

## La lettre E-SECURITY n° 51 - Juillet/Août 2008



### EDITORIAL

<b>EDITORIAL</b>	p1
<b>AGENDA</b>	p1
<b>ACTUALITES</b>	p2
<b>VEILLE</b>	p3
➤ Supervision Sécurité et Microsoft System Center Operations Manager 2007	
<b>ZOOM</b>	p5
➤ Mise en pratique du secours informatique dans une entreprise	
<b>L'ESSENTIEL</b>	p7
➤ Gestion du risque, différentes approches avec MEHARI	

#### Un air de vacances en toute sécurité

Alors que le soleil doucement nous enchante,  
Trêve dans notre travail : confiants nous le délaissons.  
Pour s'abandonner à d'agréables détentes,  
Et au bureau laisser nos préoccupations.

Pas d'inquiétude pour nos systèmes d'information,  
Car ils sont bien blindés par toutes sortes de mesures  
Techniques et au niveau de l'organisation ;  
Qui ensemble, de la sécurité nous assurent.

Tous nos équipements sont surveillés de près  
Par la supervision de leur sécurité  
Tous les incidents donc, peuvent être anticipés.

En cas de crise majeure, déjà est préparé  
Par des exercices, le secours informatique.  
Nous avons traités tous les risques analysés.

### AGENDA

#### 9<sup>th</sup> ICCC - Jeju, Corée du 23 au 25 septembre 2008

La 9<sup>ème</sup> conférence internationale sur les Critères Communs est organisée par la Corée ; elle regroupera autour des 24 pays signataires de l'accord de reconnaissance, les industriels, laboratoires et organismes de certification qui démontrent la sécurité des produits par l'application de ces critères.

➤ **Plus d'infos** : <http://www.9iccc.kr>

#### Cartes & IDentification 2008 - Villepinte, France du 4 au 6 novembre 2008

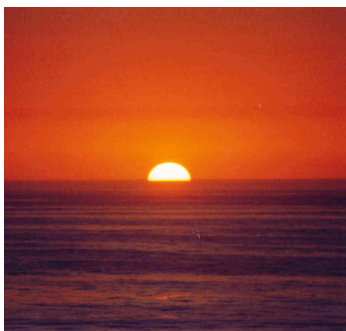
Pour la 23<sup>ème</sup> année le salon Cartes et IDentification aura lieu en novembre prochain, il regroupera les principaux acteurs du domaine avec plus de 500 exposants.

➤ **Plus d'infos** : <http://fr.cartes.com>

#### InfoSecurity France - Paris, France les 19 et 20 novembre 2008

Pour la 9<sup>ème</sup> année le salon Infosecurity accompagne le marché de la sécurité des systèmes d'information dans son développement, il se déroulera cette année Porte de Versailles à Paris.

➤ **Plus d'infos** : <http://www.infosecurity.com.fr/>



## ACTUALITÉS

### DCRI Le FBI à la française

La Direction Centrale du Renseignement Intérieur créée officiellement le 1<sup>er</sup> juillet 2008, se veut un "FBI à la française" en matière de renseignement. Forte de 4.000 fonctionnaires, dont 3.000 policiers dits "actifs", la DCRI traitera de quatre missions principales qui relèvent de l'intérêt de la nation :

- la lutte contre l'espionnage et les ingérences étrangères ;
- la lutte contre le terrorisme ;

- la protection du patrimoine et la sécurité économique ;
- la surveillance des mouvements subversifs violents et des phénomènes de société précurseurs de menaces.

Les policiers de la DCRI, dotés de l'habilitation "secret défense", seront implantés par zone dans chaque département. 175 commissaires, soit 10% de l'effectif total, y seront affectés.

Elle contribuera particulièrement à la surveillance des communications électroniques et radioélectriques susceptibles de porter atteinte à la sûreté de l'Etat ainsi qu'à la lutte, en ce domaine, contre la criminalité liée aux technologies de l'information et de la communication.

**Pour en savoir plus :**

<http://interieur.gouv.fr>



### La sécurité des impressions

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a publié un rapport qui met en garde contre les risques liés aux impressions de documents.

Son Directeur Exécutif, M. Andrea Pirotti commente : « *Le monde des affaires en Europe doit se rendre compte qu'imprimer et photocopier n'est plus*

*aussi sûr que lorsque Gutenberg a réalisé ses premières impressions il y a 540 ans. Maintenant que même les imprimantes peuvent être attaquées, les biens les plus critiques des entreprises et leurs données confidentielles sont en jeu.* »

Ce rapport rappelle que la sécurité de l'information doit considérer les informations non seulement dans les

systèmes informatiques mais également lorsque l'information se matérialise sur du papier.

**Pour en savoir plus :**

[http://www.enisa.europa.eu/doc/pdf/ENISA\\_secure\\_printing.pdf](http://www.enisa.europa.eu/doc/pdf/ENISA_secure_printing.pdf)



### Nouveaux guides de sécurité

L'Institut national des normes et de la technologie américain (NIST) a publié ce mois-ci des guides susceptibles d'améliorer nos pratiques de sécurité :

- Guide pour la sécurité de Bluetooth (SP 800-121) ;
- Recommandations pour les applications utilisant des

algorithmes de hachage approuvés (SP 800-107) ;

- Conseils pour les Firewalls et les politiques de filtrage (SP 800-41) ;
- Guide pour VPN SSL (SP 800-113) ;

- Conseil pour la sécurité des PDA et des téléphones portables (SP 800-124).

**Pour en savoir plus :**

<http://csrc.nist.gov>



### DNS La faille à rebondissement

Le bulletin d'alerte du 8 juillet dernier annonçait des défaillances dans le protocole du DNS. Certaines implémentations de ce protocole peuvent rendre les systèmes concernés vulnérables à des attaques sur le cache du DNS. Cette alerte ne donnait pas les détails techniques pour mettre en œuvre cette attaque.

Suite à cette annonce des correctifs ont été publiés pour prévenir ou restreindre les possibilités d'attaques.

Depuis le 21 juillet, des informations techniques sur la mise en œuvre de cette attaque ainsi que des programmes exploitant ces informations ont fuitées de manière prématurée par rapport à

l'exposé qui devait être fait à la conférence Black Hat.

**Pour en savoir plus :**

<http://www.us-cert.gov/>

## VEILLE

### **S**upervision Sécurité et Microsoft System Center Operations Manager 2007

Dans le cadre d'un parc de serveurs assez large ayant des rôles hétérogènes, la complexité des systèmes rend indispensable la mise en place d'une solution de supervision complète. Cette solution de supervision assure l'audit en temps réel des serveurs dans la prévision d'un incident ou d'une action d'investigation par exemple. Cet article présente d'une part l'audit d'événements de sécurité et, d'autre part, l'outil System Center Operations Manager 2007 (SCOM 2007) de Microsoft comme illustration de cette supervision globale.

#### Le traitement de l'information

La surveillance de la sécurité du système d'information s'appuie sur les données issues des différentes actions réalisées par les systèmes (ainsi que par les équipements réseau mais ceux-ci n'entrent pas dans le cadre de cet article). Cette surveillance est permise par le traitement et l'exploitation de ces données traitées de la façon suivante :

- **La collecte** : elle s'effectue à l'aide d'agents (programmes installés sur les clients dans une architecture client/serveur) présents ici sur les machines à auditer. Ils permettent de récupérer les données contenues dans des bases et/ou dans des fichiers de logs. A ce niveau, il est possible de définir des filtres sur les éléments à récupérer ;
- **L'agrégation** : les informations récupérées lors de la collecte sont prises en charge par les composants d'agrégation ; ceux-ci ont pour rôle de les rassembler et de les transférer vers le composant de consolidation des données ;
- **La consolidation** : le composant chargé de la consolidation stocke dans ses bases de données tous les événements reçus du composant en charge de l'agrégation. La consolidation permet d'exploiter les données, c'est-à-dire d'obtenir des rapports, des statistiques, des alertes, etc. A ce niveau, il est possible d'utiliser des outils annexes dédiés pour faire du reporting ou de l'administration par exemple ;
- **La corrélation** : elle consiste à traiter l'information de manière intelligente. Les données sont issues généralement du composant chargé de la consolidation. Corrélées, les données issues de la consolidation, peuvent révéler des choses *intéressantes* comme la découverte d'une attaque précise suite à une succession d'événements particuliers.

La supervision d'un Système d'Information comporte les 3 étapes « Collecte », « Agrégation » et « Consolidation ». Si l'on souhaite réaliser un monitoring plus fin, un outil de corrélation peut être ajouté ; son comportement reposera sur un système de règles et aura une certaine *intelligence* (voir l'article d'août 2006 sur les SIMS par exemple).

#### La classification des données

Avant de se lancer dans le déploiement d'une telle solution, il est important de commencer par identifier clairement les informations à auditer. En effet, le choix de l'outil, la définition de l'architecture, l'installation des composants et leurs configurations dépendent fortement de la quantité et du contenu des données à traiter.

Plutôt que de définir directement les informations à collecter, il convient de se poser les bonnes questions afin d'aiguiller les choix en fonction des contraintes et des exigences de l'entreprise :

- Quel est **le but de la collecte** ? : détection d'attaque, statistiques, rapport d'audit, demande normative, reporting ... ;
- Quel est **l'existant** ? : solution de supervision déjà mise en place, logs déjà centralisés, alertes déjà remontées, incidents déjà traités ... ;
- L'entreprise est-elle **exposée** ? : accès Internet, serveurs applicatifs en frontal, accès VPN... ;
- L'entreprise est-elle **ciblée** ? : quel est le nombre d'incidents détectés ? Quelle est la criticité de ces incidents ? ;
- Quelles sont **les moyens mis à disposition** ? : Espace disque, bande passante, et autres performances matérielles ;
- Quelle est **la nature des données** transitant sur les réseaux de l'entreprise ? : informelle, critique, confidentielle ...

La liste des critères ainsi établie doit être classifiée par priorité selon leur catégorie et leur sévérité pour les traiter de la manière la plus efficace. En effet, un événement qui implique une attaque sur un réseau doit être traité en priorité tandis qu'une alerte issue d'une modification d'un fichier de configuration pourra sûrement être prise en compte plus tard.

Les catégories peuvent être par exemple :

- Les **contrôles d'accès** (ex : les tentatives de connexion) ;
- La sécurité de **l'administration** des serveurs (ex : gestion du domaine) ;
- La sécurité des **ressources** (ex : l'accès aux données sensibles) ;
- La sécurité des **traces** (ex : les règles de traçage).

Concernant la criticité des données, trois niveaux (au moins) sont pris en compte :

- Le **niveau critique** demande une action urgente pour éviter un risque de compromission et de propagation ;
- Le **niveau intermédiaire** concerne les événements à traiter dès que possible

et les preuves dans le cadre d'une investigation ;

- Le **niveau basic** pour les autres événements qui peuvent apporter les éléments nécessaires à une action d'investigation ou d'identification d'incident de sécurité général.

A la fin de cette étape, l'entreprise dispose d'une matrice d'événements qui fait ressortir la qualification et l'importance des informations à traiter.

#### Le choix de l'architecture

Pour la suite de cet article, l'outil Microsoft System Center Operations Manager 2007 va nous servir d'exemple comme outil de mise en œuvre de la supervision en prenant en compte les principes énoncés précédemment.

Le choix de l'architecture est déterminé en premier lieu sur les composants à mettre en place. Ici, nous nous attachons seulement à traiter les événements de sécurité.

SCOM 2007 propose plusieurs types de composants. Les composants suivants sont ceux qui assurent un rôle nécessaire pour mettre en place la solution de supervision de la sécurité :

- Le **Root Management Server (RMS)** : ce composant est indispensable. C'est le point central de l'architecture d'où seront en particulier déployées les configurations ;
- Le **Management Server (MS)** : rôle intermédiaire entre le RMS et les agents (ou le rôle Gateway Server). Il consolide les informations ;
- L'**Audit Collector Server (MS-ACS)** : il s'agit d'un MS particulier, chargé de traiter les informations de sécurité. Les ACS sont reliés à une base de données dédiées aux événements de sécurité, l'Audit Database ;
- Le **Gateway Server** : ce rôle est une passerelle qui permet notamment de traverser des zones réseaux en assurant la sécurité des communications. A ce niveau, nous parlons d'agrégation de l'information. Le Gateway Server joue aussi un rôle pour limiter le nombre de connexion vers les rôles MS ou RMS ;
- Les **Agents** : ils ont pour but de superviser les serveurs ou les postes de travail. Même s'ils sont présentés comme n'étant pas indispensables, le mode sans agent est déconseillé d'un point de vue de la sécurité. (En effet, le mode sans agents utilise des flux RPC et DCOM non protégés.) Une fois l'agent installé, nous pouvons configurer des **Management Packs (MP)**, modules dédiés à la supervision de machines particulières (il existe par exemple un **MP Exchange 2007**).



Une fois les composants sélectionnés, l'architecture doit être mise en place de façon à ce que les flux soient optimisés et protégés. Les grandes étapes sont :

- Installer un rôle MS-ACS pour chaque zone cloisonnée du périmètre afin de s'assurer que tous les évènements souhaités sont collectés ;
- Relier chaque MS-ACS à une base Audit Database dans le même sous-réseau ;
- Installer chaque MS-ACS sensible en cluster ;
- Relier les MS-ACS à un RMS. Celui-ci devant être dans une zone sécurisée puisqu'il contient l'ensemble des évènements de l'entreprise ;
- Installer le rôle Gateway Server avant de traverser un pare-feu. Ainsi, une seule connexion doit être ouverte entre les deux zones ;
- Installer des agents sur les serveurs et les machines à auditer ;
- Eviter le déplacement d'information sensible ;
- Eviter la transmission d'information sur des réseaux externes ou non sécurisés (cas des entreprises internationales).

Le schéma suivant permet d'illustrer l'organisation des composants de la solution :

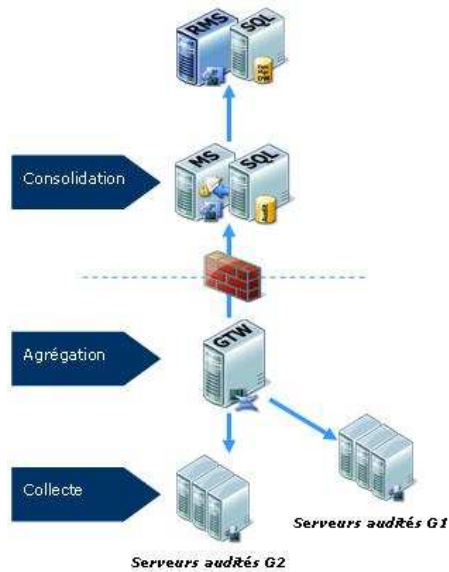


Figure 1: Composants de la solution SCOM 2007

### La sécurité des échanges

L'architecture du système étant en place, il faut s'assurer que les actions entre chaque composant sont correctement sécurisées. Des méthodes d'authentification fortes et

des flux *chiffrés* permettent de garantir l'intégrité et la confidentialité des données.

Par défaut, les authentifications reposent sur le protocole *Kerberos v5*. Il est également possible de mettre en place une authentification mutuelle basée sur *SSLv3*. Dans les deux cas, un certificat doit être installé sur chacun des composants impliqués. Par exemple, dans le cas d'un échange agent / MS, nous installerons un certificat sur chacun pour nous assurer qu'une machine non autorisée ne se substitue au MS. De même, seuls les agents identifiés peuvent de cette manière remonter des informations vers le MS. Dans le cas où les agents et le MS ne sont pas installés dans un même domaine, l'authentification via *Kerberos* n'est plus possible. Par conséquent, seul *SSL* peut apporter la sécurité suffisante.

Si l'entreprise fait le choix de mettre en place une authentification avec *SSL*, il est recommandé d'utiliser les certificats de la *PKI* existante. En effet, ces certificats sont plus sûrs que des certificats auto-générés et auto-signés. Il est également possible d'acheter un certificat tiers auprès d'une autorité de certification.

Le schéma suivant illustre la sécurité des échanges dans le cas où deux domaines sont impliqués :

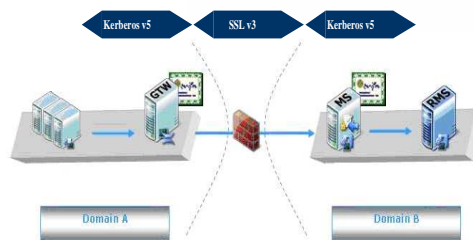


Figure 2: Sécurisation des communications

### La gestion des rôles, des comptes et des droits

Le but de cette dernière étape de sécurité est de mettre en place une politique de moindre privilège au niveau de l'infrastructure mise en place.

#### L'agent

L'agent doit disposer de droits suffisants pour récupérer les évènements de sécurité (notamment les *Event logs* de Windows par exemple). En fait, l'attribution des droits se fait sur un compte de service nommé *agent action account*. L'agent doit détenir un

compte de domaine avec uniquement les droits suivants :

- Membre du groupe *Local Users* ;
- Membre du groupe *Performance Monitor Users* ;
- Attribution du droit *Allow log on locally (Ouvrir une session localement)*.

En plus de ces droits minimaux, les droits nécessaires dépendent aussi des *Management Packs* déployés et des politiques de sécurité de l'entreprise.

Concernant le déploiement des agents, il est nécessaire d'utiliser un compte dédié avec les droits administrateurs. Ce compte devra ensuite être supprimé. En pratique, le déploiement peut être réalisé par un outil tel que *SCCM*.

#### Les serveurs

Tous les composants de la solution de supervision doivent détenir un compte de service avec des droits similaires, sans avoir à se soucier des droits nécessaires d'un *Management Pack* quelconque.

Finalement, il est nécessaire que les rôles des administrateurs au sein de l'entreprise soient clairement définis afin d'attribuer à chacun le rôle le plus juste parmi ceux proposés par *SCOM 2007*. L'organigramme suivant présente les rôles et l'importance des droits associés :



Figure 3: Rôles utilisateurs prédéfinis

Il est important de profiter de la granularité des profils proposés par la solution. En effet, cela contribue à l'application du principe de moindre privilège.

La solution que nous venons d'étudier nous montre les possibilités en termes de la supervision sécurité de l'information. Notamment, il s'agit d'assurer l'intégrité, la confidentialité et la non répudiation de l'information sur un éventail large de serveurs quantitativement et qualitativement. Cependant, il faut savoir qu'il existe de nombreuses autres solutions. Alors, le choix de l'entreprise se fera en fonction de ses besoins et de son existant. De cette manière, la solution retenue se révélera d'autant plus pertinente et augmentera la réactivité en cas d'incident et d'investigation. Il s'agit d'un critère à ne surtout pas négliger quand on sait que les environnements de production sont soumis à des SLA souvent très stricts.

## ZOOM

### Mise en pratique du secours informatique dans une entreprise

La mise en place de la continuité d'activité dans une entreprise passe par l'étape indispensable de la définition du plan de secours informatique. Le niveau de continuité assuré doit être défini en fonction des enjeux propres à l'entreprise. Pour mettre en place ce plan, chaque entreprise suit sa propre démarche en fonction de sa culture, avec son vocabulaire et son contexte opérationnel.

Une fois le plan de secours élaboré, il faut assurer sa maintenance qui passe par l'organisation régulière d'exercices de validation. Ces exercices obéissent à une logique d'évènements rapides, requérant organisation, analyse et réactivité. Cet article présente la manière dont une entreprise a conçu sa démarche d'ensemble afin d'organiser et maintenir le secours informatique.

#### Avant-propos

Face à un sinistre potentiel, il est nécessaire d'assurer la pérennité d'une entreprise. Pour cela, plusieurs actions complémentaires sont nécessaires :

- Développer un **PRA (Plan de Reprise d'activité)** ou Disaster Recovery Plan - DRP : plan prévoyant les mesures à mettre en œuvre pour faire face à une catastrophe informatique.
- Développer un **PCM (Plan de Continuité Métiers)** : Plan référençant les responsabilités, processus et opérations métiers.

L'association de ces deux plans forme un **PCA (Plan de Continuité des Activités)** ou Business Continuity Plan - BCP : Plan permettant de maintenir l'activité de l'entreprise sans interruption du service.

La démarche présentée dans cet article est spécifique dans son approche car reposant sur une succession d'exercices régulier, de la construction à la validation. Dans le contexte de l'entreprise considérée, l'objectif est la reconstruction d'une nouvelle plateforme de production à partir de matériels disponibles sur un site de repli (prêt par un fournisseur de secours, machines en réserve, serveurs d'intégration et/ou développement).

Dans ce contexte, une analyse de risques a été préalablement réalisée pour déterminer le périmètre informatique à secourir. Les résultats de cette analyse sont les préalables à l'établissement du PRA qui sera testé régulièrement afin de s'assurer de sa pertinence et son adéquation aux contraintes opérationnelles. Les résultats de ces tests permettent l'élaboration de plans d'actions pour maintenir le PRA à jour.

#### Premier exercice

Le premier exercice de secours sert à créer toutes les procédures écrites et vérifier qu'elles sont opérationnelles : procédures logistiques (gestion du site de secours, livraison de bandes, ...), documentations de reconstruction technique et fiches de validation techniques et fonctionnelles.

L'objectif lors de cet exercice est de s'assurer que tout a été prévu et noté pour rétablir la plateforme secourue dans des délais maîtrisés.

Les éléments à préparer se répartissent selon un volet technique et un volet organisationnel.

#### Volet infrastructure technique

##### Le site de repli

Une salle blanche avec accès sécurisé, puissance électrique suffisante, téléphone, réseau informatique, climatisation informatique...

Une salle des opérations techniques pour la réception des équipes techniques (bureaux, téléphone, fax, imprimante, réseaux informatiques, PC de travail, stations et Terminaux X éventuels, ...).

Une salle de gestion de crise, indépendante, pour coordonner les opérations sans déranger les équipes techniques.

Le bâtiment doit permettre une activité en 24/7, être raisonnablement éloigné du site à secourir afin de ne pas être exposé aux mêmes risques (inondation, blocage, tremblement de terre, catastrophe naturelle ou technique, etc.). Il doit être disponible rapidement sans préavis en cas de crise, mais aussi 2 fois par an pendant une semaine minimum (durée proportionnelle au périmètre secouru) pour réaliser les exercices de secours.

##### Les matériels

Inventaire de tous les matériels nécessaire au secours avec leurs configurations exactes : modèle de serveur, processeurs, quantité de mémoire, type et volume de disques, type de réseau, système d'exploitation, ...

##### Les logiciels

Inventaire de tous les médias d'installation, fichiers de configuration utilisés en production, licences d'activation et utilisation, ...

##### La date du sinistre simulé

Il est impératif de tester la cohérence des sauvegardes en restaurant des données à une date précise, et non pas les dernières disponibles au hasard.

##### Le support

S'assurer du support technique des constructeurs et éditeurs dont on utilise les matériels et logiciels, le support applicatif des équipes en interne, le support téléphonique des experts techniques (s'ils ne participent pas à l'exercice).

##### Les procédures de reconstruction

Des procédures ad hoc ou à défaut celles d'installation utilisées lors de l'intégration avant la mise en production de la plateforme.

#### Vue d'ensemble du périmètre secouru

- Schéma des dépendances entre les serveurs reconstruits et les plateformes de restauration,
- Schéma des dépendances entre les applications, les systèmes et les intervenants.

#### L'organigramme des sauvegardes

L'identification pour chaque serveur de sa plateforme de sauvegarde et, si possible, de l'heure et de la fréquence (plan de sauvegarde détaillé).

#### Les jeux de tests applicatifs

Ces jeux permettent de démontrer que les données restaurées sont utilisables et cohérentes, avec des preuves précises à collecter (pour audits et historique).

Attention: Les licences et les locations de matériels peuvent être prévues temporairement pour l'exercice. Mais, dans ce cas, elles devront impérativement faire l'objet d'un contrat sur plusieurs mois en prévision d'un sinistre, avec une clause contractuelle de mise à disposition très rapide en situation de secours réel. L'absence de contrat à ce niveau constitue un point bloquant très gênant en situation de crise.

#### Volet organisation

##### La procédure de rapatriement des sauvegardes externalisées

Si celle-ci est réalisée par une société extérieure, prévoir une clause de livraison en un temps maximal contractualisé en 24/7 (donc quelques heures pour une livraison en région).

##### L'organigramme des responsabilités techniques

Les noms et coordonnées des intervenants sur chaque technologie et système utilisés (Windows, HP-UX, AIX, Solaris, Linux, AS400, Mainframe, Réseau, Télécom, ...), de chaque application, de chaque logiciel, administrateurs comme experts. Leur contrat de travail doit comporter une clause d'intervention en 3x8 en cas de secours réel.

##### L'organigramme des responsabilités non techniques

Les coordonnées et schéma des interactions entre les décisionnaires de production, DSI, applications métiers, clients, commanditaires, fournisseurs site de secours, infogérants, sous-traitants, concepteur(s) et coordinateur(s) du secours.

## L'annuaire

Coordonnées téléphoniques de tous les personnels impliqués (participants aux exercices comme experts et managers hors site) et du prestataire de secours ou du responsable interne du site de repli.

## Le planning des opérations

L'organisation des intervenants pendant l'exercice, points réguliers sur les opérations, points communication éventuels.

Une fois tous ces éléments techniques et organisationnels préparés, le premier exercice peut être planifié.

## La réunion de préparation

Un exercice de secours fait intervenir de nombreux participants en un temps très court : la réunion de préparation permet de synchroniser les informations de tous les intervenants et mettre en place un plan d'actions pré-exercice.

Cette réunion doit permettre de répondre aux questions suivantes :

- Quelle est la date et le lieu de l'exercice ?
- Quelle est la date exacte du sinistre simulé ?
- Avons-nous tous les éléments pour fonctionner en environnement autonome sans accès au système d'information de l'entreprise (puisque considéré comme détruit) ? (la réponse se trouvant dans les listes évoqués ci-dessus).
- Parmi les participants désignés, qui sera physiquement présent et qui interviendra à distance ?
- Si la plateforme reconstruite est testée par des utilisateurs (test dit "online"), quelle est la date de mise en ligne de l'environnement, qui préviendra les utilisateurs ? L'équipe réseau est-elle au courant ?
- Les bandes seront-elles livrées à l'avance ou demandées le jour même ?  
**Note:** Il est impératif de faire livrer toutes les bandes externalisées lors des exercices, pour s'approcher le plus possible des conditions de sinistre réel.

La réunion se termine par la mise en place d'un plan d'action listant les préparatifs à réaliser, les dates d'échéances (avant et pendant l'exercice) et les responsables.

## Pendant le 1<sup>er</sup> exercice

En termes d'effectifs, le premier exercice requiert les meilleurs profils des équipes de production, afin d'élaborer les procédures

les plus pertinentes possibles en cas de sinistre. La participation d'un intervenant expérimenté ayant la vue technique d'ensemble est nécessaire pour piloter techniquement les interventions et la résolution des incidents rencontrés.

Ce premier exercice permet de réaliser les tâches suivantes :

- Relever les caractéristiques techniques des matériels utilisés (problèmes de compatibilité concernant les firmwares et drivers), leurs fiches de maintenance.
- Déclencher, si possible en temps réel, la procédure de rappel des médias externalisés (bandes, DVD, ...). Noter l'adéquation des temps de réponse avec le temps de livraison attendu. Vérifier par la suite la bonne réception de ce qui a été demandé.
- Adapter les procédures d'installation en fonction des imprévus rencontrés. Créer les fiches de qualification technique (une par équipement reconstruit, sous forme de check-list d'une page maximum).
- Créer et afficher un tableau d'avancement global. Les équipes pourront avoir une vue d'ensemble de l'avancement des opérations.
- Organiser des points techniques sur site pour le suivi des opérations : un en début de matinée et un en fin de journée.  
Selon l'autonomie des équipes et la fréquence des communiqués aux responsables / commanditaires / utilisateurs, des points peuvent être ajoutés dans le courant de la journée. Attention toutefois à ne pas surcharger les équipes avec un suivi trop rapproché.
- Noter un suivi et un reporting des opérations : timing précis des restaurations, des incidents et des solutions.

A la fin de l'exercice, diffuser un compte rendu succinct faisant un bilan rapide de l'exercice et définissant la date du débriefing.

## Après l'exercice

Une réunion de débriefing entre tous les participants doit être organisée. L'objectif est de revenir sur les incidents rencontrés, et de proposer des solutions pour leurs résolutions

Un rapport circonstancié doit être établi. Un plan d'action doit regrouper toutes les actions correctives avec les dates d'échéance et leurs responsables.

Les preuves de tests doivent être diffusées au(x) commanditaire(s) pour signature et archivage. Les fiches de qualification formalisées doivent être signées par les intervenants.

Le coordinateur des secours archive les comptes rendus, preuves, documentations, mémos, listes d'appel mis à jour.

Le suivi du plan du plan d'action doit être mise en place, la prochaine date de test doit être déterminée.

## Déroulement d'un exercice de secours validé (2<sup>ème</sup> exercice et suivants)

Cet exercice et les suivants servent à confirmer que les moyens de reconstruction (techniques et organisationnels) sont opérationnels dans les conditions prévues.

Pour cela, les opérations doivent être chronométrées. Les écarts constatés doivent faire l'objet d'un reporting précis ainsi que les solutions à apporter. Il est préférable de modifier sur le champ les procédures, afin d'éviter tout oubli après l'exercice.

A ce stade, les procédures sont prêtes pour :

- Organiser des tests "online" (connexion d'utilisateurs à distance pour tests) ;
- Déclencher un exercice par surprise : tester la réactivité des équipes et leur résistance au stress en conditions quasi-réelles ;
- Utiliser l'environnement reconstruit en exercice comme plateforme de tests, pour préparer des tests en amont d'une action risquée en production ;
- Former les nouveaux personnels au plan de secours.

Comme pour le premier exercice, la réunion de débriefing consolidera le retour d'expérience pour mettre en place un plan d'actions correctives avant d'organiser l'exercice suivant et ainsi de suite afin de toujours mieux se préparer à l'éventuel sinistre.

Dans le cas d'un exercice "surprise", il n'y a pas de briefing des équipes. On peut toutefois choisir de prévenir un cercle restreint d'intervenants pour éviter la panique et les coûts de déclenchement (prévenir notamment le fournisseur externe de site de secours, qui considère un exercice sans préavis comme un secours réel, donc payant).

**Mettre en place un plan de secours consiste à reconstruire en quelques jours un environnement qui s'est bâti sur des années. La tâche est ardue : le coordinateur et l'ensemble des responsables impliqués doivent travailler main dans la main afin d'aboutir à un plan de secours opérationnel.**

**Bien que les contraintes de production à court terme puissent sembler prioritaires par rapport à un secours que l'on espère ne jamais déclencher, l'organisation d'un tel plan a souvent des retombées inattendues en termes de réappropriation de la production et de connaissance de son système d'information.**

## L'ESSENTIEL

### Gestion du risque, différentes approches avec MEHARI

MEHARI est une méthode de management des risques qui existe depuis plus de 13 ans. Elle est développée au CLUSIF par une équipe de spécialistes qui consacrent leurs expertises à fournir un outil de gestion de risque efficace. Leurs années d'expériences du terrain apportent l'assurance d'une démarche en corrélation forte avec la préoccupation des organisations (entreprises, administration, ...) voulant gérer le risque informatique.

Depuis la version 2007 de MEHARI, la méthode est désormais librement téléchargeable sous respect du son contrat de licence publique, conforme avec les règles de GNU GPL. Cette nouvelle façon de distribuer MEHARI est en parfaite harmonie avec le travail bénévole de ses « développeurs » et de l'esprit du CLUSIF.

Parfois perçue comme complexe, MEHARI est en réalité une véritable boîte à outils avec laquelle il est possible de choisir l'approche adaptée à son besoin.

Le schéma ci-dessous présente la variété des démarches qu'il est possible d'entreprendre ; de la plus simple, l'audit des services de sécurité qui met en évidence les vulnérabilités du SI à la plus avancée qui recherche l'ensemble des situations de risque, par la détection des risques critiques.

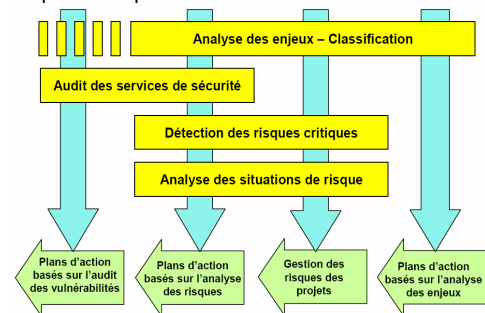


Figure 4: démarches de MEHARI / copyright CLUSIF

### Présentation synthétique des différentes démarches

Les quatre démarches présentées ci-dessous et schématisées à la figure 1 « les différentes démarches de MEHARI », permettent d'approcher le risque sous des angles très différents, suivant la préoccupation :

- Vision stratégique d'analyse des enjeux ;
- Vision pragmatique d'audit des pratiques de sécurité de l'organisation cible ;
- Vision ciblée, orientée vers un risque particulier ;
- Vision globale, afin de mettre en évidence l'ensemble des situations de risque.

Chacune des démarches est synthétisée ci-après.

#### Démarche d'analyse des enjeux et Classification

Cette démarche met l'accent sur la perception stratégique des enjeux liés à la problématique de risque des systèmes d'information.

« Les enjeux de la sécurité ne sont pas d'accroître les opportunités de gains, mais de limiter les possibilités de pertes ... »

#### Objectif

Il s'agit d'analyser les enjeux de la sécurité : « Que peut-on redouter et si cela devait arriver, serait-ce grave ? »

#### Démarche

Les étapes sont les suivantes :

- Mise en évidence des dysfonctionnements redoutés ;
- Evaluation de la gravité de ces dysfonctionnements, sous forme d'échelle de valeur des dysfonctionnements avec :
  - Description des types de dysfonctionnement,
  - Définition des paramètres influant sur la gravité,
  - Définition des seuils de criticités sur une échelle de valeurs.
- Classification des informations et des ressources SI selon les critères de disponibilité, d'intégrité et de confidentialité.

L'approche « Analyse des enjeux - classification » permet d'identifier les enjeux métiers liés au système d'information et de réaliser l'échelle de classification des dysfonctionnements redoutés.

#### Démarche d'audit des services de sécurité

L'audit des services de sécurité consiste à vérifier en fonction d'un référentiel, la base de connaissance MEHARI dans le cas présent (Il est possible de créer ses propres bases de connaissance), la conformité à un ensemble de service de sécurité.

Un service de sécurité, dans la terminologie MEHARI, est une réponse à un besoin de sécurité. Il est lui-même subdivisé en sous services de sécurité.

#### Objectif

L'objectif de l'audit des services de sécurité est la mise en évidence des vulnérabilités du système d'information.

#### Démarche

Le diagnostic des services de sécurité se réalise au travers d'un questionnaire d'évaluation des services de sécurité.

Chaque service de sécurité est mesuré en fonction des réponses aux sous services le composant.

Les paramètres d'évaluation sont les suivants :

- L'efficacité
- La robustesse
- La mise en contrôle

L'approche « audit des services de sécurité » est une démarche naturelle d'évaluation des vulnérabilités du système d'information de l'organisation cible de l'étude. C'est une démarche pragmatique,

souvent considérée indispensable. Elle permet de faire l'état des lieux à un instant donné.

#### 3<sup>ème</sup> démarche : Analyse de situations de risque

L'analyse par situation de risque est une démarche qui vise à prendre en compte un dysfonctionnement et la façon dont celui-ci va survenir. Il s'agit d'une approche orientée scénario de risque.

#### Objectif

Il faut Identifier les scénarii de risques particuliers à partir de l'échelle de valeurs des dysfonctionnements.

#### Démarche

Dans la description de la première démarche, « analyse des enjeux et classification », le travail consiste à rechercher les dysfonctionnements et l'accent est mis sur les conséquences. Dans une démarche de type scénario de risque le travail est ciblé sur les causes et origines du risque, c'est-à-dire sur les circonstances conduisant au déclenchement.

Chaque scénario est décrit par :

- Le type de conséquence ;
- Le type de ressources impliquées ;
- Les types de causes pouvant conduire à la situation de risque.

Les éléments clés de cette démarche sont :

- Une situation de risque peut être caractérisée par une potentialité et un impact intrinsèques en l'absence de toute mesure de sécurité.
- La Potentialité intrinsèque et l'impact intrinsèque peuvent être évalués.
- Des mesures de sécurité peuvent venir réduire ce risque intrinsèque par le biais de facteurs significatifs de réduction de risque.
- Ces facteurs d'atténuation de risque peuvent être évalués.

Sur la base de ces éléments, il est possible d'évaluer une potentialité et un impact résiduel, caractéristique du risque, et d'en déduire un indicateur de gravité de risque.

MEHARI propose des outils d'assistance tout au long de ce processus d'analyse et d'évaluation.

L'approche par « Analyse de situations de risque » est une démarche qui sera privilégiée lorsque l'organisation cible a connaissance de un ou plusieurs risques identifiés. En effet cela permettra de concentrer l'effort de gestion sur un risque dont l'exposition est particulièrement forte.



## ☞ Démarche de détection des risques critiques

### Objectif

Il s'agit d'identifier l'ensemble des scénarii de risques pesant sur l'organisation étudiée.

### Démarche

La détection des risques critiques est fondée sur une démarche scénario de risque, comme pour la démarche précédente. Dans ce cas, la recherche de risques critiques est réalisée de façon systématique par :

- Une analyse des enjeux matérialisés par une échelle de valeurs des dysfonctionnements ou par une classification des ressources du système d'information,
- Une évaluation s'appuyant sur la base de connaissance de MEHARI.

L'approche par « Détection des risques critiques » est une démarche globale ou semi-globale de recherche des situations de risque. L'avantage principal est la mise en évidence des risques suivant le degré de gravité sur une échelle de 1 à 4. Le traitement des situations est réalisé prioritairement en fonction de la gravité.

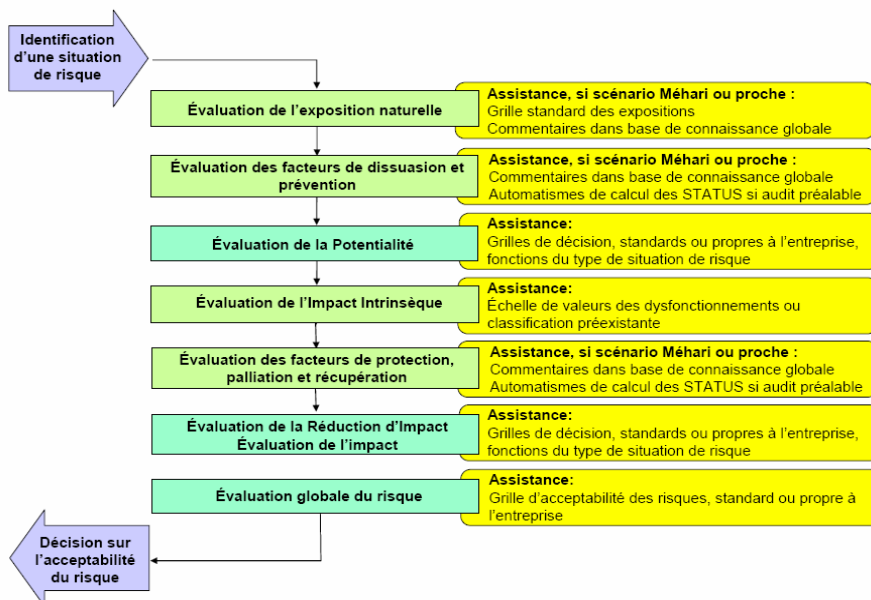


Figure 5 : démarche de l'analyse de situations de risque

### ☞ Pour aller plus loin :

- Document de référence « MEHARI 2007, principes et mécanismes » : <http://www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=METHODES>
- Télécharger MEHARI en Français : <http://www.clusif.asso.fr/fr/production/mehari/download.asp>
- Télécharger MEHARI en Anglais : <http://www.clusif.asso.fr/en/production/mehari/mehari.asp>
- Le site du CLUSIF : [www.clusif.asso.fr](http://www.clusif.asso.fr)
- Lien vers l'ensemble de la documentation MEHARI :

Cette présentation est une synthèse du document « MEHARI 2007, principes et mécanismes » présentant les différentes démarches qu'il est possible d'adopter avec MEHARI. Loin d'être une méthode d'analyse de risque monolithique, elle est une véritable boîte à outils pour le responsable sécurité ou le consultant qui adoptera la démarche correspondant au contexte du besoin.

Le choix de la démarche ou des démarches à adopter, sera fonction de l'objectif recherché. Chacune d'entre elles peut être mise en œuvre individuellement, mais également de façon complémentaire suivant la stratégie de gestion de risque adoptée par l'organisation.

Aujourd'hui l'ISO 27000, élément de normalisation des démarches SMSI, apporte un argument complémentaire à l'approche MEHARI. Loin de s'écarter de la norme, elle permet au contraire une démarche complémentaire en harmonie avec les standards de l'ISO.

**Nouveau !**

Réagissez aux articles de la newsletter sur le blog de l'ESEC :

<http://esec.fr.sogeti.com/blog>

Inscription à la Newsletter : [newsletter-subscribe@esec.fr.sogeti.com](mailto:newsletter-subscribe@esec.fr.sogeti.com)

Désinscription : [newsletter-unsubscribe@esec.fr.sogeti.com](mailto:newsletter-unsubscribe@esec.fr.sogeti.com)

### Agence ESEC

Sogeti Infrastructures Services  
6-8 rue Duret 75016 Paris - France  
Tél. : +33 (0)1 58 44 26 79  
Site : <http://esec.fr.sogeti.com>  
Mail : [esec@esec.fr.sogeti.com](mailto:esec@esec.fr.sogeti.com)

Société par Actions Simplifiées au capital de 15 999 790 € - RCS Paris 479 942 583  
Conformément à la loi « Informatique et libertés » du 6 janvier 1978, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser au directeur de l'agence ESEC.

Sogeti ne peut être tenue pour responsable en cas avéré de détournement des liens communiqués à titre d'illustration dans ses propos.

Cette newsletter a été réalisée par des consultants sécurité de l'agence ESEC.

Responsable de la publication : Edouard JEANSON

### Auteurs :

- Christian TSOTRAS
- Nicolas VINCENT
- Jérémie RENARD

Rédacteur en chef : Thomas BOUSSON

Relecteurs : François-René HAMELIN, Mojtaba FARHAT, Sylvain LABORDE, Nicolas VINCENT

Photos : Thomas BOUSSON

