TECHNICIEN SUPERIEUR TERRITORIAL

CONCOURS EXTERNE

SESSION 2010

Epreuve :

Rapport

SPECIALITE : INFORMATIQUE ET SYSTEMES D'INFORMATION

A LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET

Ce document comprend : un sujet de 1 page, un dossier de 22 pages.

- **Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni signature ou paraphe.**
- **Aucune référence (nom de collectivité, nom de personne, ...) autre que celle figurant le cas échéant sur le sujet ou dans le dossier ne doit apparaître dans votre copie.**
- **Seul l'usage d'un stylo soit noir soit bleu est autorisé (bille, plume ou feutre). L'utilisation d'une autre couleur, pour écrire ou souligner, sera considérée comme un signe distinctif, de même que l'utilisation d'un surligneur.**

Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.

Les feuilles de brouillon ne seront en aucun cas prises en compte.

SUJET NATIONAL POUR L'ENSEMBLE DES CENTRES DE GESTION ORGANISATEURS

TECHNICIEN SUPERIEUR TERRITORIAL

CONCOURS EXTERNE

SESSION 2010

RAPPORT

établi à partir d'un dossier portant sur la spécialité au titre de laquelle le candidat concourt. Cette épreuve est destinée à apprécier les capacités d'analyse et synthèse du candidat.

Durée : 3 heures
Coefficient : 2

SPECIALITE : INFORMATIQUE ET SYSTEMES D'INFORMATION

Vous êtes technicien supérieur à la Direction des systèmes d'information de la ville de Naturaville qui compte 60 000 habitants.
Face à l'ouverture des systèmes d'information sur l'extérieur et à la multiplication des outils nomades, votre responsable, la Directrice des systèmes d'information, souhaite être informée sur les risques de criticité.

Elle vous demande de rédiger à son attention, exclusivement à l'aide des documents ci-joints, un rapport sur la vulnérabilité du système d'information.

Document 1 : « TIC - systèmes d'information : la vigilance est de mise » - La Gazette des communes - 18 mai 2009 - 5 pages

Document 2 : « Sécurité des systèmes d'information - la gestion des risques » - Premier Ministre - Direction Centrale de la sécurité des systèmes d'information - 1er mars 2006 - 2 pages

Document 3 : « Un nouveau métier apparaît : le RSSI » - La Gazette des communes - 14 décembre 2009 - 2 pages

Document 4 : « Préservation des données - L'utilisateur : le maillon faible de la sécurité » - La Gazette des communes - 8 octobre 2007 - 5 pages

Document 5 : « La sécurisation des systèmes d'information des PME-PMI » - Site Internet www.e-picardie.net - 4 pages

Document 6 : « MEHARI : Méthode d'analyse de risque » - Club Sécurité des Systèmes d'information (CLUSIF) - 2 pages

Document 7 : « Utilisation de la méthode Ebios » - Université de la Méditerranée et Agence Nationale de la Sécurité des Systèmes d'Information - JRES 2009 - 2 pages

Ce document comprend : un sujet de 1 page, un dossier de 22 pages.

Certains documents peuvent comporter des renvois à des notes ou à des documents volontairement non fournis car non indispensables à la compréhension du sujet.

DOCUMENT 1

La Gazette des Communes, des Départements et des Régions
18/05/2009 N°1982

TIC - Systèmes d'information : la vigilance est de mise

Par Sophie Maréchal

- Des publics internes et externes accèdent à distance à des données sensibles.
- Des organisations mettent à niveau leur politique de sécurité, sans toutefois freiner cette évolution.

En 2008, en réaction à son licenciement pour insubordination, un administrateur de réseau bloquait, en activant un mot de passe exclusif, l'accès à 60 % des données de la ville de San Francisco. La liste des événements décrits dans le panorama annuel de la cybercriminalité présenté par le Club de la sécurité de l'information français (Clusif) réserve à chaque fois quelques sueurs froides aux responsables de la sécurité des systèmes d'information (SI). Développement des réseaux sociaux, essor du piratage des circuits électroniques, erreurs de routage et failles de sécurité des logiciels réseaux. Leur vigilance s'accroît au fur et à mesure que le nombre d'internautes grandit et que les moyens « nomades » de se connecter se multiplient.

Parallèlement, la pression est de plus en forte sur l'administration territoriale pour évoluer vers des échanges électroniques dématérialisés avec les usagers et avec d'autres administrations. Ainsi le challenge est de trouver les parades pour ouvrir l'accès en toute sécurité à un système d'information jugé stratégique par 68 % des collectivités territoriales.

Authentification unique.

« Cette pression est la même, quelle que soit la taille de la collectivité, observe Lionnel Mourer, consultant sécurité chez Bull et membre du Clusif. Les budgets et les ressources à consacrer ne sont certes pas identiques dans une petite commune ou un conseil général, mais aucun ne peut se dispenser d'une analyse des risques. Aujourd'hui, l'on ne traite plus ce sujet uniquement sous un angle technique, mais on met en perspective les enjeux stratégiques et les moyens utilisés. »

Selon la criticité des données à protéger, les plans d'action seront plus ou moins ambitieux. Les combinaisons de solutions seront étudiées en fonction du niveau de risque acceptable et du type d'utilisateurs concernés : personnel interne ou externe, prestataires, élus, citoyens. Le b.a.-ba de la sécurité commence par les informaticiens. Par exemple, la ville de Beauvais (Oise) a profité de la refonte de son SI pour installer un annuaire de gestion et de contrôle des accès au réseau (Wallix Admin Bastion, basé sur des logiciels libres). « Ma hantise est d'avoir quatre-vingts points de connexion par lesquels l'on peut accéder à nos ressources informatiques », confie Frédéric Dupuy, directeur des SI. Un enjeu d'autant plus fort que l'équipe informatique de la ville n'est

composée que de trois personnes pour gérer quarante serveurs auxquels accèdent à distance les prestataires extérieurs qui administrent le réseau. Le système mis en place identifie les personnes autorisées, supervise le réseau et conserve la trace de toutes les opérations réalisées au quotidien. Un seul identifiant et un mot de passe donnent accès à un certain nombre d'applications selon la nature du travail de chacun. Le système agit comme une zone tampon avec l'extérieur. « L'enregistrement de l'activité de chacun nécessite un accompagnement de l'installation de ce genre de dispositifs. Il faut montrer les avantages en termes de partage des connaissances, en particulier pour analyser la nature des incidents, reconnaît Frédéric Dupuy. Et aussi expliquer que cela devient obligatoire dans certaines applications de dématérialisation comme les factures. » Dans ce cas, la traçabilité des opérations a aussi un impact sur la fiabilité d'un système qui doit être disponible 24 heures sur 24, en particulier pour les serveurs qui gèrent les caméras de vidéosurveillance.

Outils nomades. Prudence.

La sensibilisation aux risques est la clé de la réussite des démarches de sécurité, d'autant plus en cas de déplacements. La direction des SI doit alors établir des règles strictes pour concilier la sécurité et le désir de disposer d'un bureau virtuel des élus et des cadres dirigeants.

Après avoir été sollicitée par les élus, la direction des SI du conseil général de Gironde a accepté de s'adapter au cas par cas à leurs demandes. Mais la condition sine qua non est de n'autoriser l'accès à distance que pour les matériels qu'elle achète et qu'elle équipe elle-même de logiciels. La même exigence de contrôle du matériel s'applique à Metz (Moselle), cette fois pour l'application de parapheur électronique lancée par la ville depuis 2002. Le circuit dématérialisé des courriers et bons de commande, soumis à l'approbation des cadres dirigeants et à la signature des élus, est maintenant ouvert aux connexions à distance sur ordinateur de poche et téléphone intelligent (couplé à un assistant personnel). « Nous combinons le cryptage proposé par le concepteur de la technologie "Blackberry", à l'annuaire d'autorisation de la mairie. Nous n'avons pas ajouté de certificats sur carte à puce ou sur clé USB, qui auraient alourdi le processus. Cette sécurité est suffisante compte tenu du caractère administratif du courrier qui y circule », précise Bertrand Lang, directeur des technologies de l'information et de la communication de la ville.

Coffre-fort électronique.

En revanche, l'ouverture du SI à l'usager repose essentiellement sur la mise en place de zones tampon sécurisées accessibles par une authentification unique, afin de protéger les données privées confidentielles dont la collectivité est dépositaire. Les questions de sécurité font partie intégrante des projets lors de mise en ligne de téléservices.

Le conseil général du Val-d'Oise met à disposition des communes du département la plateforme « Cap Démat », qui fournit un cadre technique pour activer une quinzaine de téléservices allant du culturel au périscolaire, accessibles par internet ou sur des bornes interactives. « L'accès des usagers, basé sur le protocole sécurisé "HTTPS" qui crypte les transactions, se fait via un identifiant et un mot de passe de huit caractères minimum,

détaille Philippe Usclade, chef de projet Cap Démat. L'accès à distance par les agents et le traitement des transactions se font aussi sur le principe de l'authentification unique couplée cette fois à l'annuaire d'autorisation interne à chaque commune. » Le citoyen dispose en outre d'un espace de stockage des pièces justificatives, dit « coffre-fort électronique », dont il est seul détenteur des codes d'accès, les agents ne visualiseront donc ces documents que lors de l'instruction d'une démarche.

Extension.

Les mêmes principes président à l'expérimentation de « mon.service-public.fr » par la communauté de communes de Parthenay (Deux-Sèvres) et Vandœuvre-lès-Nancy (Meurthe-et-Moselle), avant d'être généralisée à l'ensemble des collectivités, sous la forme d'un kit d'accès gratuit. Le concept de compte unique est étendu à tous les services locaux et nationaux. Parthenay teste, par exemple, une application « nouvel arrivant » qui permet à une famille avec enfant de s'inscrire aux services de la commune liés à l'enfance et fait le lien avec la Caisse d'allocations familiales. Ceci sans risque de recoupement de fichiers d'informations personnelles, conformément aux préconisations de la Commission nationale de l'informatique et des libertés.

Source : 2008 « Menaces informatiques et pratiques de sécurité en France », Clusif.

Un recueil de bonnes pratiques

Le référentiel général de sécurité (RGS) recense les bonnes pratiques en la matière pour les systèmes d'information (SI). Il propose une démarche globale d'analyse et de prise en compte de la sécurité. L'objectif est d'aider à définir un niveau de sécurité en phase avec l'état de l'art et le contexte de l'administration concernée. Le RGS propose une liste de produits et services certifiés, qui sera actualisée régulièrement pour s'adapter aux nouvelles vulnérabilités d'Internet. Prévu par l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques, le décret d'application du RGS est en cours d'examen au Conseil d'Etat, pour une publication attendue au deuxième trimestre 2009. La version déjà approuvée par la Commission européenne est en ligne sur www.references.modernisation.gouv.fr/rgs-securite

LES CHIFFRES CLÉS

- 30 % des collectivités ont formalisé une politique de sécurité de l'information.

- 42 % interdisent la connexion des appareils mobiles même sous contrôle (contre 13 % dans le secteur privé).

- 95 % ont installé des antivirus, 82 % des antispam, 87 % des pare-feu, mais seuls 40 % utilisent l'authentification forte par certificat.

- 69 % sont en conformité totale avec la loi « informatique et libertés » (64 % dans le secteur privé).

- 42 % ont réalisé une analyse globale ou partielle des risques liés à la sécurité du SI.

Loire-Atlantique - Un processus d'amélioration continu de la sécurité

C'est à la suite d'une mise à niveau des micro- ordinateurs au conseil général de Loire-Atlantique qu'une perte de confidentialité sur certaines données est apparue. Première réaction : un audit technique est commandé. Mais, rapidement, la direction générale des services comprend que le sujet mérite de sortir du seul champ de la direction des SI.

Enjeu stratégique.

La protection et la disponibilité des données sont en effet devenues pour le conseil général un enjeu stratégique, compte tenu de l'évolution vers l'e-administration de ses nombreux métiers. Ainsi, dès 2005, une démarche globale de management de la sécurité des SI est engagée, s'inspirant des méthodologies de la norme ISO 27 000 qui définit les exigences de ce type de dispositif. « Jusqu'à présent, l'on sécurisait l'informatique sans savoir si cela correspondait aux enjeux des métiers. Il était nécessaire de penser différemment en définissant un plan d'action axé prioritairement cette fois sur les métiers », confie Nicolas Bunoust, responsable de la sécurité du système d'information, dont le poste est créé à cette occasion pour animer la démarche. Parallèlement, un comité sécurité du SI (Cosi), présidé par la directrice générale adjointe des ressources, Madeleine Goineau, est organisé. Il est le lieu d'échange des services directement concernés par le partage des données : informatique, juridique, moyens généraux, ressources humaines et directions opérationnelles. Il est aussi l'endroit où se décident les actions à lancer.

Niveaux de criticité.

Leur premier exercice a été de définir les objectifs de sécurité, en estimant, par exemple, des niveaux de criticité des applications de 1 à 4, ou en analysant l'impact de pertes ou de fuites d'information. Des actions en ont découlé comme l'organisation d'un plan de continuité d'activité. Une salle de secours a été installée à 1 km du site central de production et accueille l'ensemble des sauvegardes. Le Cosi a dressé la liste des vingt applications qui doivent redémarrer en moins de cinq jours si un sinistre détruit la salle informatique (par exemple, le système de surveillance des ponts, 24 heures maximum ; la messagerie interne 48 heures). La sensibilisation des 4 000 agents est aussi au cœur du dispositif. Un guide de conduite du système a été élaboré à leur intention (« Les 14 réflexes de la sécurité informatique ») et différentes actions pédagogiques accompagnent sa diffusion. Au total, un plan de 50 mesures opérationnelles est planifié sur quatre ans, avec une évaluation et un réajustement des objectifs tous les six mois.

TÉMOIGNAGE - François Fouillet, DSI de la communauté de communes Parthenay (Deux-Sèvres) - « Un sas de sécurité entre notre site et les citoyens »

« Nous expérimentons la plateforme mon.service-public.fr [*] pour offrir aux Parthenaisiens un accès cohérent aux téléservices locaux et nationaux. Nous bénéficions ainsi d'une plateforme nationale puissante qui garantit la sécurité des transactions grâce à un ensemble de mécanismes, comme la fédération d'identité. Le citoyen dispose d'un compte unique et d'un mot de passe, il bénéficie d'un espace dédié, autrement dit un coffre-fort électronique où il stocke tous ses documents scannés ou sous format électronique.

Ce sas entre la mairie et le citoyen résout un certain nombre de points de sécurité qui impliqueraient une organisation et des investissements financiers au-dessus de nos moyens. Nous pouvons nous consacrer au suivi de nos téléprocédures, à l'organisation interne des informations transversales et rester vigilants au respect de la loi "informatique et libertés". »

CONTACTS

- Nicolas Bunoust, responsable de la sécurité du système d'information de Loire-Atlantique, tél. : 02.40.99.11.93.

- François Fouillet, DSI de Parthenay, tél. : 05.49.94.90.00.

- Bertrand Lang, directeur des technologies de l'information et de la communication de Metz, tél. : 03.87.55.51.10.

RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale
de la sécurité des systèmes d'information

Sécurité des systèmes d'information

La gestion des risques

Le risque

Le risque[1] de sécurité des systèmes d'information (SSI) est une combinaison d'une menace et des pertes qu'elle peut engendrer.

La menace SSI peut être considérée comme un scénario envisageable, avec une certaine opportunité (représentant l'incertitude).

Ce scénario met en jeu :

- une méthode d'attaque (action ou événement, accidentel ou délibéré),
- les éléments menaçants (naturels ou humains, qui agissent de manière accidentelle ou délibérée) susceptibles de l'employer,
- les vulnérabilités des entités (matériels, logiciels, réseaux, organisations, personnels, locaux), qui vont pouvoir être exploitées par les éléments menaçants dans le cadre de la méthode d'attaque.

Les pertes sont généralement estimées en termes d'atteinte des besoins de sécurité des éléments essentiels (le patrimoine informationnel et les processus associés) et d'impacts induits sur l'organisme.

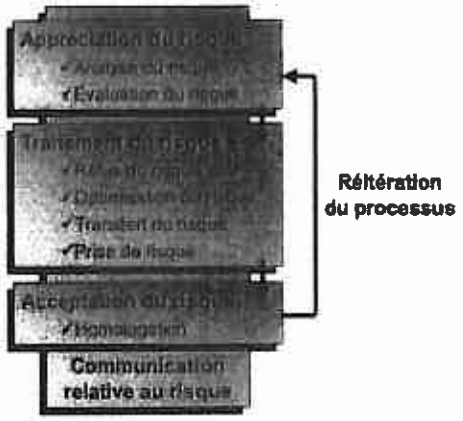
Exemple de risque décomposé :

Méthode d'attaque	***piégeage** du logiciel (introduction d'un ver)*
Élément menaçant	***un** pirate expérimenté engagé par **un concurrent***
Entité	***réseau** WiFi*
Vulnérabilité	*possibilité d'administrer **le** réseau à distance*
Opportunité	*jugée moyenne*
Atteinte des éléments essentiels	*atteinte à la confidentialité (vol d'informations)*
*Impact **sur l'organisme***	***perte** d'avantages **concurrentiels***

[1] Le vocabulaire lié au risque et à la gestion des risques SSI est décliné du Guide ISO 73 – *Management du risque – Vocabulaire – Principes directeurs pour l'utilisation dans les normes* – International Organization for Standardization (ISO) (2002).

La gestion des risques

La gestion des risques SSI consiste à coordonner, de manière continue, les activités visant à diriger et piloter un organisme vis-à-vis des risques. Elle inclut l'appréciation, le traitement, l'acceptation et la communication relative aux risques SSI.



L'appréciation des risques

L'appréciation des risques SSI représente l'ensemble du processus d'analyse (mise en évidence des composantes) et d'évaluation du risque (estimation de leur importance).

L'appréciation des risques consiste tout d'abord à décrire le contexte : l'organisme, le système d'information (SI), les éléments essentiels à protéger (informations, fonctions...), les entités sur lesquelles ils reposent, les enjeux liés au SI, les contraintes à prendre en compte...

Les besoins de sécurité des éléments essentiels doivent ensuite être exprimés (couramment en termes de disponibilité, d'intégrité et de confidentialité).

Les menaces pesant sur le SI doivent être identifiées et caractérisées en terme d'opportunité (représentant l'incertitude de ces menaces).

Les risques doivent enfin être déterminés en confrontant les menaces aux besoins de sécurité.

Le traitement des risques

Le traitement des risques SSI représente le processus de sélection et de mise en œuvre des mesures visant un refus, une optimisation, un transfert ou une prise de risque.

Il consiste tout d'abord à identifier les objectifs de sécurité en déterminant le mode de traitement (refus optimisation, transfert ou prise de risque) et en tenant compte des éléments du contexte. Ces objectifs représentent un cahier des charges exprimant la volonté de traiter les risques et ne préjugeant pas des solutions à mettre en œuvre.

Le traitement des risques se poursuit par la détermination d'exigences de sécurité, techniques ou non, satisfaisant les objectifs de sécurité identifiés et décrivant la manière de traiter les risques (dissuasion, protection, détection, récupération, restauration, compensation...).

Enfin, les mesures de sécurité, techniques ou non techniques, spécifiées par les exigences de sécurité peuvent être mises en œuvre.

À l'issue, les risques ont été soit réduits, soit transférés (vers des tiers) et un ensemble de risques résiduels peut subsister. Il convient de les mettre en évidence et d'exprimer explicitement le choix de prendre ces risques.

L'acceptation des risques

L'acceptation des risques SSI représente la décision d'accepter les risques traités.

Cette activité consiste en une homologation de sécurité. Elle est prononcée pour une durée déterminée, par une autorité d'homologation, qui doit être désignée et qui peut se reposer sur une Commission d'homologation qu'elle préside.

L'homologation de sécurité se base sur un dossier de sécurité dont le contenu doit être défini. Généralement, il est composé de l'étude des risques SSI, d'un document faisant état des objectifs de sécurité, d'une cible de sécurité précisant les exigences de sécurité et de la politique de sécurité (avec éventuellement ses documents d'application).

La communication relative aux risques

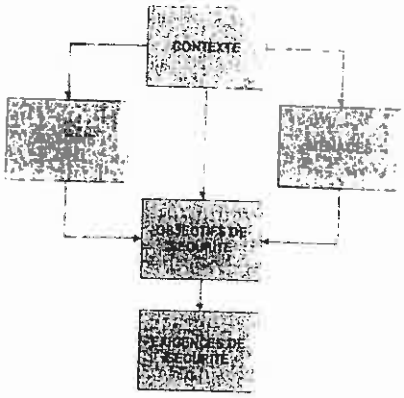
La communication relative aux risques SSI représente l'échange ou le partage d'informations concernant les risques.

La gestion des risques SSI doit être considérée comme un processus continu et itératif.

EBIOS : la boîte à outils de gestion des risques SSI

La méthode EBIOS et son logiciel

EBIOS (Expression des Besoins et Identification des Objectifs de sécurité) est la méthode de gestion des risques SSI diffusée gratuitement par la DCSSI.



Elle permet d'apprécier les risques SSI, de contribuer à leur traitement en spécifiant les exigences de sécurité à mettre en œuvre, de préparer l'ensemble du dossier de sécurité nécessaire à l'acceptation des risques et de fournir les éléments utiles à la communication relative aux risques.

EBIOS est actuellement employée dans le secteur public, dans le secteur privé, en France et à l'international.

Le logiciel libre EBIOS permet de suivre la démarche méthodologique, de personnaliser des bases de connaissances et de produire des livrables appropriés.

Par ailleurs, le Club EBIOS assure la pérennité de la méthode et des outils associés. Il réunit les experts du secteur public et du secteur privé en gestion des risques SSI.

Enfin, le centre de formation de la DCSSI propose des séances d'information et de formation sur la méthode EBIOS aux agents de l'État.

Informations et contacts

ebios.dcssi@sgdn.pm.gouv.fr
conseil.dcssi@sgdn.pm.gouv.fr
http://www.ssi.gouv.fr/fr/confiance/methodes

© 2006 SGDN / DCSSI. Tous droits réservés. Imprimé en France

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 15 - Fax 01 71 75 84 00

SÉCURITÉ DES SYSTÈMES D'INFORMATION

Un nouveau métier apparaît : le RSSI

- La fonction de responsable sécurité du système d'information (RSSI), encore rare, devrait croître dans les collectivités.
- Le plus souvent, les agents sont recrutés au sein de la direction des SI.

Installer des pare-feu, des antivirus et des antispam ne suffit pas à assurer la sécurité d'un système d'information. Les collectivités les plus averties, qui ont compris que cette dernière n'était pas qu'une affaire d'informaticiens, commencent ainsi à nommer des responsables sécurité du système d'information (RSSI). Leur mission : avoir une vision globale de la sécurité de la collectivité et faire des propositions pour l'améliorer en prenant en compte les processus et la dimension métier des différents services. Car « tout projet de dématérialisation renforce la dépendance des métiers au système d'information et modifie les risques et les vulnérabilités », explique Nicolas Bunoust, RSSI au conseil général de la Loire-Atlantique. « Nous avons énormément de projets qui nous obligent à ouvrir notre système aux partenaires, aux prestataires, aux citoyens, etc. Nous ne pouvons plus fonctionner en bulle fermée », ajoute Christophe Forgin, responsable sécurité et architecture du système d'information au conseil général de la Mayenne.

Méthodes. Le travail du RSSI consiste à recenser les menaces qui pèsent sur le système d'information, ses vulnérabilités et proposer les mesures à déployer pour limiter ces risques. Pour cela, il dispose de méthodes telles que l'ISO 27 000, Ebios ou Mehari. « Ce responsable définit la planification, effectue les contrôles et propose les améliorations. Le danger pour lui serait de plonger dans la mise en œuvre au quotidien », estime Thierry Henniart, RSSI de la région Nord-Pas-de-Calais. En théorie, il ne devrait pas s'occuper du déploiement et de l'exploitation des outils de sécurité. Mais notamment pour des raisons budgétaires, parfois il s'en charge tout de même. Ainsi, moins de 6 % des collectivités en ont recruté un à plein temps. « A Reims, c'est un rôle qui est partagé entre différentes personnes : mon adjoint, un coordinateur et moi-même, explique David Mercier, DSI de la ville et de Reims métropole. Actuellement, chaque cellule travaille sur le sujet. »

« En parallèle, le RSSI fait également beaucoup de sensibilisation auprès de la direction et des utilisateurs. Nous ne sommes pas là pour les empêcher de travailler, mais pour trouver les meilleures solutions pour sécuriser l'information », résume Thierry Henniart. C'est aux services utilisateurs de définir leurs objectifs. Ensuite, le responsable adaptera le bon niveau de sécurité par rapport à ceux-ci. « Si on a une vision uniquement technique de la sécurité, on peut avoir tendance à sur-sécuriser. Mais on peut ainsi imposer trop de contraintes aux agents », prévient Nicolas Bunoust. « Avant de faire l'analyse de risques

AVIS D'EXPERT — Lionel Maurel, directeur d'ESR Consulting, chargé de l'enquête du Club de la sécurité de l'information français (Clusif) sur les pratiques de sécurité des collectivités

« Le rattachement à la direction informatique n'est pas idéal »

« La fonction de RSSI n'est clairement identifiée que dans 22 % des collectivités que nous avons interrogées [*], contre 37 % pour les entreprises privées. La plupart du temps, c'est le DSI qui occupe ce poste [37 % des cas] ou le responsable informatique [31 %]. Seul un quart des RSSI, quand ils existent, occupe cette fonction à plein-temps. Ceux qui travaillent dans les collectivités sont le plus souvent rattachés à la DSI [60 %] et parfois à la DGS [15 %], contrairement aux RSSI du privé dont 45 % dépendent de la direction générale et seulement 32 % du service informatique. Le rattachement à l'informatique n'est pas idéal car, en cas d'arbitrage, le DSI pourrait favoriser la production informatique au détriment de la sécurité. Lorsqu'il est rattaché directement à la DG, c'est celle-ci qui arbitre et peut jouer un rôle de contre-pouvoir. »

[*] L'étude réalisée en 2008 à laquelle près de 200 collectivités ont répondu porte sur les mairies de plus de 30 000 habitants, les CU de plus de 20 000 hab., les CA de plus de 50 000 hab., les conseils généraux et régionaux. Elle est téléchargeable sur www.clusif.asso.fr

Ce qu'ils en pensent

« La gestion de risque est une nécessité »

« Gérer la sécurité c'est se poser des questions face aux risques et voir comment les prendre en charge. Cela oblige à redéfinir des choix d'organisation et leur intégration dans le système d'information. Le RSSI voit au-delà des systèmes informatiques. C'est un métier d'avenir, car les systèmes d'information sont aujourd'hui au cœur de nos métiers. Si nous ne prenons pas, aujourd'hui, la mesure des risques, nous obérons l'avenir. La gestion de ceux-ci est une nécessité. Une fois les risques mis à jour, c'est aux métiers de décider de les réduire, transférer, éviter ou accepter. Toutefois, les impacts sont difficiles à chiffrer, car ils sont souvent immatériels. Combien coûterait la reconstitution de la comptabilité électronique ou le fait d'avoir entaché l'image de la collectivité ? »

Fabrice Marie, responsable sécurité du système d'information du département des Côtes-d'Armor

« Savoir une force de conviction et savoir mobiliser »

« Un bon RSSI, au-delà d'avoir des compétences techniques larges, doit avant tout être un communicant. Il doit savoir dialoguer avec toutes les instances de l'organisation, depuis les agents jusqu'à la direction, en sachant adapter son discours en fonction de l'interlocuteur. Ces qualités sont à compléter avec une dimension tactique. Une posture coercitive est vouée à l'échec, il faut avoir une force de conviction et savoir mobiliser les gens. En effet, la sécurité ne se vend pas du jour au lendemain. Souvent, c'est une problématique nouvelle et on ajoute une charge de travail supplémentaire aux gens des métiers. Les normes et les référentiels, type ISO 27000, m'aident beaucoup à démontrer que mes calculs de potentialité de risques sont crédibles, et ainsi être écouté. »

Benoît Dehais, chargé des systèmes d'information du département de Seine-Maritime

« La protection de l'information hors de la DSI »

« En 2006, nous avons d'abord nommé un RSSI rattaché à la DSI, afin de mettre en place la politique de sécurité du système d'information. Cependant, même s'il échangeait avec les directions métiers, sa vision était encore très "maîtrise d'œuvre". En 2008, j'ai proposé au DGS que soit créée une cellule de protection de l'information. Elle a une vision de maîtrise d'ouvrage, définit les grands principes de la protection de l'information et fixe les objectifs à atteindre en termes de sécurité. Elle communique étroitement avec le RSSI, qui est resté au sein de la DSI, et qui propose des solutions techniques et organisationnelles. En effet, la protection de l'information couvre un périmètre plus large que l'informatique, et la DSI n'est pas toujours légitime pour auditer les processus métier. »

avec les métiers, nous avions "priorisé" les actions par rapport à des a priori», reconnaît Christophe Forgin. Ainsi, croyait-il que le logiciel de paie était très "critique", alors qu'il est tout à fait possible, en cas de problème informatique majeur, de régler les salaires en se basant sur le mois précédent. En revanche, son analyse des risques conduite avec les métiers a révélé des applications critiques qu'il n'aurait pas forcément décelées seul. « Le RSSI est l'interface entre la maîtrise d'œuvre [la DSI] et la maîtrise d'ouvrage [les directions métier]. C'est un animateur qui doit donc comprendre les deux parties et se positionner en termes d'organisation, de pilotage et de gouvernance», souligne Nicolas Bunoust.

Evolution interne. Le RSSI se trouve parfois dans une situation délicate face à ses collègues de la DSI, qui estiment « savoir faire de la sécurité». Il doit pourtant les sensibiliser et les former, notamment afin qu'ils prennent en compte les problématiques dès le début des projets. La nomination du RSSI résulte souvent d'une évolution interne, car il s'agit de bien connaître les métiers de la collectivité pour occuper cette fonction. « Actuellement, il n'y a pas vraiment de filières établies, les gens se forment sur le "tas". Cela nécessite des capacités techniques, mais aussi organisationnelles. Le RSSI doit posséder une forte capacité à faire adhérer les personnes », résume Benoît Dehais, DSI au conseil général de la Seine-Maritime. Selon lui, les directeurs des systèmes d'information (SI) sont conscients de la problématique sécurité du SI, mais ils ont des difficultés à la retranscrire et à la faire passer auprès de la direction.

Cependant, ce métier a de l'avenir, car il s'avérera indispensable. Pour contourner le problème budgétaire, « il pourrait y avoir des postes mutualisés, car nombre de collectivités n'ont pas les moyens de s'offrir un technicien à plein temps», propose Fabrice Marie, qui, ayant été nommé RSSI en 2002, fait partie des pionniers !

Claire Chevrier

CONTACTS

- **RSSI à la région Nord-Pas-de-Calais**, tél. : 03.28.82.60.07.
- **RSSI au conseil général des Côtes-d'Armor**, tél. : 02.96.62.46.12.
- **RSSI au conseil général de Loire-Atlantique**, tél. : 02.40.99 11.93.
- **RSSI au** conseil général de **Mayenne**, christophe.forgin@cg53.fr
- **DSI du** conseil général **de Seine-Maritime**, tél. : 02.35.03.56.00.

La Gazette des Communes, Départements et Régions
08/10/2007 – n° 1904 supplément TIC

Préservation des données
L'utilisateur : le maillon faible de la sécurité

Par Claire Chevrier

La direction des systèmes d'information, en lien avec la DRH, doit faire adhérer les agents à sa politique de sécurité. Sans leur collaboration, rien n'est vraiment possible.

Depuis cinq ans, les différents sites et applications métiers des collectivités sont interconnectés, et leurs systèmes d'information sont de plus en plus ouverts vers l'extérieur. Les élus peuvent se connecter depuis chez eux, certains agents possèdent des ordinateurs portables, etc. Les directions des systèmes d'information (DSI) travaillent pour garantir l'étanchéité entre les différentes applications et assurer la sécurité des données. Cependant, elles pourront bien déployer tous les équipements qu'elles voudront, si les utilisateurs - agents et élus - ne respectent pas un minimum de règles, la disponibilité, la confidentialité et l'intégrité des informations ne pourront être garanties.

Importance de l'information.

Le maillon faible d'un système de sécurité, c'est l'utilisateur et son poste de travail. Des mots de passe trop faciles à trouver, des antivirus désactivés, des informations copiées sur des clés USB, etc. sont autant de risques qu'il faut prévenir. Il est donc nécessaire de sensibiliser les agents à l'importance de la sécurité et au respect de certaines règles. « Souvent, les agents se demandent pourquoi ils devraient se préoccuper de sécurité et en quoi cela les concerne, remarque Jalal Boularbah, chef de service à la direction des systèmes d'information du conseil général du Val-de-Marne. J'essaie de leur expliquer que, lorsqu'ils utilisent le système d'information, ils sont sur une ressource mutualisée, où chacun doit participer à la sécurité pour qu'elle n'en soit que meilleure. » Sensibiliser c'est donc, d'abord, informer, car nombre d'utilisateurs commettent des erreurs par manque de connaissance. Reste ensuite à tenter d'influencer les comportements.

Sans l'adhésion des usagers, un responsable sécurité ne peut rien. Si certaines règles sont non négociables, mieux vaut utiliser la pédagogie plutôt que l'autoritarisme. Tout ce qui oblige à changer les habitudes de travail est souvent mal perçu. Une mesure aussi anodine que programmer la mise en veille automatique des postes lorsqu'ils restent inactifs pendant plus de quinze minutes peut provoquer un tollé si la DSI n'explique pas aux agents pourquoi c'est nécessaire. Les utilisateurs ne ressentent que la gêne occasionnée : ressaisir leurs codes à chaque fois. Et, s'ils n'en comprennent pas la raison, ils ont l'impression d'être brimés.

Charte de sécurité.

Une politique de sensibilisation commence souvent par la publication d'une charte sécurité. Dans certaines collectivités, les agents doivent signer cette charte, annexée au contrat de travail ou au règlement intérieur, pour obtenir leur identifiant et leur mot de passe. « C'est un moyen de s'adresser à tous les agents. Le texte rappelle les droits et devoirs de chacun, et, en annexe, reprend les bonnes pratiques recommandées. Le principe central est la responsabilisation de l'agent », explique Martin de Mijolla, DSI du conseil général des Hauts-de-Seine. Au quotidien, le centre de support, qui traite 2 000 appels par mois, renvoie dès que c'est nécessaire les utilisateurs à cette charte. Si un agent fait passer des emails qui s'apparentent à du spam (comme les chaînes de solidarité), la DSI lui rappelle que le document l'interdit.

Discours attractif.

Le lancement d'une charte peut être l'occasion d'élaborer un document synthétique résumant, par exemple, les dix grands principes à respecter : changer régulièrement son mot de passe, y introduire des chiffres, ne pas le donner à un collègue, etc. « Rédiger une charte de sécurité est un bon début. Cela permet, quand il y a un problème, d'avoir des moyens d'action juridique, mais ce n'est pas parce qu'il y a une charte que les gens vont se préoccuper de sécurité » prévient Paul Grassart, consultant en sécurité.

La DSI doit d'abord définir les thèmes sur lesquels elle veut communiquer : les virus, les mots de passe, l'usage des email, l'importance des déclarations à faire à la Commission nationale de l'informatique et des libertés (Cnil), le respect des droits d'auteur, etc. Ensuite, il existe de nombreux moyens, en collaboration avec le service de la communication interne, d'atteindre les utilisateurs. Il est possible de publier des messages sur l'intranet, d'insérer des articles dans des publications internes, d'intervenir trente minutes dans des séminaires d'accueil des nouveaux personnels, d'organiser des séminaires de sensibilisation, etc. « Il faut entretenir une relation et être à l'écoute, laisser les gens s'exprimer et expliquer que "ça n'arrive pas qu'aux autres" », estime David Mercier, directeur adjoint de la DSIT de Reims. L'objectif est de mener une véritable campagne de lobbying, et de marteler ses messages le plus souvent possible. Il est aussi possible de faire de l'information plus ciblée et plus approfondie en fonction des catégories de personnes. Il faut adapter le discours en fonction des préoccupations quotidiennes de chacun. On n'abordera pas les mêmes thèmes si l'on s'adresse à une personne du service de la voirie, au sein des écoles, à l'état civil, etc. Le discours doit être attractif. « Lorsque l'on parle de sécurité, les risques ne semblent pas concrets. Pour sensibiliser les directions, nous avons donc pris des exemples de collectivités qui, à la suite d'un problème de sécurité, se sont retrouvées en panne de messagerie électronique pendant plusieurs jours », se rappelle David Mercier.

En amont.

Autre moyen : intégrer les services dans la définition de la politique de sécurité en les faisant travailler, par exemple, sur la criticité de leurs applications. Par ailleurs, « dans chaque note de cadrage, pour les nouveaux projets, nous avons systématiquement un chapitre "sécurité", note Martin de Mijolla. Car, comme la qualité, c'est un aspect à

prendre en compte dès la conception ». Les préoccupations de sécurité sont ainsi réinjectées à chaque phase du déploiement du nouvel applicatif, jusqu'à la prise en main par les utilisateurs et leur formation.

Chantier permanent.

Cependant, ces politiques de sensibilisation sont difficiles à mener. Tout d'abord, il est encore trop rare que, dans les collectivités, une personne travaille à plein temps sur les problématiques de sécurité de l'information et possède, en plus de compétences techniques pointues, une aisance à communiquer. Ces profils sont difficiles à recruter et souvent chers. Mais, « dans la pratique, s'il n'y a pas un responsable sécurité pour impulser une politique de sensibilisation, souvent, rien n'est fait », constate Paul Grassart. Lorsque cette personne existe, elle doit, de plus, savoir travailler avec le service des ressources humaines et ne pas vouloir agir seul, sous peine de mal concevoir son plan et de manquer sa cible. La sensibilisation est une mission de RH car elle joue sur le relationnel. Son objectif est de faire acquérir aux agents et aux élus de nouvelles compétences et de changer leur comportement. Responsable sécurité et DRH doivent donc travailler main dans la main. D'autant que la sensibilisation des agents à cette sécurité est un chantier permanent : il faut travailler en continu.

Contacts

Clusif, tél : 01.53.25.08.80.

DSIT de la ville de Reims,tél : 03.26.77.32.00.

DSI du conseil général du Val-de-Marne, tél : 01.43.99.85.79.

« La protection des données doit être le souci de tous les services »

Témoignage David Mercier, directeur adjoint de la DSIT de Reims (*)

« La sécurité impose des contraintes aux agents. Toute la difficulté est de savoir où placer le curseur pour avoir un système d'information réellement sécurisé, mais sans conséquences trop lourdes pour l'utilisateur, qui l'empêcheraient de travailler. L'approche de la DSI ne doit pas être rigide, car trop de sécurité risque d'être contre-productif. Par exemple, nous n'avons pas interdit l'usage des clés USB, malgré les risques que cela comporte. La protection des données doit être le souci de tous les services. Pour une réelle efficacité, toute la chaîne doit être sûre : une porte blindée ne sert à rien si une fenêtre est restée ouverte ! Il est essentiel que tous les process liés à la sécurisation soient expliqués.

Lexique

Parfeu / firewall : outil logiciel ou matériel qui protège le réseau local d'intrusions extérieures et de piratage.

Antivirus : il repère les fichiers ou les applications contenant un virus et les bloque. Il doit être remis à jour régulièrement pour être efficace.

Antispam : limite les messages électroniques non sollicités, via des filtres sur le titre, le contenu du message, etc.

Antispyware : détecte les logiciels espions qui ont pu s'installer sur l'ordinateur pour collecter et transférer des informations à l'insu de l'utilisateur.

Les collectivités en retard

44 % des municipalités de plus de 30 000 habitants déclarent consacrer plus de 3 % de leur budget informatique à la sécurité, soit un chiffre équivalent à celui du secteur privé. Mais, si la sécurité est perçue comme un enjeu important, 42 % reconnaissent que la conduite des missions la concernant est ralentie par des problèmes budgétaires. Seules 4 mairies sur 10 ont rédigé une charte de sécurité. Le Clusif constate un déficit de communication auprès des utilisateurs et une fréquence « relativement faible » des programmes de sensibilisation. Ces derniers n'existent que dans un tiers des mairies interrogées. 80 % se présentent sous la forme de publications et 15 % sont des formations.

Une mauvaise gestion des mots de passe

Les agents ne sont pas assez sensibilisés à l'importance des mots de passe. Il n'est pas rare de les trouver inscrits sur un Post-it collé sur l'écran ou sous le clavier. Seules 10 % des boîtes à lettres électroniques du conseil général du Val-de-Marne utilisent des mots de passe complexes, mélangeant lettres et chiffres. « Les agents verrouillent la porte de leur domicile. Il faut qu'ils fassent de même avec leur poste de travail », estime Jalal Boularbah, chef de service à la direction des systèmes d'information.

« Pour être efficace, il faut agir sur les comportements des agents, dans la durée »

ENTRETIEN Paul Grassart consultant en sécurité et membre du Club de la sécurité de l'information français (Clusif)

Que faire pour que les gens se rendent aux séances de sensibilisation ?

Il est toujours possible de rendre celles-ci obligatoires, avec des sanctions à la clé, mais les participants seront réfractaires et peu disposés à collaborer. Mieux vaut donc utiliser quelques « trucs ». Pour cela, je conseille d'adopter une technique bien connue des commerciaux : il a été démontré que les gens collaborent plus facilement lorsque l'on a déjà noué un contact avec eux. Par exemple, dans un premier temps, vous pouvez leur envoyer un email leur demandant de répondre à cinq questions sur la sécurité. Cela demande peu d'effort et n'engage à rien. Une fois qu'ils l'auront fait, il sera temps de leur proposer de participer à une conférence d'information sur la sécurité. Le contact initié par le biais du questionnaire va permettre de doubler le nombre des personnes qui viendront de leur propre chef. Cette conférence sert à les interpeller, à stimuler leur curiosité. On y pose de nombreuses questions, sans donner de réponses. Pour en savoir plus, ils devront s'inscrire à une session, qui cette fois sera réellement de la sensibilisation à l'importance de la sécurité. Et les participants seront motivés !

Pourquoi informer n'est-il pas suffisant ?

Informer est important, mais il y a souvent un fossé entre ce qu'une personne envisage de faire et ce qu'elle fait réellement, même si elle est consciente de l'importance de la chose. Avec une campagne de sensibilisation basée sur la délivrance d'un message, on essaie de convaincre que la sécurité est importante. Mais, pour être efficace, il faut aussi jouer sur les comportements. Et pour cela, il faut aller au-delà de l'information.

Que faire d'autre pour modifier les comportements de manière durable ?

Lors des séances de sensibilisation, après avoir passé en revue les bons et les mauvais comportements, je demande aux participants d'en choisir un et de s'engager à le mettre en œuvre. Chacun prend celui qu'il préfère, qui doit être réalisable assez facilement. Cela peut être, par exemple, de ne plus désactiver son antivirus, de ne plus donner son mot de passe à un collègue, etc. Le collaborateur entre ainsi dans une logique où il a décidé qu'il avait un rôle à jouer en matière de sécurité. Ceci l'entraîne dans une spirale positive. Lors de la réunion suivante, il devra s'engager à respecter un autre bon comportement, et ainsi de suite. La difficulté de cette stratégie est qu'elle s'inscrit dans la durée et qu'il faut s'organiser pour suivre les utilisateurs. Il est donc très important de travailler en étroite collaboration avec la direction des ressources humaines.

Le programme national « Sécurité des systèmes d'Information »

Le MINEFI/HFD (Haut Fonctionnaire de Défense) et l'ACFCI ont signé en 2002 une convention cadre pour sensibiliser et former à la sécurité des systèmes d'information les petites et moyennes entreprises.

Cette convention prévoyait deux phases ; la première concernait la rédaction d'une brochure d'information destinée aux PME-PMI sur les risques liés à l'utilisation des TIC et s'est achevée fin 2002.

La deuxième phase, qui débute, doit permettre de mettre en place dans les C(R)CI des cellules de sensibilisation aux menaces visant les systèmes d'information des PME-PMI et aux parades adéquates.

La région Picardie, par l'intermédiaire de la CRCI, fait partie des huit régions pilotes désignées pour organiser les premières actions de sensibilisation.

La Sécurité des Systèmes d'Information

Dans ce dossier, le Service d'Information Economique de la Chambre Régionale de Commerce et d'Industrie de Picardie se propose de présenter les systèmes d'information, les menaces dont ils sont l'objet et les risques encourus du fait d'incidents de sécurité.

Les évolutions récentes et rapides de l'informatique ont contribué à l'accélération des échanges d'informations. Les entreprises se trouvent désormais confrontées au contrôle efficace de la confidentialité, de l'intégrité et de la disponibilité de ces informations.

Véritable point névralgique, le système d'information est souvent la proie de multiples attaques qui menacent l'activité économique des entreprises et requièrent la mise en place d'une politique interne de sécurité.

Système d'information et sécurité des systèmes d'information

D'une manière générale le système d'information concerne l'ensemble des moyens (organisation, acteurs, procédures et systèmes informatiques) nécessaires à l'élaboration, au traitement, au stockage, à l'acheminement et à l'exploitation des informations.

Dans les faits, de nos jours, l'essentiel du système d'information est porté par le système informatique et la notion de sécurité informatique recouvre pour l'essentiel la notion de sécurité des systèmes d'information (SSI).

Le concept de SSI recouvre donc un ensemble de méthodes, techniques et outils chargés de protéger les ressources d'un système informatique afin d'assurer la disponibilité des services, la confidentialité et l'intégrité des informations.

Les échanges au travers notamment d'Internet ont rendu également nécessaire le développement de propriétés nouvelles comme l'authentification, la paternité et la traçabilité de l'information.

La sécurité fait donc appel à différentes techniques complémentaires dont :

- *le chiffrement de l'information (cryptologie)*
- *la protection contre les signaux parasites compromettants (sécurité électronique)*
- *la protection contre les intrusions dans les logiciels, mémoires ou banques de données (sécurité informatique).*
- *la protection contre les accidents naturels et les actes malveillants (sécurité physique)*

Quelles menaces ?

Bien que souvent invisibles, du moins tant qu'elles n'ont pas eu de conséquences directes, les menaces sont cependant bien réelles :

Les menaces physiques

Actes de délinquance (vols, détérioration) et accidents naturels sont des menaces physiques qui visent directement le matériel. Souvent ignorés, les évènements naturels, accidentels ou malveillants, représentent pourtant jusqu'à 8% des sinistres déclarés (source : étude 2003 du CLUSIF sur la sinistralité).

Quelle entreprise peut se prétendre totalement à l'abri d'une inondation, d'une tempête ou d'un incendie d'autant que, si le matériel peut être, le plus souvent, aisément remplacé il n'en va pas de même des données qu'il contenait ?

Les menaces informatiques

Bien plus connues et envisagées, dès lors qu'on parle de sécurité des systèmes d'informations, les menaces informatiques (virus, chevaux de Troie, spams...) n'en sont pas moins de réels dangers. En 2003 environ 18% des entreprises ayant répondu à l'enquête du CLUSIF (étude sur la sinistralité) ont déclaré avoir été infectées par un ou plusieurs virus et l'impact financier en a été jugé élevé dans 11% des cas.

Heureusement la plupart des entreprises ont désormais saisi l'importance et l'intérêt des outils destinés à se prémunir de ces attaques (antivirus, firewall) et ces dernières voient leur efficacité reculer d'années en années.

Les menaces internes

Bien moins identifiées, les menaces internes sont plus souvent liées à la négligence et à l'ignorance du personnel de l'entreprise ; il s'agit plus d'inconscience que d'une réelle volonté de nuire.

En général ces menaces correspondent à un usage personnel du matériel informatique de l'entreprise avec d'une part le risque d'infection par virus (surtout dans le cas des ordinateurs portables confiés aux employés) et d'autre part un risque pénal par le téléchargement de programmes ou de fichiers pirates (films, musiques) qui sont incompatibles avec les applications professionnelles ou utilisés en dehors du cadre légal (licences d'exploitation).

Les cas d'espionnage industriel sont plus rares mais restent néanmoins un danger bien réel qui pèse sur les entreprises oeuvrant sur des marchés stratégiques. La sécurité des systèmes d'information passe aussi par la mise en place d'une politique efficace de protection visant à empêcher toute possibilité d'action malveillante par du personnel temporairement affecté à l'entreprise (stagiaires...)

Quels risques ?

Les risques sont tout aussi multiples et doivent être pris au sérieux. Nombre de personnes ne jugent ces risques que sous l'angle de l'entreprise agressée et peu savent ou même imaginent que leur propre responsabilité est engagée.

Les risques financiers

En 2003, selon une étude publiée par KPMG, les dégâts occasionnés par des incidents de sécurité génèrent des pertes qui peuvent se chiffrer, en Europe, entre 0,2 et 0,5 % du chiffre d'affaires.

S'il est assez facile de mesurer la perte financière représentée par la destruction, le vol et le remplacement du matériel informatique, la perte que représente le vol ou la destruction d'un fichier clients, par exemple, est beaucoup plus difficile à mesurer mais bien réelle. Certaines entreprises n'ayant pas prévu de plan de redémarrage de leur activité en cas de problèmes informatiques graves ne sont pas à même de faire face rapidement et à moindre frais à une telle catastrophe.

La responsabilité pénale

La loi relative à l'informatique, aux fichiers et aux libertés, oblige toute personne ordonnant ou effectuant un traitement d'informations nominatives à prendre toutes les précautions pour préserver la sécurité de ces informations et empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés.

Les risques encourus en cas de violation de cette loi sont très lourds : 5 ans d'emprisonnement et 300 000 € d'amende.

La responsabilité civile de l'employeur

Le code civil énonce que chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence. L'absence de moyens de sécurisation du serveur de l'entreprise est susceptible de constituer une faute donnant lieu à responsabilité.

Si un collaborateur de l'entreprise venait à introduire un virus sur le serveur de l'entreprise et si le système informatique de clients ou partenaires venait à être infecté par un virus émanant de ce serveur, ces derniers pourraient engager la responsabilité pénale du salarié mais aussi la responsabilité civile de l'employeur qui est responsable des dommages causés par ses collaborateurs.

MEHARI : MÉTHODE D'ANALYSE DE RISQUE

ÉLABORÉE PAR DES PROFESSIONNELS DU CLUSIF

La pérennité des entreprises et des collectivités dépend largement des Systèmes d'Information. Sur ces points névralgiques pèsent des risques qui, non maîtrisés, peuvent affecter lourdement vos enjeux métiers.

MEHARI propose une approche claire et rigoureuse qui vous permet de mettre en œuvre les mesures de réduction de risques adaptées à vos objectifs.

MEHARI apporte :

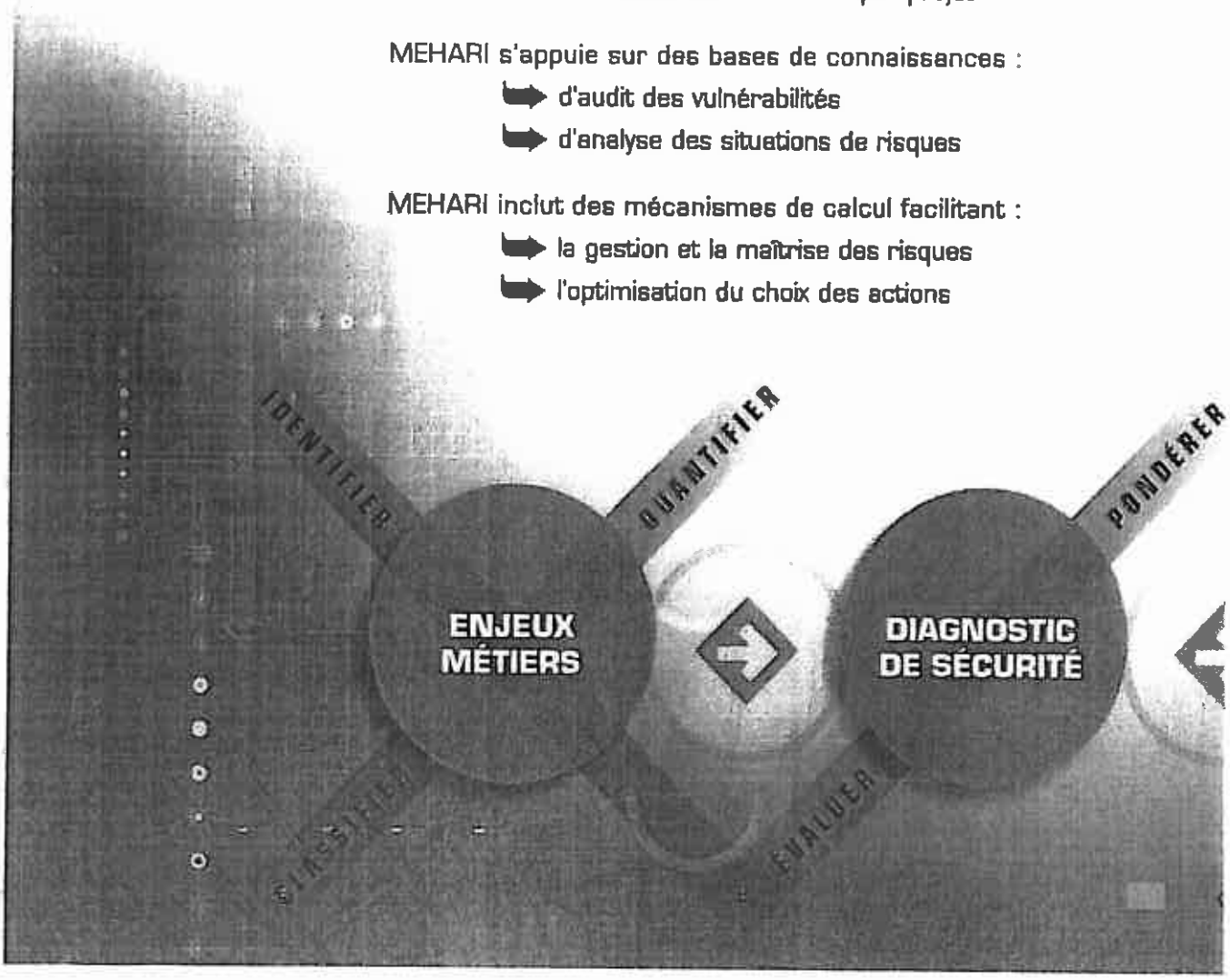
- un modèle de gestion du risque
- une démarche modulable par projet

MEHARI s'appuie sur des bases de connaissances :

- d'audit des vulnérabilités
- d'analyse des situations de risques

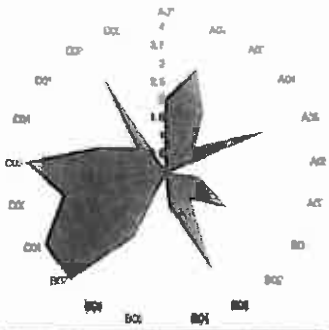
MEHARI inclut des mécanismes de calcul facilitant :

- la gestion et la maîtrise des risques
- l'optimisation du choix des actions



LES POINTS FORTS DE MEHARI

LA BOÎTE À OUTILS DES PROFESSIONNELS DE LA SÉCURITÉ DE L'INFORMATION



Exemple de rosace d'audit de service de sécurité

SOUPLE :

- Utilisable dans des contextes diversifiés tant en terme de structure, de secteur ou de taille que d'objectifs recherchés

EVOLUTIVE :

- Prend en compte l'expérience acquise
- S'adapte aux évolutions du marché et au contexte propre à l'entreprise

COMPATIBLE :

- Avec les modèles de gouvernance des risques
- Avec les normes et standards en vigueur

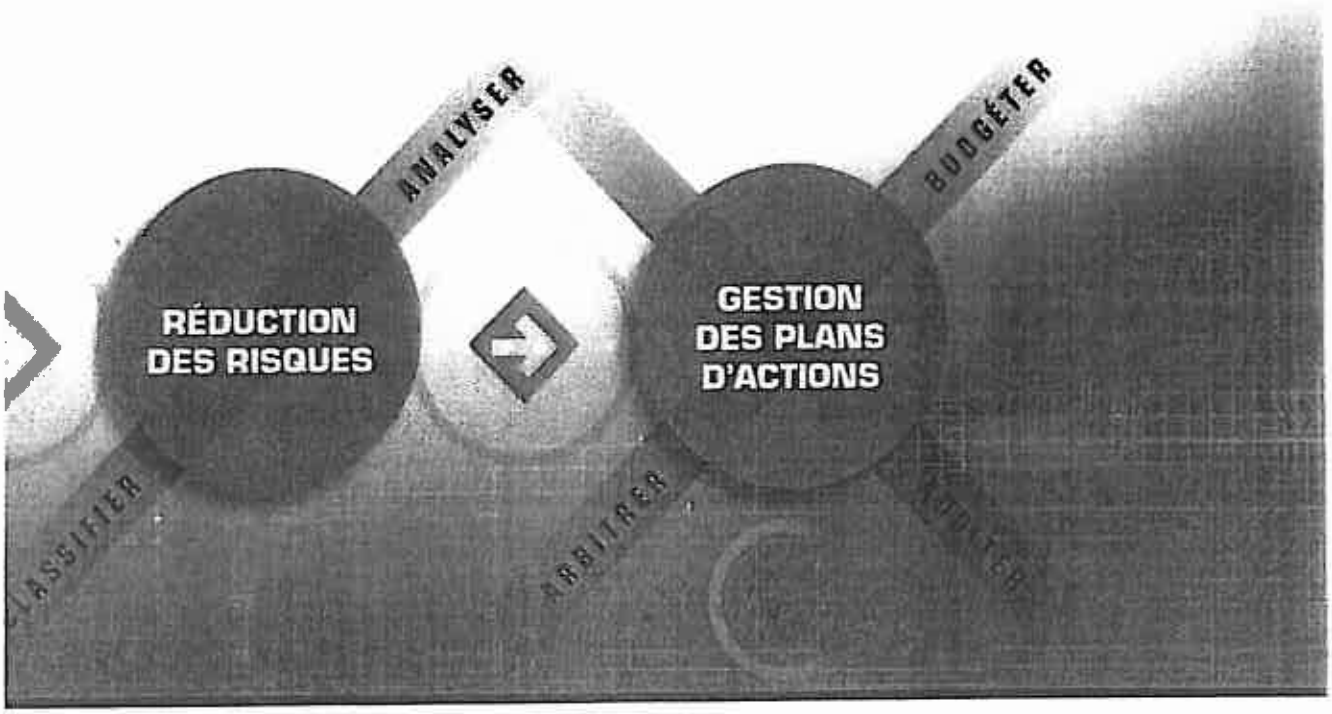
➥ **MEHARI se distingue par :**

- une approche qualitative et quantitative de la gravité du risque
- la modularité et la souplesse de ses composants
- l'existence de progiciels de présentation et de traitement des résultats

Avec MEHARI :

➥ Vous construisez vos plans d'actions par étape en fonction de vos enjeux

➥ Vous vous inscrivez dans une démarche qualité



Utilisation de la méthode EBIOS :

de l'organisation projet aux composants du SMSI (Système de Management de la Sécurité de l'Information)

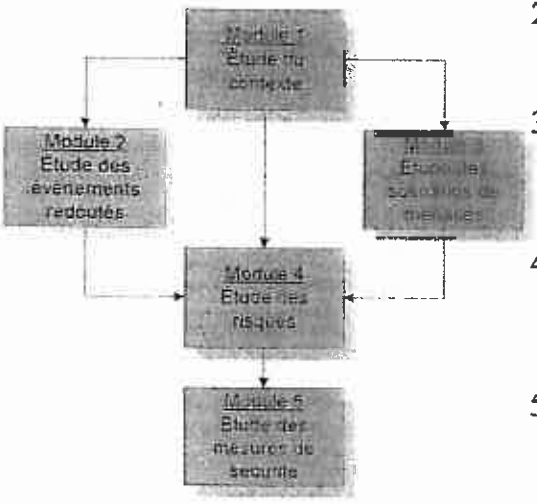
Philippe TOURRON
Direction Opérationnelle des Systèmes d'Information/Université de la Méditerranée

Matthieu GRALI
Secrétariat Général de la Défense Nationale/Agence Nationale de la Sécurité des Systèmes d'Information

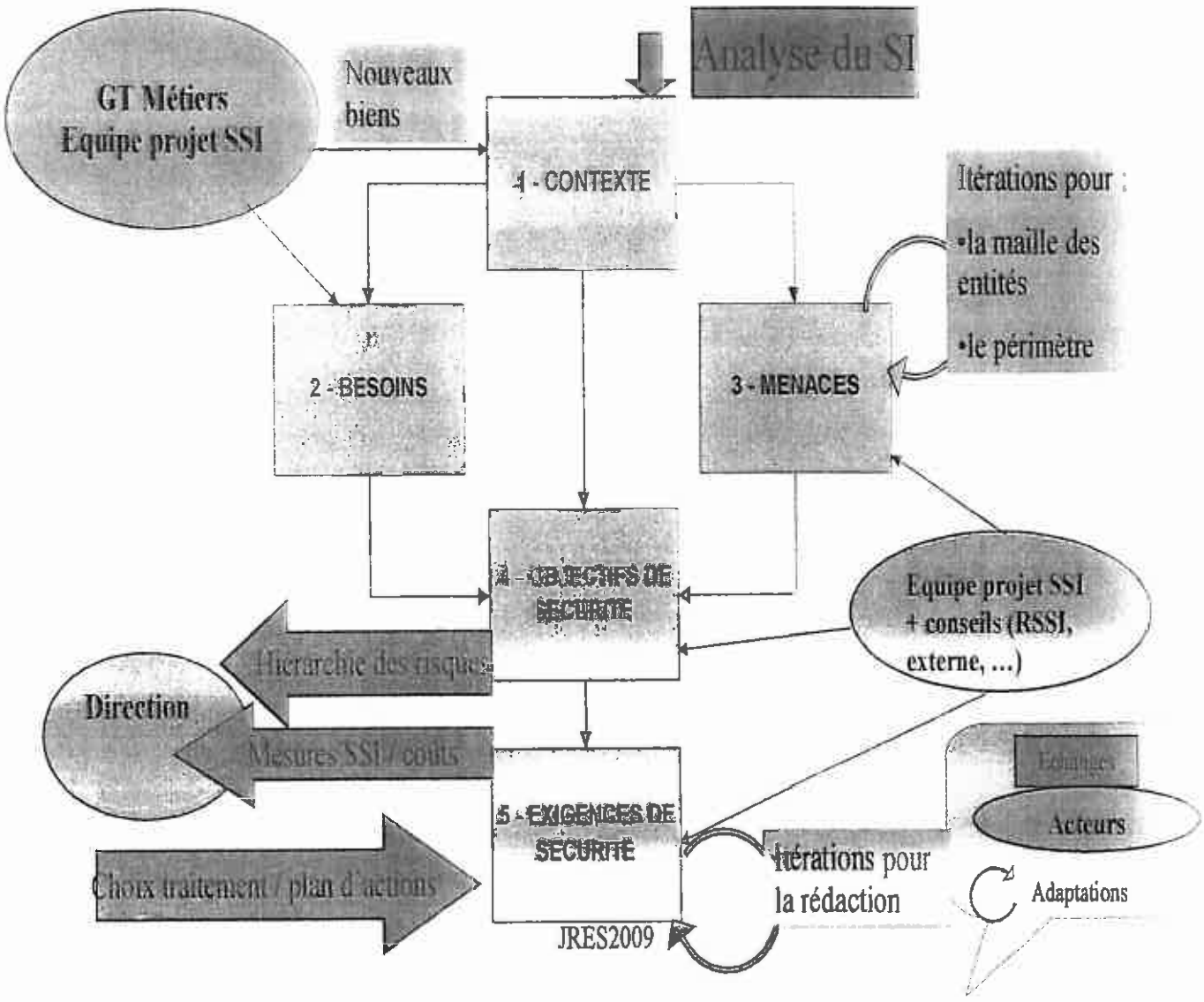
JRES 2009

jres 2009

Une boîte à outils en 5 modules itératifs pour appliquer l'ISO 27001



1. Le **cadre** de la gestion des risques, les **métriques** et le sujet de l'étude sont définis
2. Les **événements redoutés** sont analysés (besoins de sécurité des biens essentiels, impacts, sources de menaces, gravité)
3. Les **scénarios de menaces** sont analysés (menaces, vulnérabilités des biens supports, sources de menaces, vraisemblance)
4. Les risques sont déduits, estimés (gravité, vraisemblance) et évalué (cartographie), et les objectifs de sécurité identifiés (choix des options de traitement)
5. Les **mesures de sécurité** sont spécifiées (défense en profondeur), leur mise en œuvre est planifiée, les risques résiduels sont mis en évidence et l'homologation prononcée

JRES2009

Projet UFR : Usage de la méthode EBIOSv2