Partie 3
Outils et exemples

Chapitre 3-1
Méthodes

1. Introduction

Ce chapitre est dédié aux méthodes de gestion des risques. Il en existe un très grand nombre et cela peut être source de confusion. Pour rappel, les normes ISO n'imposent en aucun cas une méthode à suivre. L'organisation est libre de sélectionner une méthode parmi celles existantes, ou de créer et suivre sa propre méthode.

Nous décrirons ici les trois méthodes les plus connues que sont OCTAVE, MEHARI et EBIOS. En France, et à ce jour, c'est la méthode EBIOS qui est la plus utilisée.

Chaque méthode est structurée autour de processus logiques, d'outils opérationnels et d'une philosophie propre. Leur connaissance permet à une organisation de choisir celle qui sera la plus adaptée à ses enjeux spécifiques, ou de s'en inspirer pour construire sa propre démarche de gestion des risques

2. OCTAVE

OCTAVE signifie « Operationally Critical Threat, Asset, and Vulnerability Evaluation ». Il s'agit d'une série de méthodes d'évaluation et de planification stratégique de la sécurité de l'information basées sur les risques.

Il y a trois versions différentes d'OCTAVE :

– OCTAVE
– OCTAVE-S pour les petites organisations
– OCTAVE Allegro, qui est une approche simplifiée pour l'évaluation de la sécurité de l'information.

2.1 La méthode OCTAVE

La méthode OCTAVE se déroule en trois phases. La phase 1, dite organisationnelle, durant laquelle les équipes identifient les actifs importants liés à l'information et la stratégie actuelle de leurs protections. C'est alors que l'équipe déterminera quels sont les actifs les plus critiques pour l'organisation, puis documentera les exigences en matière de sécurité de l'information et identifiera les menaces.

La phase 2, dite technologique, permet à l'équipe d'analyse d'effectuer une évaluation de l'infrastructure, d'identifier les actifs techniques critiques et les vulnérabilités techniques qui y sont liées.

La phase 3, dite d'analyse de risques, permet de mettre en place un plan d'actions en se basant sur les résultats obtenus lors des deux premières phases.

2.2 La méthode OCTAVE-S

La méthode OCTAVE-S est une méthode simplifiée d'analyse de risques liés à la sécurité des actifs critiques d'une entreprise. Elle se déroule également en trois phases distinctes que nous détaillerons ci-dessous. Il est à savoir qu'OCTAVE-S suppose que tous les intervenants (l'équipe d'analyse) possèdent une connaissance pratique des actifs, des menaces et des exigences de sécurité. Ainsi, il ne s'agira pas de faire des entretiens dans le but d'obtenir les connaissances, mais bien de constituer une équipe d'analyse autonome.

2.2.1 Phase 1 : Construire des profils de menaces basés sur les actifs

Cette phase sert à définir les critères d'évaluation des impacts, à identifier les actifs de l'entreprise et à évaluer les pratiques actuelles en matière de sécurité. Seules les informations nécessaires sont recueillies et on limite le nombre d'actifs à approfondir au nombre de 5. La phase 1 se termine par la définition des exigences de sécurité et d'un profil de menace pour chacun des actifs critiques sélectionnés.

2.2.2 Phase 2 : Identifier les vulnérabilités de l'infrastructure

Cette phase sert à examiner l'infrastructure informatique de l'entreprise, en mettant l'accent sur les méthodes d'accès aux différents actifs critiques et en identifiant les personnes responsables de la configuration et de la maintenance de ceux-ci. L'objectif sera de se rendre compte de la manière dont ces personnes maintiennent la sécurité de l'infrastructure.

2.2.3 Phase 3 : Élaborer des stratégies et des plans de sécurité

Lors de cette phase, l'équipe d'analyse identifie les risques liés aux actifs listés précédemment et décide de la façon de les traiter. Une stratégie de protection est alors créée ainsi que des plans d'actions.

2.3 La méthode OCTAVE Allegro

La méthode OCTAVE Allegro est une méthode d'évaluation des risques axée sur les actifs informationnels, contrairement à OCTAVE qui est une évaluation des risques axée sur les actifs technologiques. La méthode Allegro est également plus simple que les deux méthodes précédentes, et de fait la plus utilisée à ce jour.

Elle se compose de huit étapes regroupées en quatre grands domaines d'activités :

– Établir des déterminants : l'entreprise définit des critères de mesure du risque (étape 1).
– Profiler l'actif : l'entreprise identifie les actifs à évaluer ainsi que leurs conteneurs (étapes 2 et 3).
– Identifier les menaces : l'entreprise identifie les domaines de préoccupation et les scénarios de menaces (étapes 4 et 5).
– Identifier et atténuer les risques : l'entreprise identifie et analyse les risques et choisit une méthode de traitement de ces derniers (étapes 6, 7 et 8).

Nous détaillerons ci-après chacune des étapes qui composent la méthode OCTAVE Allegro.

2.3.1 Étape 1 - Établir des critères de mesure du risque

Cette première étape consiste à établir les critères qui seront utilisés pour évaluer les effets d'un risque sur la mission et les objectifs d'une organisation. Ces critères sont un ensemble de mesures qualitatives permettant d'évaluer les effets d'un risque et ils constituent le fondement d'une évaluation du risque lié aux actifs informationnels.

Cette étape sert également à hiérarchiser les domaines en fonction de leur importance pour l'organisation. Certains d'entre eux peuvent être prioritaires sur d'autres en fonction de l'entreprise dans laquelle nous effectuons notre analyse de risques. Un fournisseur d'accès à internet privilégiera sa réputation auprès de sa clientèle, alors qu'une banque mettra l'accent sur le domaine financier.

Les domaines d'impact identifiables sont les suivants :

– réputation/confiance des clients ;
– productivité ;
– sécurité et santé ;
– amendes/sanctions légales ;
– zone d'impact définie par l'utilisateur (champ libre).

Des feuilles de travail sont mises à disposition par la méthode OCTAVE Allegro permettant de réaliser cette évaluation. Il est ainsi possible de traiter pour chacun des domaines l'impact potentiel du risque identifié. La feuille de travail se présente sous forme d'un tableau qui nous permet de déterminer l'incidence en choisissant entre « faible », « modéré » ou « haut ». Le dernier document de travail de l'étape 1 consiste tout simplement à classer les différents domaines par ordre d'importance.

Zone d'impact	Notation
Finance	4
Réputation	3
Sécurité et santé	2
Productivité	2
Amendes/juridique	1

2.3.2 Étape 2 - Élaborer des profils d'actifs informationnels

Cette étape consiste à créer des profils pour les actifs informationnels identifiés pour l'analyse de risques décrivant leurs particularités, qualités, caractéristiques et valeur. Ce profilage permet de s'assurer que l'actif est bien défini, de manière claire et sans ambiguïté aussi bien sur ses limites que sur ses exigences en matière de sécurité.

Une feuille de travail existe afin de consigner ce profilage qui sera utile par la suite pour identifier les menaces et les risques.

2.3.3 Étape 3 - Identifier les conteneurs d'actifs informationnels

Les conteneurs sont les endroits où les ressources informationnelles sont stockées, transportées ou traitées.

Si un risque est identifié pour le conteneur de l'actif, il est automatiquement hérité par l'actif lui-même. Ces espaces de stockage peuvent être localisés au sein de l'organisation mais également à l'extérieur. En effet, stocker des données dans le cloud est un exemple typique de conteneur d'actif informationnel délocalisé.

Cette troisième étape permet d'identifier tous les conteneurs dans lesquels les données sont stockées, traitées ou transportées, à l'intérieur ou à l'extérieur de l'organisation.

Une feuille de travail est fournie par OCTAVE Allegro pour identifier ces emplacements. Il s'agira donc d'identifier les conteneurs techniques (réseau, hébergeurs, cloud, etc.), physiques (centres de données, disques durs, etc.) ou encore les personnes ayant accès ou une connaissance détaillée de ces derniers.

2.3.4 Étape 4 - Identifier les domaines de préoccupation

Cette étape débute par une réflexion sur les situations possibles qui peuvent menacer les actifs informationnels de l'organisation. Il ne s'agira pas d'établir une liste exhaustive de toutes les situations possibles, mais seulement les plus évidentes, les premières qui viennent à l'esprit.

Un exemple de sujet de préoccupation : « une mauvaise configuration des droits d'accès au serveur de fichiers permet à un employé de visualiser les fiches de salaire de ses collègues. »

Là encore une feuille de travail fournie par OCTAVE Allegro nous aide à détailler ces sujets de préoccupation.

2.3.5 Étape 5 - Identifier les scénarios de menace

Un scénario de menace est une situation dans laquelle un actif informationnel peut être compromis. Il se compose généralement d'un acteur, d'un motif, d'un moyen et d'un résultat indésirable.

Cette étape reprendra donc les sujets préoccupants de l'étape précédente et les approfondira en détaillant davantage les propriétés de la menace. Un outil fourni par OCTAVE allegro, nommé l'arbre des menaces, permet d'aller plus loin dans l'identification des scénarios, ainsi qu'un formulaire nous aidant à déterminer les probabilités et impacts de chacun des scénarios identifiés.

2.3.6 Étape 6 - Identifier les risques

Le risque correspond à la combinaison de la vraisemblance d'un scénario de menace de l'impact potentiel sur les actifs concernés. Il s'agira donc ici d'identifier les impacts aux scénarios identifiés précédemment, qui peuvent être multiples (réputation, productivité, finances, sécurité et santé, amendes et frais juridiques).

Par exemple, pour un hébergeur de données de santé, une faille liée à la confidentialité des données aura plusieurs conséquences sur l'organisation, notamment sur sa réputation, ses obligations légales et ses finances).

2.3.7 Étape 7 - Analyser les risques

Lors de cette étape, une mesure quantitative simple est calculée. Ce score est obtenu en tenant compte de l'incidence de la menace mais aussi de l'importance relative des domaines dans lequel le risque est présent. Si, pour une organisation, la réputation est le domaine privilégié, tous les risques qui y sont liés généreront des scores plus importants, bien que l'impact soit équivalent s'il touche un autre domaine.

La première partie consistera à évaluer les conséquences relatives à chacune des zones d'impact en attribuant une note entre « faible », « modéré » et « élevée », valant respectivement 1, 2 et 3 points.

La seconde partie consistera à calculer un résultat de risque relatif en multipliant le score par zone d'impact définie lors de l'étape 1, par la valeur de l'impact défini lors de l'étape 7. Cela nous permet donc de hiérarchiser les risques.

Zone d'impact	Notation	Valeur de l'impact	Score
Finance	4	Modéré (2)	8
Réputation	3	Faible (1)	3
Sécurité et santé	2	Fort (3)	6
Productivité	2	Faible (1)	2
Amendes/juridique	1	Modéré (2)	2
		Score total	21

2.3.8 Étape 8 - Sélectionner une approche d'atténuation

Une fois les risques hiérarchisés, des stratégies d'atténuation sont élaborées en tenant compte de la valeur de l'actif et de ses exigences de sécurité, des conteneurs dans lesquels il se trouve et de l'environnement opérationnel de l'organisation. Les risques devant être atténués sont choisis en fonction de leurs impacts et de leurs probabilités. Pour cela, il n'existe pas de voie décisive à suivre, il s'agira d'une décision des parties intéressées.

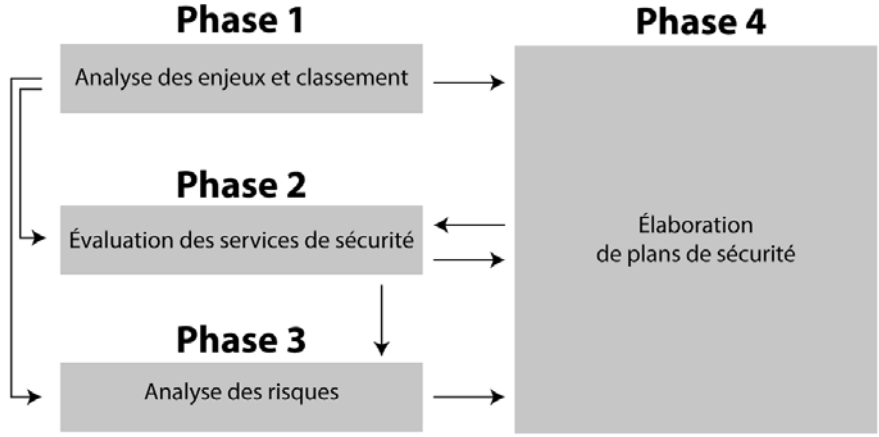
Le traitement des risques reprend les quatre options que nous avons déjà détaillées auparavant dans le chapitre Traitement et acceptation des risques, à savoir la réduction, le maintien, le refus et le transfert des risques.

3. MEHARI

La méthode MEHARI (Méthode Harmonisée d'Analyse de Risques) est une méthode d'analyse de risques développée par le CLUSIF (Association Française des professionnels de la sécurité de l'information). Créée en 1995, elle permet d'évaluer et de gérer les risques associés aux scénarios.

Cette méthode se décline en quatre phases distinctes qui sont les suivantes :

– Phase 1 : Analyse des enjeux et classement
– Phase 2 : Évaluation des services de sécurité
– Phase 3 : Analyse des risques
– Phase 4 : Élaboration de plans de sécurité



3.1 Phase 1 : Analyse des enjeux et classement

Cette phase consiste à identifier les dysfonctionnements de l'organisation au niveau fonctionnel et technique en commençant par analyser les activités de l'organisation et ses objectifs. Pour ce faire, une collaboration entre les décideurs, le management et les parties prenantes est obligatoire.

Cette analyse nous apportera une échelle de valeurs des dysfonctionnements potentiels ainsi qu'une classification des actifs.