Endommagement physique	Événement naturel accidentel dû à l'environnement : - Incendie - Inondation - surcharge éléctrique - pollution chimique, vieillissement, etc. - etc.
			Accident provoqué par erreur humaine - Erreur de manipulation - Erreur de procédure
			Malveillance : - Dégradation volontaire physique directe - Dégradation indirecte (accident provoqué)
		Inopérabilité	Accident touchant le personnel d'exploitation : - Intoxication alimentaire - Epidémie ou pandémie
			Accident touchant des éléments nécessaires aux opérations : - Destruction de licence ou de jeton - Destruction ou endommagement de clé - Absence d'énergie, de climatisation, - Incapacité logistique (locaux, transports, restauration, etc.)
			Erreur humaine touchant des éléments nécessaires aux opérations : - Perte de licence, de jeton ou de clé - Moyen de lecture inadapté (non conservé ou non mis à jour)
			Action volontaire du personnel d'exploitation : - Démission collective massive - Mouvement social avec arrêt de travail
		Inexploitabilité	Non fonctionnement matériel : - Panne matérielle - Saturation accidentelle (réseau, système)
			Malveillance : - Saturation volontaire (attaque en déni de service)
		Disparition	Disparition accidentelle : - Perte / Oubli
			Disparition volontaire : - Vol
	Défaut d'intégrité	Altération	Modification par erreur de la configuration matérielle : - modification erronée de câblage - suppression/inhibition par erreur de dispositifs de sécurité
			Modification volontaire de la configuration matérielle : - modification de câblage - suppression/inhibition volontaire de dispositifs de sécurité
		Échange	Echange volontaire avec un élément matériiel modifié
	Divulgation	Duplication de l'élément matériel	Duplication volontaire de l'élément matériel
		Acquisition par un tiers de l'élément matériel	Acquisition accidentelle : - Perte / Oubli - Envoi par erreur ou accident à un mauvais destinataire
			Disparition volontaire : - Vol

Tableau d'analyse préliminaire des menaces (causes des dommages)			
Type d'actif secondaire	***Type de conséquence***	***Type de dommage***	***Evénements déclencheurs possibles***
Élément immatériel : Logiciel, automatisme, paramétrage de processus, procédure, etc. Données (fichiers constitués, données fugitives, etc.)	Indisponibilité	Endommagement logique	Accident provoqué par erreur humaine - Erreur de manipulation entâchant la cohérence des éléments - Erreur de procédure
			Malveillance : - Dégradation volontaire directe - Dégradation indirecte (accident provoqué)
		Inopérabilité	Accident touchant des éléments nécessaires aux opérations : - Destruction de licence ou de jeton - Destruction ou endommagement de clé
			Erreur humaine touchant des éléments nécessaires aux opérations : - Perte de licence, de jeton ou de clé - Logiciel de lecture inadapté (non conservé ou non mis à jour)
		Inexploitabilité	Non fonctionnement logiciel : - Panne logicielle - Saturation accidentelle (incapacité système à traiter des appels mutiples)
			Blocage de comptes utilisateurs : - Attaque en déni de service - Blocage volontaire pour raisons de sécurité
		Disparition	Accident provoqué par erreur humaine - Erreur de manipulation ou procédure entraînant l'effacement de l'élément
			Malveillance : - Effacement volontaire direct - Effacement indirect provoqué
	Défaut d'intégrité	Altération logique	Modification par erreur de la configuration logicielle ou des données : - erreur de frappe ou de saisie - modification erronée de séquencement et d'enchaînements - suppression/inhibition par erreur de dispositifs de sécurité
			Modification volontaire de la configuration logicielle ou des données : - falsification de données - falsification de programmes - suppression/inhibition volontaire de dispositifs de sécurité
	Divulgation	Copie de l'élément	Duplication volontaire de l'élément immatériel
		Acquisition par un tiers	Acquisition accidentelle : - Non effacement avant rebut, transfert, etc. - Envoi par erreur ou accident à un mauvais destinataire
Services extérieurs ou tiers	Indisponibilité	Inopérabilité	Accident touchant le personnel d'exploitation : - Intoxication alimentaire - Epidémie ou pandémie
			Accident touchant des éléments nécessaires aux opérations : - Indisponibilité des moyens de communication avec le prestataire - Indisponbiilité des conditions administratives (contrat, financement)
			Action volontaire du personnel d'exploitation : - Démission collective massive - Mouvement social avec arrêt de travail
		Inexploitabilité	Non fonctionnement des éqipements du prestataire : - Panne matérielle - Saturation accidentelle (réseau, système)
			Malveillance : - Saturation volontaire (attaque en déni de service)
		Disparition	Disparition du prestataire : - Dépôt de bilan
			Arrêt volontaire d'activité : - Cessation d'activité (partielle ou totale)

Il convient de noter que les types d'événements déclencheurs signalés ci-dessus peuvent être développés ou au contraire synthétisés, en fonction du degré de détail souhaité et jugé optimal.

Il convient également de noter que seule la nature de l'événement déclencheur a une influence sur la potentialité intrinsèque du risque, les conditions de survenance et le type

d'acteur n'intervenant que sur la potentialité résiduelle, par l'intermédiaire des mesures dissuasives et préventives qui peuvent dépendre de ces circonstances ou du type d'acteur.

Typologies de conditions de survenance

Certaines circonstances de survenance ont une influence directe sur la potentialité résiduelle d'un risque, une fois des mesures spécifiques mises en place.

C'est en particulier le cas pour :

- Les actions volontaires menées, sur des éléments matériels ou immatériels, à distance ou non, depuis l'intérieur de l'entreprise ou non, pendant les heures de présence du personnel ou non, selon certaines phases d'un processus, etc.
- Les accidents ou erreurs survenant à certaines phases particulières d'un processus (saisie de données, stockage, traitement, impression, envoi, etc.)
-

Le tableau précédemment utilisé d'analyse des menaces peut alors être complété pour décrire les conditions de survenance qu'il conviendrait de distinguer pour une meilleure évaluation des menaces et des risques, et, en particulier :

- Les lieux dans lesquels l'événement déclencheur survient,
- Les périodes de temps auxquelles il survient,
- Les voies d'accès utilisées,
- Les étapes de processus concernées.

Typologie d'acteurs

Les types d'acteurs ont une influence sur la potentialité résiduelle d'un risque pour la simple raison que certaines mesures sont spécifiques à certains types d'acteurs (les contrôles d'accès n'ont pas d'effet contre des utilisateurs légitimement autorisés)

Le tableau d'analyse des menaces précédemment utilisé peut alors également être complété pour décrire les types d'acteurs qu'il conviendrait de distinguer pour une meilleure évaluation des menaces et des risques, et, en particulier :

- Les acteurs internes ayant des droits permanents,
- Les acteurs internes ayant des droits privilégiés de par leur fonction,
- Les acteurs externes ayant des profils particuliers,
- Les acteurs externes à qui il a été octroyé des droits temporaires,
- Etc..

Description de la menace dans la base de connaissance

La description de la menace d'un risque dans la base de connaissance doit ainsi comprendre :

- La description de l'événement déclencheur,
- Le type de dommage,
- Les conditions de survenance,
- Le type d'acteur.

6. Construire la base de scénarios (liste de scénarios et éléments descriptifs)

La base de scénarios sera ainsi construite en rassemblant les divers éléments analysés plus haut à savoir :

- Le type d'actif
  - Type d'actif primaire
  - Type d'actif secondaire
- Le type de vulnérabilité
  - Type de dommage
  - Type de vulnérabilité intrinsèque
- Le type de menace
  - Type d'événement déclencheur
  - Type de conditions de survenance
  - Type d'acteur

Il est fortement recommandé de compléter cette description d'une expression littérale décrivant le risque en termes simples et parlant pour tout utilisateur de la base de connaissance.

7. Définir les services de sécurité

Dans MEHARI, on fait appel aux services de sécurité pour évaluer la potentialité et l'impact résiduels et ceci en fonction du niveau de qualité de ces services.

Cela impose que l'on sache évaluer cette qualité, mais aussi que l'on soit sûr que l'efficacité ainsi évaluée s'applique bien dans le cas du scénario de risque analysé, conformément au principe n° 1 rappelé en début de document. Une première condition pour cela est, bien entendu, qu'il n'y ait aucune ambiguïté sur la finalité du service.

C'est pour cette raison que le Clusif a établi en principe la nécessité d'établir, pour chaque service de sécurité, une fiche décrivant :

- la finalité du service,
- les scénarios de risque sur lesquels il agit, c'est-à-dire les résultats attendus de la mise en œuvre du service,
- les mécanismes ou solutions possibles de réalisation et de mise en oeuvre,
- les éléments caractéristiques de la qualité du service, c'est-à-dire les critères de jugement de :
  - son efficacité,
  - sa robustesse,
  - sa mise sous contrôle.

Ceci étant, il faut être conscient qu'un service peut toujours être décomposé en « sous-services », à l'infini, chaque question posée aujourd'hui ayant sa propre finalité et pouvant, à la limite, être élevée au rang de service et décomposée en sous-questions et ainsi de suite.

La question du niveau de détail des services de sécurité est donc une question clé, ayant une influence décisive sur la charge d'évaluation et de diagnostic de la qualité desdits services.

Pour définir au mieux ce niveau de détail, il faut tenir compte de plusieurs paramètres :

- Définir des services de sécurité cohérents avec la typologie d'actifs (voir chapitre 3).
- Définir des services de sécurité cohérents avec la typologie des vulnérabilités
- Définir des services de sécurité cohérents avec la typologie des menaces
- Faire un choix entre définir des services différents ou utiliser des variantes du même service (par le schéma d'audit)

Nous allons aborder, ci-dessous, ces différents aspects.

Définir des services de sécurité cohérents avec la typologie d'actifs

Nous avons déjà évoqué ce point au chapitre 3. Précisons les impératifs et les options.

Il peut sembler indispensable qu'aux actifs distingués dans la typologie des actifs correspondent des services de sécurité distincts. Outre que cela parait naturel, cela permet des diagnostics plus précis et donc une meilleure analyse des risques auxquels l'entité est exposée.

En fait, cela n'est pas obligatoire, tant que l'on respecte les principes définis pour établir les questionnaires de diagnostic des services (voir chapitre suivant). En effet, si ces principes sont respectés, tout ce que l'on risque à regrouper des services protégeant des actifs différents est de

faire un diagnostic pessimiste. En effet, le même service étant évalué pour plusieurs types d'actifs différents, on sera amené à poser des questions relatives à chaque type d'actif et à faire une évaluation globale fonction de la plus mauvaise réponse.

Un tel diagnostic pessimiste n'est pas dangereux en terme d'analyse de risque mais peut conduire à des plans d'action inutiles et donc à des dépenses inutiles.

Autrement dit, si les actifs sont distincts, ils peuvent avoir des classifications différentes, c'est-à-dire des besoins différents, et le regroupement de services peut conduire à surprotéger des actifs qui ne nécessitaient pas un tel niveau de protection.

Sans être obligatoire, il est donc conseillé de définir des services de sécurité distincts pour des actifs distincts.

A l'inverse, si des actifs ont été confondus et regroupés, un niveau de détail plus fin au niveau des services de sécurité qu'au niveau des actifs ne présente pas d'inconvénient au plan de l'analyse des risques. Le seul inconvénient est l'accroissement de la charge de travail, mais il n'est même pas sûr que le surcroît de travail ne puisse pas s'avérer utile par la suite pour le choix des mesures de sécurité.

Prenons un exemple pour éclairer ce dernier point :

Supposons que l'on ait défini comme type d'actif l'infrastructure informatique (sans faire de détail entre le réseau étendu, le réseau local, les systèmes informatiques et les systèmes bureautiques), alors que des services de sécurité distincts sont évalués lors du diagnostic, il sera aisé de prendre en compte la variété des services dans les formules de calcul des facteurs de réduction de risque, par l'emploi des fonctions « min » et « max ».

Définir des services de sécurité cohérents avec les typologies de vulnérabilités et de menaces

Nous avons également évoqué ce point plus haut dans ce document.

Disons globalement que le même raisonnement que ci-dessus s'applique et que l'on peut énoncer le principe suivant :

Sans être obligatoire, il est donc conseillé de définir des services de sécurité distincts pour pallier des vulnérabilités ou des menaces distinctes.

Pour préciser ce point, on peut ajouter les arguments suivants :

Les tableaux utilisés pour analyser puis définir les types de vulnérabilités ont été utilisés et complétés pour définir les types de menaces. Or ce sont ces menaces et ou ces vulnérabilités qui devront être combattues ou réduites par des services de sécurité pour limiter les risques.

De la même manière que pour les types d'actifs, des types de services de sécurité distincts pour des vulnérabilités ou des menaces distinctes ne sont pas obligatoires mais conduiront à des plans de sécurité plus optimisés et à une moindre dépense d'énergie.

A l'inverse et de même que pour les types d'actifs, des services de sécurité définis de manière plus fine que les vulnérabilités ou les menaces ne l'imposent ne sont pas un inconvénient du point de vue de l'analyse de risque, les formules de calcul des facteurs de réduction de risque permettant d'en tenir compte.

Définir des services de sécurité différents ou travailler avec des variantes d'un même service

La question se pose parfois de définir des services de sécurité différents ou de traiter les différences par des variantes de services au niveau du schéma d'audit.

Cette question a maintes fois été posée, par exemple pour les contrôles d'accès : faut-il définir des services de contrôle d'accès différents pour le réseau étendu, le réseau local, l'accès aux systèmes, aux applications et pour les contrôles d'accès applicatifs aux données, etc, avec l'inconvénient inévitable de devoir répondre autant de fois à des questions très proches, si ce n'est identiques, pour des actifs différents éventuellement sécurisés avec une politique de sécurité commune et ne peut-on plutôt travailler avec des variantes.

Une première réponse factuelle est que, même avec des variantes, il faudra poser autant de questions que de variantes et que cela ne simplifiera donc pas la tâche mais imposera en outre un vocabulaire unique ce qui peut être un inconvénient de compréhension.

La deuxième réponse, plus fonctionnelle, est à rechercher dans les formules de calcul des facteurs de réduction des risques et dépend donc, en grande partie, de l'architecture des systèmes et de l'imbrication des services de sécurité qui assurent les services.

Si plusieurs services de sécurité pouvant être différents ou assurés par des variantes différentes sont utilisés « en série », le meilleur d'entre eux assurant et imposant le niveau de sécurité de l'ensemble ce qui se traduit par des « max » dans les formules, ils ne peuvent être traités avec efficacité par des variantes et doivent être considérés comme des services distincts (à noter que c'est bien le cas des contrôles d'accès évoqués plus haut).

Si, par contre, les différents services sont des options, donc utilisés en parallèle et appelés par des formules avec des « min », ils peuvent être traités par des variantes.

Dernière remarque sur ce sujet. Si on ne considère qu'un service unique, sans variante, les questionnaires devront être généraux et ne pas détailler les questions par type d'actifs à l'intérieur d'un même questionnaire : c'est lors de la réponse globale que les personnes interviewées devront tenir compte de l'architecture pour faire une réponse appropriée.

8. L'évaluation de la qualité des services de sécurité et l'élaboration des questionnaires de diagnostic

Considérations générales

Le but du diagnostic et des questions étant d'évaluer la qualité de chaque service de sécurité, il importe de définir l'échelle de cotation.

La « théorie » est que la qualité reflète à la fois ***l'efficacité*** du service (pour atteindre sa finalité), ***sa robustesse*** pour se défendre contre une attaque directe visant à le court-circuiter et sa ***mise sous contrôle***. Il s'agit donc d'une échelle « absolue », indépendante des capacités de la technologie à répondre à l'exercice du service.

Une autre vision « réaliste » serait une référence à « ce qui se fait généralement ».

Cette voie consisterait, par exemple, à considérer qu'un mot de passe est la méthode d'authentification très majoritairement employée et donc que l'on doit pouvoir atteindre une note de 3, voire de 4, si ces mots de passe sont très bien gérés (toutes les règles connues sont appliquées, il n'est pas stocké ni transmis en clair, on ne peut tenter de le découvrir par essais successifs, etc.). Avec une telle approche, on pourrait obtenir une note de 3 ou de 4 avec une authentification par mot de passe, alors que le service est inefficace dans nombre de cas : attaque menée par un initié situé dans l'entourage immédiat de l'utilisateur qui s'authentifie et qui peut tout simplement l'observer, attaque menée par une personne ayant accès au poste et capable d'y introduire un logiciel espion, attaque menée par un informaticien capable de modifier le code du processus d'authentification, etc.

Cette dérive est, bien évidemment, contraire à l'esprit de la méthode. Elle est, en pratique, impossible à maîtriser puisque la référence ne peut être définie (quel est le niveau de « ce qui se fait » ?).

La qualité de service doit être jugée « dans l'absolu » par rapport aux critères standards de qualité (efficacité, robustesse, mise sous contrôle), indépendamment des pratiques courantes.

Des définitions de niveau de qualité de service ont été données, et se trouvent dans la documentation standard de MEHARI.

Questionnaires d'évaluation de la qualité de service

Les deux principes généraux exposés en début de document conduisent à exiger des questionnaires que, pour chaque service, chaque question posée soit pertinente et justifiée.

Toute question superflue par rapport à la finalité du service peut conduire à une surévaluation du service (contraire au principe de précaution) ou à une sous-évaluation qui ne saurait être justifiée (contraire au principe de justification).

Toute question posée doit être pertinente et justifiée eu égard à la finalité du service.

Ceci impose un certain nombre de contraintes à ceux qui établissent les questionnaires ou qui les valident :

- Vérifier que chaque question posée correspond bien à la finalité du service.

- Vérifier que chaque service abordé l'est bien en profondeur et que les questions essentielles sont bien posées. Sinon, choisir entre rajouter des questions ou supprimer le service.
- Vérifier que l'on traite bien tous les aspects de la qualité de service, à savoir son efficacité, sa robustesse et sa mise sous contrôle.
- Vérifier que si l'on répond oui (ou 1) à toutes les questions du service (et que, par définition, on obtient alors la note maximale de 4) la qualité du service correspond bien à la définition de qualité retenue, c'est-à-dire que le service accomplit totalement sa fonctionnalité, qu'il est bien sous contrôle avec un excellent niveau de robustesse.

9. Construire la base de connaissance des scénarios

La construction de la base de connaissance des scénarios, une fois établie la base des scénarios (leur liste et leurs caractéristiques descriptives), consiste essentiellement à établir pour chacun les formules de calcul des facteurs de réduction de risque.

Pour respecter l'esprit de la méthode, les principes fondamentaux cités en début de document doivent être respectés. L'application de ces principes conduit à un certain nombre de prescriptions développées ci-dessous.

Services appelés dans les formules de calcul des STATUS

Pertinence de l'évaluation des services pour les scénarios qui l'appellent

Par application du principe de précaution, il est nécessaire que l'appel à un service de sécurité soit pertinent, c'est-à-dire que l'on soit sûr que l'évaluation du service, faite lors d'un audit, soit pertinente pour le scénario. Ceci a deux types de conséquences :

- Si une seule question parmi d'autres, dans le questionnaire de diagnostic du service, a un effet sur le scénario, mais si l'ensemble des autres questions du questionnaire n'a pas d'effet sur ce scénario, il ne faut pas faire appel à ce service (sinon une bonne note due aux autres questions réduirait sans raison le niveau de risque du scénario).
- Il est nécessaire enfin que le service s'applique avec efficacité, dans toute la généralité de sa définition et que les questions qui auront été posées pour évaluer le service soient pertinentes **dans le contexte** du scénario étudié. Exemple : Si on fait appel au PCU (Plan de Continuité des activités Utilisateurs), c'est dans la généralité de sa fonction, c'est-à-dire en appui d'un PRA (Plan de Reprise d'Activités informatiques) Si le scénario est tel que le PRA ne s'appliquera pas, c'est à un PCU particulier qu'il faudrait faire appel et on ne doit pas faire appel au service général PCU (mais éventuellement créer un service spécifique de Plan de secours entièrement « manuel »).

En toute rigueur, le principe qui découle des deux points ci-dessus, pourrait s'exprimer ainsi :

Les services appelés dans des formules de calcul de STATUS sont tels que toute question posée pour évaluer le service est pertinente pour les scénarios qui l'appellent.
On prendra garde, néanmoins, qu'une application trop stricte de ce principe ne conduise à un trop grand émiettement des services et on retiendra plutôt un énoncé moins radical :

Un scénario ne doit faire appel à un service que si son évaluation est pertinente pour le scénario, quelles que soient les questions auxquelles il est répondu affirmativement.

Pertinence d'un service pour réduire l'impact intrinsèque

Il s'agit ici des services appelés par les formules de calcul des facteurs de réduction d'impact, pouvant donc avoir un rôle de confinement ou comme mesure palliative.

Par application du principe de précaution, il est nécessaire que l'on soit sûr que ce service agira effectivement sur l'impact résiduel et donc sur les critères et seuils d'impact qui ont été à la base de l'évaluation de l'impact intrinsèque.

Prenons quelques exemples :

- Si un critère d'impact a été la destruction ou l'indisponibilité durable d'éléments d'infrastructure avec des seuils variant avec l'étendue ou l'ampleur des éléments

atteints, un service de détection d'incendie aura bien une influence sur l'impact résiduel. Si, par contre, pour le même niveau d'impact maximal, le critère était la destruction ou l'indisponibilité de certains éléments précis de l'infrastructure (impact maximal dû, par exemple, à une classification de niveau 4 pour tel serveur, de niveau 2 pour tel autre), alors il n'est pas sûr que la détection d'incendie soit pertinente car si l'incendie nait à proximité immédiate de l'élément le plus critique, sa détection pourrait ne pas changer le niveau d'impact résiduel (détection trop tardive).

- Si un critère d'impact est la fraude, avec des seuils fonction du montant de la fraude, un service de contrôle permanent applicatif peut être pertinent pour réduire l'impact d'un scénario de fraude. Si, par contre, pour le même critère d'impact, les seuils sont uniquement fonction des domaines concernés (RH, gestion de clientèle, etc.), les contrôles permanent ne seront peut-être pas pertinents et ne devraient pas être retenus.

Ceci conduit à exprimer le principe suivant :

L'appel à un service pour réduire l'impact doit être pertinent, quels que soient les critères et seuils d'impact qui ont été à l'origine de l'évaluation de l'impact intrinsèque du scénario.

L'application stricte de ce principe serait néanmoins pénalisante pour les scénarios pour lesquels on ne peut décider à l'avance, dans la base de connaissance, si tel service sera pertinent ou non car on ignore les critères utilisés et la nature des seuils d'impact correspondants, comme dans les exemples ci-dessus.

Il est nécessaire de prévoir alors une variable permettant au responsable de l'analyse de risque de décider, au cas par cas, si on peut faire appel à ces services ou non.

C'est ainsi qu'a été créée, dans la base de connaissance de MEHARI, une variable permettant de déclarer un scénario confinable ou non.

Le principe devient alors :

L'appel effectif à un service pour réduire l'impact d'un scénario, appel éventuellement fonction d'une variable de commande spécifique, doit être pertinent compte tenu des critères et seuils d'impact utilisés pour évaluer l'impact intrinsèque.

S'agissant ici de construire une base de connaissance, l'application de ce principe doit être comprise ainsi :

Dans les cas où il y doute sur le caractère général de la pertinence du service de sécurité pour un scénario donné, il convient, par application des deux principes de précaution et de justification, de mettre en place les formules faisant appel au service mais de positionner la variable de commande sur la position où l'appel au service est inhibé, de sorte qu'il faille une action volontaire de validation (ou de suppression de l'inhibition) pour que l'appel au service devienne effectif.

Pertinence d'un service pour réduire la potentialité

Il s'agit ici des services appelés par les formules de calcul des facteurs de réduction de potentialité, pouvant donc avoir un rôle de dissuasion ou de prévention.

Par application du principe de précaution, il est nécessaire que l'on soit sûr que ce service agira effectivement sur la potentialité résiduelle et donc sur les considérations qui ont été à la base de l'évaluation de la potentialité intrinsèque.

C'est le parallèle de ce qui a été dit ci-dessus. Il est, cependant, beaucoup plus simple à mettre en œuvre car la potentialité intrinsèque des événements déclencheurs ne dépend pas (généralement) d'éléments externes non définis.

On peut néanmoins exprimer le principe de base suivant :

L'appel effectif à un service pour réduire la potentialité d'un scénario doit être pertinent quelles que soient les raisonnements utilisés pour évaluer la potentialité intrinsèque.

L'application de ce principe revient en pratique à recommander une parfaite adéquation entre le niveau de détail des événements déclencheurs et le niveau de détail des services de sécurité, ainsi que nous l'avons déjà expliqué.

Traitement des scénarios d'atteinte à l'intégrité

Quand on analyse des scénarios d'atteinte à l'intégrité, on traite, en pratique, plusieurs types de scénarios :

- Les scénarios d'atteinte à l'intégrité d'une base de données ou de fichiers, pour lesquels, une fois le défaut d'intégrité détecté, les mesures palliatives consistent à réparer les fichiers ou bases endommagées pour pouvoir redémarrer sur des bases saines. Ces scénarios peuvent être évolutifs (confinables) ou non (voir paragraphe suivant).
- Les scénarios de type fraude pour lesquels il n'y a guère de mesures palliatives et qui ne sont pas évolutifs (l'impact maximum est atteint dès l'action consommée) mais pour lesquels il existe des mesures de limitation d'impact direct (contrôles permanents, seuils de détection, etc.) qui font qu'ils doivent être considérés comme confinables.
- Certains scénarios d'erreurs ou d'accident ayant le même type de conséquences qu'une fraude, c'est-à-dire un impact limitable ou confinable, sans mesures palliatives possibles.

Les premiers sont, en fait, des scénarios d'atteinte à la disponibilité ; la cause initiale est bien un défaut d'intégrité mais **dès que ceci est connu, on se trouve ramené à un problème de disponibilité et, lors de l'évaluation de l'impact intrinsèque on suppose très généralement, que l'intégrité est atteinte mais que l'on ne le sait pas.**

Ces scénarios sont intitulés « Pollution massive de données » et doivent être traités comme des scénarios d'atteinte à la disponibilité.

Par contre, pour les scénarios d'atteinte à l'intégrité de type fraude ou équivalent (deuxième et troisième type cité ci-dessus), on doit considérer que le défaut d'intégrité n'est pas connu.

Dès lors, il ne devrait pas exister de service pertinent en mesures palliatives susceptibles de réduire l'impact. Par contre des mesures de confinement restent possibles.

Les scénarios d'atteinte à l'intégrité sont considérés comme confinables mais ne devraient pas faire appel, en standard, à des mesures palliatives.

10. Finaliser la base de connaissance MEHARI

La dernière étape dans la construction d'une base de connaissance MEHARI est sa finalisation et sa mis en forme dans un format final, directement exploitable ou non.

Nous n'aborderons pas ici les aspects techniques car ils dépendent du type de support que l'on souhaite offrir. Les bases de connaissance MEHARI ont été livrées, avant la version 2010 sous une forme non directement exploitable alors que depuis la dernière version, les bases Excel ou OpenOffice permettent une exploitation directe.

11. Conseils de mise en œuvre

Il pourrait sembler que l'ordre présenté, actifs, puis vulnérabilités, puis menaces, puis services de sécurité, puis scénarios et base de scénarios, etc. ne soit pas obligatoire et que l'on puisse commencer par les services de sécurité et remonter en sens inverse.

Nous considérons qu'il est préférable de commencer par les actifs et non l'inverse, mais le débat peut être ouvert à ce sujet, tant que l'ensemble des principes présentés dans ce document est respecté.

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11, rue de Mogador

75009 Paris

✆ 01 53 25 08 80

clusif@clusif.asso.fr

Téléchargez les productions du CLUSIF sur

www.clusif.asso.fr