Humbert LESCA, Moufida SADOK (2008) - Veille anticipative et sécurité des ressources informationnelles de l'entreprise à l'ère numérique. Colloque « *Le e-Management : Rupture ou continuité organisationnelle, Opportunités et risques majeurs ?* » AFME Association Francophone de Management Electronique, Grenoble (France), 27-28 mars 2008

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

Moufida SADOK
Enseignante - Chercheur
Institut Supérieur des Etudes Technologiques en Communications de Tunis
Moufida.Sadok@isetcom.rnu.tn
Humbert LESCA
Professeur émérite
CERAG UMR 5820 CNRS UPMF Grenoble
http://www.veille-strategique.org

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.

Mots clés : risque numérique, veille anticipative, signal faible, intelligence collective

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

Introduction

La sécurité des ressources informationnelles de l'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. Cependant, 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 à travers l'utilisation des solutions physiques et logicielles de sécurité adaptées à leurs besoins et en fonction des caractéristiques de leurs services offerts. Pourtant, 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 pirates informatiques sont de plus en plus inventifs. Le danger des agressions numériques pour une entreprise ne se limite pas à des pertes financières, mais il peut toucher également son image de marque ou son capital clients, ainsi que l'efficacité et la continuité de son activité. Les enjeux stratégiques 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. De ce fait, la pratique de la veille anticipative stratégique est confrontée dans cette recherche 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.
Toutefois, les ERI manquent de méthodes adéquates pour assister cette étape d'interprétation des informations collectées de type signal 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 adéquate.
Ainsi, les objectifs de ce papier se situent sur un triple plan. Il s'agit, d'abord, de montrer la nécessité de développement d'une approche proactive de gestion du risque numérique à travers la mise en place d'un système de veille anticipative. Ensuite, nous proposons le cadre conceptuel d'une Méthode d'Analyse et de Réduction du Risque des Agressions Numériques (MARRAN). Enfin, nous présentons les résultats d'évaluation de MARRAN par des experts en sécurité informatique en se basant sur certains indicateurs de mesure utilisés en systèmes d'information, notamment l'utilité perçue et la facilité d'utilisation.

1. Enjeux stratégiques des agressions numériques

Les développements importants en matière des technologies de l'information et de la communication (TIC) ont permis à l'entreprise de se disposer d'un ensemble de nouveaux moyens pour augmenter la flexibilité des processus de travail, réduire les coûts de coordination et gérer avec une relative facilité plusieurs activités à distance avec ses différents partenaires et même avec ses employés.

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 de son 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 leurs activités.

D'une façon générale, une agression est toute action compromettant la sécurité de 1'information d'une organisation (Stallings, 2000). La sécurité 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 (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 analyses et les statistiques effectuées récemment par le CERT (*Computer Emergency Response Team* www.cert.org), 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. De même, 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. 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.

De même, le douzième rapport annuel réalisé par le Computer Security Institute (www.gocsi.com) relatif à l'année 2007 sur l'état de sécurité dans plusieurs entreprises américaines opérant dans plusieurs secteurs d'activité indique que plus de 78% des entreprises interviewées reconnaissent avoir été victimes, au moins une fois, d'une attaque provenant de l'extérieur ou de l'intérieur alors que 23% sont incapables de savoir si elles ont été cibles d'attaques ou non. D'après ce même rapport, 44% des entreprises interrogées ont enregistré plus que dix incidents de sécurité qui ont ciblé leurs sites Web, alors que 56% sont incapables d'évaluer 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, les rapports publiés par ces organismes spécialisés officiels signalent que le vol des informations, la fraude financière, le déni de service, et les virus sont les agressions numériques qui ont causé les pertes financières les plus élevées et ce sur plusieurs années d'études consécutives. Le calcul des ces pertes demeure un exercice parfois très difficile pour certaines entreprises endommagées à cause du caractère complexe et incertain des agressions numériques.

2. Adaptation de la veille anticipative stratégique dans le cas de réponse aux agressions numériques

Le risque des agressions numériques est corrélé à l'incertitude de leurs occurrences. L'insuffisance des solutions techniques et physiques de sécurité, avec la complexité et l'imprévisibilité croissantes des agressions numériques, poussent les entreprises à développer des approches proactives de sécurité afin de pouvoir réagir rapidement et au bon moment. Par conséquent, il est nécessaire de collecter des informations de type signal faible (au sens de Ansoff, 1975) relatives à des alertes précoces liées à des problèmes potentiels de sécurité. Ces informations doivent avoir un caractère anticipatif 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 qui peut être 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 devoir trouver une application prometteuse dans le domaine de la sécurité des ressources informationnelles de l'entreprise. En effet, la veille anticipative stratégique (lesca, 2003) 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, 1999). Dans notre cas, la veille anticipative stratégique est un dispositif qui porte l'attention sur des nouveaux acteurs particuliers de l'environnement de l'entreprise, les pirates informatiques, dont les actions présentent un risque énorme pour l'efficacité et la continuité de son activité à l'ère numérique.

Dans le domaine de la sécurité, la veille anticipative est un système d'information dédié à l'aide à la protection des ressources informationnelles de l'entreprise en permettant la détection et l'analyse :

- Des agressions numériques qui ont été préalablement répertoriées (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.
- Des agressions numériques inconnues non encore répertoriées à travers l'analyse de certains signaux faibles collectés par des systèmes de détection, d'évaluer les dégâts potentiels occasionnés et de préparer une réponse appropriée et rapide à ces attaques.

Ainsi, 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 (au sens de Weick, 1995) 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.

La détection des signaux nécessite la présence d'une équipe capable d'interpréter, d'analyser et de traiter ces signaux 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'agressions. Cette interprétation nécessite une véritable intelligence collective (Lesca, 2001) 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 logicielles et physiques.

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

La conception et la construction de MARRAN (Sadok, 2004) sont issues d'une série d'observations du terrain et d'une articulation et extension de certaines connaissances théoriques et actionnables disponibles. 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 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 faible dans un contexte d'incertitude et d'urgence. 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 figure ci-dessous décrit les différentes phases de MARRAN.

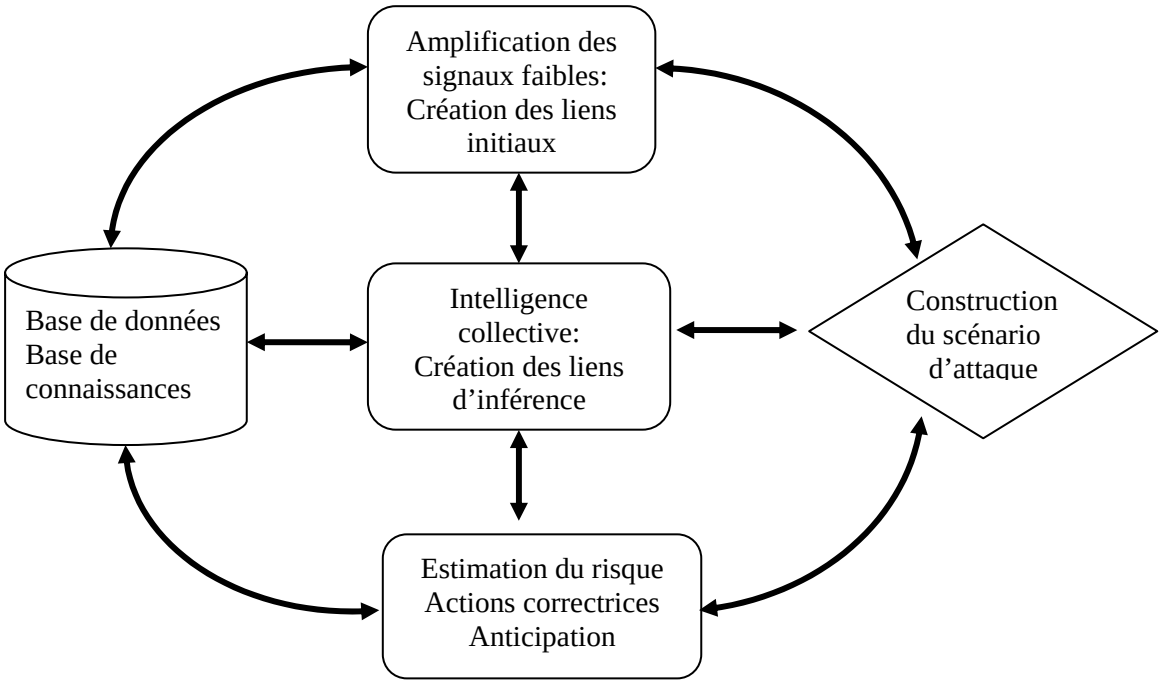

Figure 1 : Les phases de MARRAN

La première phase décrit l'activité de création des liens initiaux. Son objectif est d'amplifier le signal faible détecté et d'établir des liens capables de donner une première idée sur le risque 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 collectées. Celles-ci proviennent des signaux faibles amplifiés, des sources internes ou externes, ainsi que de la contribution des membres de l'ERI.

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 membres de l'ERI qui peuvent également extraire des informations documentaires prélevées dans des archives structurées et actualisées tout au long du processus, dans le but d'aboutir à une vision plus intelligible de la situation et la construction du scénario de l'attaque.

Il est important ici de signaler que 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.

Les liens probabilistes permettent d'élargir le champ du raisonnement alors que les liens dynamiques, variables en fonction du temps, permettent d'adapter le raisonnement au contexte et aux objectifs de la prise de décision.

Dans la troisième phase, des critères de satisfaction sont définis (par les membres de l'ERI et/ou les responsables qui auront à prendre la décision finale) 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,
- la compréhension des mécanismes qui ont généré les signaux faibles détectés, et
- l'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.

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 faibles ainsi que la trace de tous les liens inférés lors du processus d'intelligence collective.

4. Résultats empiriques de l'évaluation de MARRAN

L'évaluation de MARRAN, à travers le traitement des entretiens semi-directifs effectués auprès des experts en sécurité, vise principalement à affirmer l'utilité perçue et la facilité d'utilisation 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 sont chargés de surveiller d'une façon permanente le trafic sur le réseau de leur 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.
Tous les interviewés sont confrontés quotidiennement à des problèmes de sécurité et ils ont déjà pilotés des projets importants dans ce domaine. L'expérience des experts contactés varie entre cinq et dix ans.

4.1. 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 faible et la phase de mémorisation des raisonnements lors des constructions des scénarios d’attaques.

Les étapes d'amplification progressive des signaux 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 tout en signalant que l’output du processus collectif de création de sens dépend également de la méthode de travail utilisée et des compétences et des expertises des membres de l’ERI.

De même, 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 acquises 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 son efficacité.
A travers la mémorisation, l'activité de réponse aux agressions numériques permet la capitalisation des connaissances dans l'entreprise. Ainsi, les connaissances explicitées, formalisées et mémorisées, émergeant de l'activité de réponse aux agressions numériques, constitue une ressource de grande valeur pour l'entreprise, et même un produit susceptible d’être vendu, puisque sa réplication sur d'autres entreprises est possible.

4.2. Enseignements tirés concernant la facilité perçue d'utilisation

Tous les experts interviewés sont d'accord sur le fait que les informations de type signal faible caractérisent bien les alertes et les anomalies détectées par les équipements ou le personnel et constituent le point de départ de travail d'une ERI qui requiert effectivement, selon eux, la création collective de sens à partir des signaux faibles.
Toutefois, sur un plan pratique, ils mentionnent la difficulté de réaliser les trois étapes de la méthode à cause de la difficulté de détecter à temps les signaux faibles, l'abondance des informations liée à l'étendue du champ d'investigation et la complexité du raisonnement lors de la phase de création collective du sens surtout dans le cas des agressions inconnues par l'entreprise.

Par ailleurs, les experts sont tous d'accord sur l'aide que peut fournir certaines potentialités offertes par les TIC afin d'assister le travail de l'ERI. Ainsi, 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 et de l'expérience des membres de l'ERI.

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

Par rapport à l'état des pratiques, l'étape d'initiation du traitement du signal faible détecté et la convocation de l'ERI pour effectuer l'opération d'interprétation sont différentes d'une entreprise à une autre. La gestion de l'intervention, l'organisation et le fonctionnement de l'ERI sont également différents.

Sur le plan organisationnel, 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 seraient en difficulté pour remplir leur rôle. Nous avons constaté l'existence très fréquente d'une structure minimale ne dépassant pas trois personnes, chargées de la tâche de réponse aux problèmes de sécurité. Il n'y a pas d'existence réelle ou formelle 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'amplification et

d’interprétation des signaux faibles détectés. En outre, la définition des tâches et des responsabilités liées aux activités d’interprétation des signaux faibles n’est pas suffisamment visible comme fonction dans la structure de l’entreprise. Ceci est de nature à limiter l’apprentissage collectif qui pourrait en résulter.

Conclusion et perspectives de recherche

L’essor de la société numérique et le développement important des réseaux, et plus particulièrement de l’Internet, devraient faire de la sécurité des ressources en informations une priorité absolue pour les entreprises. Les enjeux financiers importants ajoutés au nombre croissant 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. Le travail de l’ERI s’inscrit bien dans ce cadre mais exige des méthodes et des outils 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 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 devant être ensuite poursuivie afin d’accroître progressivement la portée des résultats obtenus et ce, conformément à une démarche inductive et itérative.

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 le gain de réactivité de l’ERI par rapport à des agressions nouvelles ou inconnues par l’entreprise. Ceci permettrait de voir dans quelle mesure la méthode proposée permet la gestion du flou voire de l’inconnu.

Références

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

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 C. W., (1999), "The art of scanning the environment", *American society for information science*, 25(3), February/ March.

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 H., (2001), "Veille stratégique orientée signaux faibles : concept et méthode d'identification, retours d'expérience", *Actes du Colloque VSST'2001*, octobre, Barcelone, 20p.

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.

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.