SADOK, M. et LESCA, H. (2007) -Veille anticipative et Sécurité des ressources informationnelles de l'entreprise à l'ère numérique. Article proposé à la Revue Gestion (HEC Montréal).

# Veille anticipative et Sécurité des ressources informationnelles de l'entreprise à l'ère numérique

**Moufida SADOK**
Institut Supérieur des Etudes Technologiques en Communications de Tunis
*Moufida.Sadok@isetcom.rnu.tn*

**Humbert LESCA**
CERAG UMR 5820 CNRS UPMF Grenoble

**Résumé**

Avec l'utilisation de plus en plus importante des technologies de l'information et de la communication et notamment l'Internet, l'entreprise est amenée à gérer et à réduire le risque des agressions numériques à travers une approche proactive dans la mesure où les informations constituent l'une des ressources les plus importantes à protéger dans une entreprise. L'insuffisance des solutions techniques et physiques de sécurité face à la complexité et l'imprévisibilité croissantes des agressions numériques, de même que l'absence de réelle formation de spécialistes dans ce domaine, obligent les entreprises à valoriser le rôle des équipes de réponse aux incidents de sécurité (ERI) dans une perspective de réduction du temps de réponse aux agressions numériques voire même l'anticipation de leurs occurrences. Cependant, les ERI manquent de méthodes adéquates pour assister l'activité de réponse aux agressions numériques et particulièrement l'étape d'interprétation collective des informations collectées de type signal faible, et de capitaliser les expériences et les connaissances qui pourraient émerger de ce processus d'interprétation. Nous présentons dans ce papier le cadre conceptuel et la réalisation d'une Méthode d'Analyse et de Réduction du Risque des Agressions Numériques (**MARRAN**) afin d'aider une ERI à réagir vite ou par anticipation et ce, dans le but, de minimiser les dégâts matériels et immatériels occasionnés par celles-ci. Les résultats d'évaluation de MARRAN auprès d'experts en sécurité informatique seront également exposés.

## Introduction

La sécurité des ressources informationnelles d'une entreprise est devenue un élément vital pour le développement et la pérennisation de son activité avec l'évolution notable de son contexte économique et technologique, notamment la forte évolution de l'informatique et de l'Internet ainsi que de leurs usages. Le besoin de l'entreprise de demeurer ouverte à ses employés, à ses partenaires et à ses clients l'expose à des menaces et à des agressions qui ne cessent de se multiplier et dont les conséquences tangibles et intangibles sont néfastes.

Les entreprises mettent en place des politiques de sécurité pour réduire le risque des agressions numériques à un niveau acceptable par l'utilisation des solutions de sécurité adaptées à leurs besoins et en fonction des caractéristiques de leurs services offerts. Cependant, les agressions numériques sont de plus en plus incertaines et complexes. L'incertitude est liée au fait que leur visibilité n'est clairement possible que lorsqu'elles sont terminées, mais aussi au fait qu'une entreprise peut être victime d'une agression sans en avoir conscience. La complexité s'accroît dans la mesure où les hackers sont de plus en plus inventifs. Les enjeux stratégiques des agressions numériques pour une entreprise ne se limitent pas à des pertes financières. Ils peuvent concerner également son image de marque ou son capital clients, ainsi que l'efficacité et la continuité de son activité. Les enjeux importants des agressions numériques mettent en évidence la nécessité de réagir à temps et de développer une capacité d'anticipation. La veille anticipative stratégique semble pouvoir permettre à l'entreprise de réduire l'incertitude et le risque ainsi que le temps de réponse face aux changements de son environnement voire même de les anticiper. Dans le cadre de notre recherche, la pratique de la veille anticipative stratégique est confrontée à une activité fondamentale et vitale pour l'entreprise à savoir la sécurité de ses ressources informationnelles contre les agressions numériques. Notre application, dans le domaine de réponse aux agressions numériques, concerne une solution particulière de sécurité à travers le travail des équipes de réponse aux incidents (ERI) de sécurité. Nous montrons que la réponse aux agressions numériques est une activité où le processus d'interprétation collective des informations de type signal faible est fondamental pour agir vite ou par anticipation. Les ERI

**manquent de méthodes** (Killcrece *et al*., 2003) adéquates pour assister cette étape d'interprétation des informations collectées de type signal et/ou signe faible. Le retour sur investissements, évalué en termes de valorisation des compétences acquises et du savoir faire des membres de l'ERI, pourrait justifier des investissements engagés pour la recherche de **méthodes** appropriées afin de soutenir leur travail, et pour la mise en place de **formation**.
Ainsi, nous présentons dans ce papier le cadre conceptuel d'une MARRAN qui a fait l'objet d'une évaluation par des experts en sécurité informatique.

**Enjeux stratégiques des agressions numériques**

Aujourd'hui, l'utilisation des Technologies de l'Information et de la Communication (TIC), et notamment l'Internet, est généralisée dans les entreprises pour gérer plusieurs activités à distance avec leurs différents partenaires et même avec leurs employés. Les avantages de l'utilisation des TIC peuvent être situés sur un plan opérationnel, organisationnel et stratégique.
En effet, les développements importants en matière des TIC ont permis à l'entreprise de se disposer d'un ensemble de nouveaux moyens pour augmenter la flexibilité des processus par une réduction des temps et des coûts du changement ainsi que par la facilitation de la communication, de la coordination et de la coopération entre les acteurs (Prax, 1997 ; Reix, 1999). L'introduction des TIC a également favorisé la réorganisation et la reconfiguration de la chaîne de valeur (Porter, 1986) notamment par la mise en place d'une chaîne virtuelle capable de créer de la valeur tout autant que la chaîne de valeur physique (Rayport et Sviokla, 1995; Venkatraman et Henderson, 1998).
Par ailleurs, la complète diffusion de l'Internet a largement favorisé le traitement et la transmission de données notamment texte, son et image. Ceci est de nature à permettre des possibilités d'interfaces directes entre clients et producteurs ce qui a permis le développement du commerce électronique qui devient un vecteur de croissance privilégié (Bitouzet, 1999 ; Hervier, 2001) par les entreprises en permettant l'amélioration de la qualité de service, l'attraction de nouveaux clients et la création de nouveaux modes de vente des produits existants (Boyle, 2001 ; Grandon et Pearson, 2003). L'Internet est également utilisé comme un outil important et efficace de gestion de la relation client (Bradshaw et Brash, 2001 ; Ab Hamid et Kassim, 2004) dans une optique de personnalisation des produits et des services pour des clients exigeants, qui demandent de plus en plus des solutions globales adaptées à leurs besoins spécifiques et des qualités de services plus élevées.

Cependant, l'ouverture et l'extension du réseau de l'entreprise expose celle-ci à un nouveau type de risque lié à la sécurité de ses ressources informationnelles : le **risque des agressions numériques**. Les actions des pirates informatiques ont des conséquences qui ne se limitent pas à des pertes financières et matérielles mais aussi des pertes immatérielles et indirectes qui peuvent concerner la réputation et l'image de marque d'une entreprise, la perte de certaines opportunités d'affaires ainsi que la dégradation de la performance et de la productivité du système d'information.
En effet, la connectivité de plus en plus importante des entreprises et la dépendance accrue à l'égard des réseaux dont la maîtrise leur échappe en grande partie font des actions des pirates, qu'ils soient internes ou externes, des sources extrêmes de menaces pour l'efficacité et la continuité de l'activité de l'entreprise.

D'une façon générale, une **agression** est toute action compromettant la sécurité de 1'information d'une organisation (Stallings, 2000). La sécurité réseau concerne la protection des ressources en informations (notamment les informations personnelles et financières des utilisateurs, projets de recherche, prototypes virtuels de produits,..etc.) de l'entreprise en assurant la confidentialité, l'intégrité, et la disponibilité (Canavan, 2001 ; Vermeulen et Solms, 2002). La confidentialité doit assurer l'accès aux ressources pour les personnes autorisées. L'intégrité de l'information concerne l'authenticité des données qui ne peuvent être modifiées que par les personnes autorisées. La disponibilité est le concept garantissant l'accès à l'information quand un utilisateur autorisé en a besoin.

Selon les statistiques du CERT (*Computer Emergency Response Team*), une agence fédérale chargée de la surveillance de la sécurité informatique des Etats-Unis, le nombre de vulnérabilités susceptibles d'être exploitées pour mener une agression numérique est en croissance accélérée. Ce nombre est passé de 3783 en 2003 à 5990 en 2005. De même, pour l'an 2002, le CERT (www.cert.org) a recensé plus de 82000 incidents de sécurité, soit quatre fois plus qu'en 2000. Ce chiffre est passé à plus que 137000 incidents pour l'année 2003. De même, des analyses effectuées récemment par le CERT ont montré que les outils utilisés lors des agressions numériques ont beaucoup évolué en devenant de plus en plus sophistiqués notamment pour les rendre difficilement identifiables dans les phases d'investigation sur les incidents. La rapidité dans la découverte des vulnérabilités rend de plus en plus difficile la

conservation d'un niveau de sécurité satisfaisant sur un système d'information hétérogène et géographiquement dispersé.
Le onzième rapport annuel réalisé par le CSI/FBI (www.gocsi.com) relatif à l'année 2006 sur l'état de sécurité dans plusieurs entreprises américaines opérant dans plusieurs secteurs d'activité indique que plus de 72% des 341 entreprises interviewées reconnaissent avoir été victimes, au moins une fois, d'une attaque provenant de l'extérieur ou de l'intérieur. Le reste des entreprises (28%) sont incapables de savoir si elles ont été cibles d'attaques ou non. D'après ce même rapport, 59% des entreprises interrogées ont enregistré plus que dix incidents de sécurité qui ont ciblé leurs sites Web, alors que 36% sont incapables de cerner le nombre.

Les mêmes tendances sont affichées dans les rapports publiés par le CLUSIF (Club de la Sécurité des systèmes d'Information Français www.clusif.asso.fr) en France ou par l'AusCERT (www.auscert.org.au) en Australie.

Par ailleurs, le vol des informations, le déni de service, et les virus sont les agressions numériques qui ont enregistré les pertes financières les plus élevées.

**L'adaptation de la veille anticipative stratégique dans le cas de réponse aux agressions numériques**

Le risque des agressions numériques est étroitement lié à l'incertitude de leurs occurrences. Cette relation est traduite par les pertes financières engendrées par ces agressions ainsi que par la diversité de leurs types et de leurs sources comme en témoignent les rapports des organismes spécialisés officiels internationaux.
Ce qu'il faut signaler c'est que certaines propriétés des systèmes de communication rendent les agressions numériques plus difficiles à détecter, à analyser et à répondre que les agressions usuelles. Ces propriétés incluent notamment :

- le caractère automatique des tâches,
- la possibilité d'effectuer des actions à distance,
- la possibilité de faire propager les techniques d'attaques,
- le fait que l'identité du pirate soit facilement dissimulable puisqu'il s'agit généralement d'une adresse.

Par conséquent, il est nécessaire de collecter des informations d'un certain type relatives à des **alertes précoces** liées à des problèmes potentiels de sécurité. Ces informations doivent avoir un caractère anticipatif « ***early warning*** » dont l'interprétation est susceptible de réduire le risque des agressions et de minimiser les coûts de réparation (Killcrece *et al*., 2003). En effet, la rapidité avec laquelle une entreprise détecte, analyse et répond à une agression contre son système d'information limite d'une façon significative les dommages occasionnés par celle-ci et réduit considérablement les coûts de son recouvrement.

Il devrait être donc impératif, dans ce cas, d'anticiper les agressions numériques le plus tôt possible pour pouvoir se protéger à temps et aux moindres coûts. Dans la plupart des cas, l'anticipation des agressions numériques s'effectue à travers la détection des informations de type signal faible générées par le réseau de l'entreprise. Toutefois, la détection de ces signaux générés par le réseau est difficile et complexe, ce qui explique en grande partie le nombre croissant des agressions numériques.
Ainsi, la mise en place d'un dispositif de veille anticipative stratégique pour réduire le risque lié à l'incertitude des agressions numériques nous paraît trouver une application prometteuse dans le domaine de la sécurité des réseaux d'entreprise. En effet, la veille anticipative stratégique est un dispositif d'**attention** permettant de réduire le risque lié à l'incertitude et de sécuriser ou améliorer dans le futur la position de l'organisation (Choo, 1997). Dans notre cas, la veille anticipative stratégique est un dispositif qui porte l'attention sur des nouveaux acteurs particuliers dont les actions représentent un risque énorme pour l'efficacité et la continuité de l'activité de l'entreprise dans le contexte des TIC.

Dans le domaine de la sécurité des réseaux, la veille anticipative est un système d'information dédié à l'aide à la protection des ressources informationnelles de l'entreprise. Elle permet la détection :

- des agressions numériques qui ont été <u>préalablement répertoriées</u> (et largement commentées dans des sites destinés à leur analyse) et la prise de décision relative à la réponse à ces agressions compte tenu de leur impact sur l'activité de l'entreprise.
- Ce même processus permet de caractériser les agressions <u>non encore répertoriées</u> à travers l'analyse de certains signaux et/ou signes faibles collectés par des systèmes de détection, d'évaluer les dégâts potentiels occasionnés et de préparer une réponse appropriée et rapide à ces attaques.

Néanmoins, la veille anticipative stratégique est appréhendée comme étant un système d'interprétation (Daft et Weick, 1984) et un processus de construction de sens (Weick, 1995) à partir d'informations. Il s'agit d'informations susceptibles d'annoncer des ruptures ou des discontinuités dans l'environnement. Les informations de la veille stratégique peuvent être des signaux faibles (Ansoff, 1975) : elles ont alors pour caractéristiques d'être incertaines, qualitatives, ambiguës, fragmentaires (Gorry et Scott-Morton, 1971 ; Argyris, 1976 ; Lesca, 1986), fugaces (Marmuse, 1992), rapidement obsolètes (Bourgeois et Eisenhardt, 1988), incomplètes, imprécises et de fiabilité fragile (Lesca, 2003). Le traitement de ces informations est de type « interprétation et induction», et requiert la création d'une **intelligence collective** nécessitant la mobilisation d'expériences et d'expertises diverses au sein de l'entreprise, voire extérieures à celle-ci (Lesca, 2003).

Dans le domaine de la sécurité des ressources informationnelles de l'entreprise, la prise de décision, tout comme l'analyse des agressions, nécessite une activité d'interprétation **collective** des informations à caractère anticipatif selon un processus de création de sens afin d'élaborer des réponses techniques et managériales appropriées. De plus, ces agressions ainsi que les liens générés lors du processus d'interprétation devraient être mémorisés pour enrichir le processus de réponse aux incidents de sécurité et pour soutenir un processus d'apprentissage efficace.

Dans le domaine de réponse aux agressions numériques, le processus d'interprétation collective des informations de type signal et/ou signe faible est une activité fondamentale pour agir vite ou par anticipation.

En effet, l'utilisation des solutions techniques et physiques de sécurité s'avère insuffisante vu la complexité et l'imprévisibilité croissantes des agressions numériques. Les rapports des organismes spécialisés officiels internationaux (CERT, AusCERT, CLUSIF) montrent que l'utilisation massive des antivirus, des *firewalls* et des systèmes de détection d'intrusion est d'une efficacité limitée dans le cas des agressions compliquées ou inconnues.

La détection des signes nécessite la présence d'une équipe capable d'interpréter, d'analyser et de traiter ces signes car la seule implémentation des outils et techniques software et hardware est insuffisante.

La constitution d'une ERI comme étant une solution complémentaire de sécurité se trouve largement justifiée afin de détecter et d'interpréter des **signes précoces** d'intrusion ou des tentatives d'intrusion. Cette interprétation nécessite une véritable intelligence au sein d'une ERI et devrait permettre de réduire et d'anticiper le risque des agressions numériques. La composition d'une ERI s'avère comme étant une solution de sécurité nécessaire et complémentaire à l'analyse de risque, la définition d'une politique de sécurité et l'implémentation d'un ensemble de solutions techniques et physiques.

**Proposition d'une Méthode d'Analyse et de Réduction du Risque des Agressions Numériques (MARRAN)**

La conception et la construction de MARRAN sont issues d'une série d'observations du terrain et d'une articulation et extension de certaines connaissances théoriques et actionnables disponibles (Sadok, 2004). Des études (Caron-Fasan, 1997 ; Lesca, 2001, par exemple) ont signalé un vide dans les méthodes à mettre en œuvre ainsi que dans les techniques à utiliser pour le traitement des informations de type signal et/ou signe faible à cause notamment de la difficulté de cette opération étant donné la nature de ces informations.

Le modèle conceptuel de MARRAN est structuré selon trois phases essentielles. Ces phases décrivent le processus collectif de raisonnement créatif et itératif à partir d'informations de type signal et/ou signe faible dans un contexte incertain et turbulent. Dans le cas du travail d'une ERI l'objectif d'un tel processus est de **construire le scénario de l'agression** numérique afin de réduire le risque, d'y **répondre** le plus rapidement possible et d'**anticiper** l'occurrence d'agressions similaires dans le futur.

La première phase décrit l'activité de **création des liens initiaux**. Son objectif est d'amplifier le signal et/ou signe faible détecté et d'établir des liens capables de donner une première idée sur le risque potentiel encouru par l'entreprise. Il est nécessaire dans ce cadre d'établir une typologie des liens de raisonnement pour organiser, d'une façon significative, les informations disponibles. Celles-ci proviennent des signaux et/ou signes faibles amplifiés, des sources internes ou externes, ainsi que de la contribution des acteurs du processus de création collective de sens. La deuxième phase, cruciale dans le processus, décrit l'activité de création des **liens d'inférence** par raisonnement itératif. Durant cette phase, de nouveaux liens sont inférés itérativement en utilisant les liens existants, les **connaissances tacites** des acteurs du

processus de création collective de sens. Les acteurs peuvent également extraire des **informations documentaires** prélevées dans des archives structurées et actualisées tout au long du processus, afin d'aboutir à une vision plus intelligible de la situation.

Dans la troisième phase des critères de satisfaction (des membres de l'ERI et des responsables qui auront à prendre la décision finale) sont définis pour mettre fin au processus de raisonnement sur les liens. Cette phase a pour objectifs:

- la **vérification** si le processus itératif de raisonnement parvient à une connaissance claire du risque encouru,
- une bonne compréhension des mécanismes qui ont généré les signaux et/ou signes faibles détectés, et
- une estimation globale d'autres risques potentiellement liés à l'agression en cours d'examen.

A la fin de cette phase, un plan d'action peut être déclenché pour proposer, en cas de besoin, les réponses requises pour réduire le risque identifié et anticiper des décisions liées à celui-ci. Par ailleurs, le modèle conceptuel peut être est représenté par un graphe orienté, composé d'un ensemble de nœuds et de relations liant ces nœuds entre eux. Les nœuds représentent des actions, des hypothèses, des informations, ou des objectifs. Les relations permettent une estimation qualitative de l'effet d'un nœud sur un autre et répondent au besoin de quantifier ensuite cet effet. Ceci devrait permettre la construction du scénario définitif de l'agression et l'estimation de ses conséquences.

L'instrumentation du modèle conceptuel et sa mise en œuvre peuvent être basées sur l'utilisation de la technologie Internet, qui peut fournir :

- une **base de données** pour stocker des informations liées aux risques encourus par l'entreprise et pour **garder la trace** de toutes les informations générées lors de la phase de raisonnement sur les liens,
- une base de connaissances qui stocke tous les **raisonnements** sur les signaux et/ou signes faibles ainsi que la trace de tous les liens inférés lors du processus d'intelligence collective.

Les bases de données et de connaissances fournissent un support pour un processus de création collective de sens dynamique (Sadok. et al., 2003). Ces bases peuvent être assistées par des mécanismes intelligents d'extraction permettant la **recherche approchée**, la recherche des heuristiques et la transformation automatique des liens stockés.
A cet effet, un logiciel a été conçu et mis en œuvre pour assister MARRAN utilisant certaines applications de la technologie Internet et permettant :

- La représentation graphique de l'ensemble des nœuds et des liens montrant les points de vue élaborés par les membres de l'ERI lors du processus de la création collective de sens. Les objets graphiques générés au cours de cette activité bénéficient d'une construction évolutive, flexible et structurelle (par exemple, un simple clic sur un nœud ou un arc peut faire accéder à une information riche).

- La construction de bases de données et de connaissances afin d'assister le processus de la création collective de sens et de mémoriser des connaissances **acquises** lors des validations passées de scénarios ayant servi à l'ERI de résoudre des problèmes de sécurité dans le passé, ou **intégrées** dans le processus de raisonnement ou d'affinement et acquises suite à des recherches d'informations à l'interne ou à l'externe de l'entreprise (disponibles par exemple dans des sites Web spécialisés).

- L'intégration de moteurs de recherche de type « recherche exacte et/ou approchée » pour la collecte des informations complémentaires lors de la construction du scénario de l'agression. Les mécanismes de recherche de type « **recherche approchée** » sont basés sur des relations diverses entre les éléments en mémoire incluant notamment l'analogie, la similarité, la proximité.

- L'intégration de moteurs d'inférence qui représentent des outils permettant la déduction automatique à partir d'hypothèses et de règles de déduction approchée à travers la création de liens sémantiques et/ou probabilistes.

La mise en place d'une assistance technique au raisonnement collectif permet la construction et l'analyse des scénarios d'attaque afin de réduire la complexité du raisonnement et faciliter la navigation sur les graphes représentant les points de vue des membres de l'ERI.

**Les apports de MARRAN**

La diversité et la complexité des raisonnements, notamment les raisonnements non linéaires, dans un contexte fortement incertain requièrent une richesse de la typologie des liens. L'enrichissement de la typologie des liens est réalisée en intégrant la **probabilité**, **l'approximation** dans la création de relations entre des informations incomplètes ainsi que la **pression du temps** comme étant des facteurs très significatifs dans le domaine de prise de décision relative à la détection et à l'analyse des agressions numériques. En effet, le processus d'interprétation est dynamique (Drazin et al., 1999), et le travail d'une équipe de « *sensemaking* » est plutôt continu et dynamique (Ashmos et Nathan, 2002).

Les liens probabilistes permettent d'élargir le champ du raisonnement dans un contexte incertain et turbulent. Les liens dynamiques, variables en fonction du temps, permettent d'adapter le raisonnement au contexte et aux objectifs de la prise de décision. De plus, l'enrichissement de la typologie prend en compte des relations de nature diverse entre les éléments du raisonnement telles que les relations sémantiques, quantitatives, transactionnelles, etc.

Par ailleurs, la création de sens est un processus collectif où il est important de définir des mécanismes de conciliation et d'intégration des différents points de vues.

En effet, au cours de ce processus chaque membre présente ses propres éléments de raisonnement. Des divergences ou des conflits entre les points de vue peuvent se produire durant le processus d'évaluation et d'analyse de la situation. Pour l'intégration des points de vue, la médiation et la négociation sont des mécanismes nécessaires pour construire une vision globale, collective et intelligible.

La médiation cerne les zones de conflit, les analyse en vue de trouver des arrangements possibles pour plus de compatibilité entre les relations et les liens de raisonnement. La négociation dans ce cadre se traduit, d'une part, par l'altération d'un point de vue vers un autre plus compatible avec le reste du graphe par persuasion et discussion. D'autre part, la négociation se traduit par l'enrichissement et la modification des points de vue en conflit à travers des mécanismes d'affinement des liens de raisonnement.

La ré**conciliation** des différences entre les points de vue des membres de l'ERI devrait se focaliser sur trois principaux objectifs suivants :

- la réalisation d'une définition commune et/ou partagée de tous les concepts, les actions et les informations pertinents pour l'évaluation et l'analyse de la situation,

- l'élimination des désaccords partiels en utilisant la négociation ou encore l'investigation notamment en s'appuyant sur les TIC,

- la réduction du nombre des points de vue unilatéraux et les zones de désaccords partiels visant à diminuer les différences.

L'activité de médiation est effectuée par un médiateur dont le rôle est l'**animation**, la convergence vers des actions collectives, la construction des alternatives en matière de décision, et l'extraction des concepts/informations si nécessaire.
Pour résoudre les problèmes et intégrer les différents graphes, le médiateur devrait avoir également certaines **compétences** pour accomplir ce rôle efficacement. Les principales compétences appropriées sont la **pédagogie**, la **crédibilité** (fondée sur l'expertise et l'expérience), la **confiance**, la **communication,** et la **coordination**. Ceci soulève les questions de la sélection et de la **formation** du médiateur.

Ainsi, le médiateur a besoin d'outils efficaces pour assister la représentation des nœuds et des liens ainsi que la manipulation des relations entre les nœuds. De plus, il a besoin des moteurs de recherche efficaces (pour des raisons liées à la pression du temps) pour extraire des informations complémentaires stockées dans des bases de données internes ou externes. Des heuristiques peuvent être employées pour aider à la prise de décision collective et à gérer des chemins de raisonnement alternatifs.

**Résultats empiriques de l'évaluation de MARRAN**

Nous présentons dans ce paragraphe les résultats d'évaluation de MARRAN à travers le traitement des entretiens effectués auprès des experts en sécurité. Cette évaluation vise principalement à affirmer l'utilité perçue et la facilité perçue de la méthode en analysant les réponses concernant le fonctionnement de la méthode proprement dite.

Le canevas d'entretien se présente sous la forme d'une grille de questions devant nous permettre d'évaluer, d'abord, ces deux aspects de la méthode. Ensuite, nous avons préparé des

questions qui concernent l'état des pratiques en matière de réduction et d'anticipation du risque des agressions numériques afin de savoir si notre proposition apporte une amélioration par rapport à l'état des ces pratiques.
Nous avons contacté neuf experts en sécurité informatique. Trois membres de l'ERI d'une entreprise de certification électronique et six experts travaillant dans des entreprises qui sont des fournisseurs des services Internet et pour lesquelles le risque des agressions numériques est d'une ampleur considérable compte tenu de la nature de leurs activités. Les trois membres de l'ERI ont une expérience de quatre ans dans le domaine de la sécurité informatique. Ils sont chargés de surveiller d'une façon permanente le trafic sur le réseau de l'entreprise et de répondre en cas d'urgence à des problèmes de sécurité. Quant aux autres experts, ceux-ci sont impliqués directement dans la prise de décision concernant la réponse aux agressions numériques au sein de leurs entreprises qui sont classées comme étant des entreprises fortement utilisatrices des TIC. Ils sont également impliqués dans le développement et la mise à jour de la politique de sécurité de leurs entreprises. Ces experts sont confrontés quotidiennement à des problèmes de sécurité et ils ont déjà pilotés des projets importants dans ce domaine. L'expérience de ces experts varie entre cinq et dix ans.

**Enseignements tirés concernant l'utilité perçue**

L'analyse des résultats empiriques liés à l'utilité perçue de la méthode concerne le traitement des informations de type signal/signe faible, l'activité de médiation et la phase de mémorisation des raisonnements lors des constructions des scénarios d'attaques.

Les étapes d'amplification progressive des signaux/signes faibles, de recherche complémentaire d'informations et du raisonnement itératif sont reconnues à l'unanimité des experts comme étant des étapes utiles dans le cadre du travail d'une ERI pour répondre aux agressions numériques, et particulièrement dans le cas des agressions numériques inconnues par l'entreprise. De ce fait, ils pensent que les trois étapes de la méthode permettent une construction significative des scénarios d'attaques.
De même, les experts sont tous d'accord sur le fait que le processus de création de sens devrait être collectif vu la nature des informations de type signal/signe faible. Cependant, l'output de ce processus dépend également de la méthode de travail utilisée et des compétences et des expertises des membres de l'ERI.

**Enseignements tirés concernant le rôle du médiateur**

S’agissant de l'activité de médiation, celle-ci est perçue comme étant une activité nécessaire pour le travail d'une ERI. De plus, elle est susceptible d’améliorer les temps de réponse particulièrement en présence de méthodes de travail et des outils appropriés. Les experts contactés sont tous d'accord sur le fait que le rôle du médiateur est important et même déterminant pour l'efficacité du travail de l'ERI. Il est également essentiel pour détecter de nouvelles attaques. Certains experts sont concernés par l’activité de médiation et découvrent lors des entretiens qu'ils pratiquent la médiation, « sans le savoir » c’est-à-dire sans une démarche explicite ou une formation appropriée.

Toutefois, l'utilité du médiateur peut être faible dans le cas des agressions classiques ou connues lorsque le raisonnement est simple à réaliser.

**Enseignements tirés concernant la mémorisation des raisonnements**

Lors des entretiens, les experts ont été particulièrement intéressés par les possibilités offertes par la méthode proposée de garder des traces des raisonnements effectués lors des constructions des scénarios d’attaques. La mémorisation de ces raisonnements est nécessaire à cause de la grande mobilité des ingénieurs et le coût élevé de leur formation dans les tâches d’investigation électronique (enquête numérique à la détection d’un signal faible) et de réponse aux incidents de sécurité.

Les bases de données et de connaissances sont considérées par l'ensemble des experts comme étant déterminantes et indispensables dans le processus d'itération et d'affinement des raisonnements. Dans ce cadre, la nécessité de démarrer avec une base de connaissances acquise est une condition qui paraît très importante, selon les experts rencontrés, pour l'utilisation de la méthode. Certains experts considèrent même qu'il s'agit d'une condition sine qua non pour l'efficacité de la méthode.
A travers la mémorisation, l'activité de réponse aux agressions numériques permet la capitalisation des connaissances dans l'entreprise. Ainsi, les connaissances acquises et mémorisées, émergeant de l'activité de réponse aux agressions numériques, constitue une ressource de valeur pour l'entreprise, et même un produit susceptible d’être vendu, puisque sa réplication sur d'autres entreprises est possible.

**Analyse des résultats concernant la facilité perçue d'utilisation de la méthode**

Les experts mentionnent la difficulté de réaliser (facilité d'utilisation) les trois étapes de la méthode à cause de la complexité du raisonnement surtout dans le cas des agressions inconnues par l'entreprise, et l'abondance des informations liée à l'étendue du champ d'investigation.
De même, le rôle du médiateur est perçu difficile et intimement dépendant des compétences et de la formation du médiateur. Certains experts soulignent même que la facilité d'utilisation de la méthode proposée est principalement liée à l'expertise du médiateur.

Par ailleurs, les experts sont tous d'accord sur l'aide que peut fournir l'outil informatique afin d'assister le travail de l'ERI.

Cependant, la facilité perçue d'utilisation de la méthode reste très dépendante de la réalisation de la base de données et de connaissances ainsi que de l'expertise des membres de l'ERI et du médiateur.

**Analyse des résultats par rapport à l'état des pratiques des experts rencontrés**

Ce qui diffère dans l'état des pratiques des entreprises contactées c'est l'étape d'initiation du traitement du signal/signe faible détecté et la convocation de l'ERI pour effectuer l'opération d'interprétation. La gestion de l'intervention de l'ERI et le rôle du médiateur sont également différents d'une entreprise à l'autre. Ceci est dû principalement à des différences au niveau de la structure et du fonctionnement de l'ERI.

**Enseignements tirés concernant la structure de l'ERI**

La réponse aux agressions numériques à travers le travail de l'ERI est une activité qui a été jugée comme étant fondamentale, par les experts rencontrés. Ils soulignent que sans ressources allouées à cette activité, ni outils adéquats ils sont en difficulté pour remplir leur rôle. Nous avons constaté l'existence très fréquente d'une structure minimale ne dépassant pas trois personnes, chargée de la tâche de réponse aux problèmes de sécurité. Il n'y a pas d'existence réelle d'une ERI mais plutôt d'une cellule qui s'occupe du travail d'une ERI.

L’organisation du travail d’une ERI, en termes de répartition des tâches et d’élaboration des mécanismes de coordination, est insuffisante aux yeux des experts rencontrés.

Les ERI dans les entreprises contactées ne disposent pas de procédures formalisées ni d’outils appropriés pour assister la démarche d’interprétation des signaux/signes faibles détectés.

**Enseignements tirés concernant le fonctionnement de l’ERI**

Tous les experts interviewés sont d’accord sur le fait que les informations de type signal/signe faible caractérisent bien les alertes et les anomalies détectées par les équipements ou les personnes et constituent le point de départ de travail d’une ERI.

Le travail de l'ERI requiert effectivement, selon eux, la création collective de sens à partir des signaux/signes faibles. Ils soulignent que la médiation, qu’ils découvrent parfois à l’occasion de l’entretien, joue un rôle important dans ce processus même si elle n’est pas visible.

La démarche d'interprétation n'est pas suffisamment formalisée dans les entreprises contactées. La définition des tâches et des responsabilités liées à la démarche d’interprétation des signaux/signes faibles n’est pas suffisamment visible comme fonction dans la structure de l’entreprise.

**Conclusion**

L’essor de la société numérique et le développement important des réseaux, et plus particulièrement de l’Internet, devraient faire de la sécurité du système d'information une priorité absolue pour les entreprises. Les enjeux financiers importants ajoutés au nombre croissant et complexe des agressions numériques, poussent les entreprises à développer des approches proactives et efficaces de sécurité afin de maintenir un niveau de sécurité optimal et de réagir le plus rapidement possible. Notre intérêt a porté sur le travail de l’ERI qui exige des outils et des méthodes de travail appropriés répondant à la nécessité de réduire le temps de réponse à une agression numérique et ce, dans le but, de minimiser les dégâts matériels et immatériels occasionnés par celle-ci.
Pour répondre à cette problématique de terrain, nous avons conçu MARRAN, assistée par une utilisation innovante de la technologie Internet, afin de pouvoir agir vite voire par anticipation

face au risque des agressions numériques. Cette réponse s'inscrit dans le cadre d'une recherche exploratoire.

Nous avons été amenés à choisir les entretiens semi directifs auprès des experts en sécurité pour l'évaluation de MARRAN. Cependant, l'évaluation qualitative de la méthode à travers les interviews doit être suivie par une évaluation quantitative qui requiert une période assez longue et variable d'une entreprise à l'autre. La période de l'apprentissage dépend aussi de l'état des pratiques dans le domaine de réponse aux agressions numériques. Une perspective intéressante de cette recherche serait la définition d'un certain nombre de **critères quantitatifs** dans le but de mesurer l'impact de l'implémentation de MARRAN sur l'activité de l'entreprise (en termes de gain sur le coût de sécurité, la gestion de la clientèle, la performance des services offerts…etc) ainsi que de mesurer la réactivité de l'ERI par rapport à des agressions nouvelles ou inconnues par l'entreprise. Ceci permet de voir dans quelle mesure la méthode proposée permet la gestion du flou voire de l'inconnu.

**Références**


Ab Hamid N-R., Kassim N., (2004), "Internet Technology as a tool in Customer Relationship Management", *Journal of American Academy of Business*, March, 4, p.103-108.

Ansoff I., (1975), "Managing strategic surprise by response to weak signals" *California Management Review*, 18 (2), p.21-33.

Argyris C., (1976), "Single-loop and double-loop models in research on decision making", *Administrative Science Quarterly*, 21 (3), p.363-375.

Ashmos D.P., Nathan M.L., (2002), "Team sense-making: a mental model for navigating uncharted territories", *Journal of Managerial Issues*, 14 (2), Summer, p.198-217.

Bitouzet Ch., (1999), *Le commerce électronique : création de valeur pour l'entreprise*, Hermès, 185p.

Bourgeois L. J., Eisenhardt K. M., (1988), "Strategic decision processes in high velocity environments: four cases in the microcomputer industry", *Management Science*, 34 (7), p.816-835.

Boyle B. A., (2001), "The Internet in industrial channels: the use in (and effects on) exchange relationships", *Journal of Business & Industrial Marketing*, 16, p.452-469.

Bradshaw D., Brash C., (2001), "Managing customer relationships in the e-business world: how to personalize computer relationships for increased profitability", *International Journal of Retail and Distribution Management*, 29, p.520-529.

Canavan, 2001

Caron-Fasan M.L., (1997), *Veille stratégique : Création de sens à partir de signaux faibles*, Thèse de Doctorat en Sciences de Gestion, École Supérieure des Affaires, Grenoble, 428 p.

Choo, 97

Daft et Weik 95

Drazin R., Glynn M.A., Kazanjian R.K., (1999), "Multilevel theorizing about creativity in organizations: a sensemaking perspective", *Academy of Management Review*, 24 (2), p.286-307.

Gorry A., Scott-Morton M. S., (1971), "A framework for management information systems", *Sloan Management Review*, 13 (1), p. 55-70.

Grandon E., Pearson J., (2003), "Strategic Value and Adoption of Electronic Commerce : An empirical Study of Chilean Small and Medium Business", *Journal of Global Information Technology Management*, 6 (3), p.22-43.

Hervier G., (2001), *Le commerce électronique*, Editions d'Organisations, 276p.

Killcrece G., Kossakowski K-P., Ruefle R., Zajicek M., (2003), *State of the Practice of Computer Security Incidents Response Teams (CSIRTs)*, Carnegie Mellon, 153p.

Lesca H., (2003), *Veille stratégique La méthode L.E.SCAnning*, Ed. ems Management et société, 190 p.

Lesca 83

Lesca 2001

Marmuse C., (1992), *Politique Générale : langages, intelligence, méthode et choix stratégiques*, Ed. Economica, 592 p.

Moore A. P., Ellison R. J., Linger R. C., (2001), *Attack Modeling for Information Security and Survivability*, Technical Note CMU/SEI, 33p.

Porter M., (1986), *L'avantage concurrentiel*, InterEditions, Paris, 647p.

Prax J.Y., (1997), *Manager la connaissance dans l'entreprise*, INSEP éditions, 270 p.

Rayport.J.F, Sviokla.J.J, (1995), "Exlpoiting the virtual value chain", *Harvard Business Review*, Nov-Dec, p.14-24.

Reix R., (1999), " Les technologies de l'information, facteur de flexibilité ?", *Revue Française de Gestion*, Mars-Avril-Mai, p.111-119.

Sadok M., Benabdallah S., Lesca H., (2003), "Apports Différentiels de l'Internet pour la Veille Anticipative : Application au cas de réponse aux Atteintes à la Sécurité des Réseaux d'entreprise ", *Actes du 8ième Colloque de l'AIM*, MAI, Grenoble, 8 p.

Sadok M., (2004), "Veille anticipative stratégique pour réduire le risque des agressions numériques", Thèse de Doctorat en Sciences de Gestion, Ecole Doctorale, CERAG, 220p.

Stallings W., (2000), *Network Security Essentials: Applications and Standars*, Prentice Hall, 366 p.

Venkatraman.N, Henderson.J.C, (1998), "Real Strategies for Virtual Organizing", *Sloan Management Review*, p.33-47.

Vermeulen C., Solms R. V., (2002), "The information security management toolbox-taking the pain out of security management", *Information Management & Computer Security*, 10 (3), p.119-125.

Weick K.E., (1995), *Sensemaking in Organizations*, London: Sage Publications, 231p.