

Apports Différentiels de l'Internet pour la Veille Anticipative : Application au cas de Réponse aux Atteintes à la Sécurité des Réseaux d'Entreprise

Moufida SADOK

Enseignante Universitaire

Iset'Com

Cité Elghazala 2083 Ariana Tunisie

(216) 71 85 70 00

Moufida.Sadok@isetcom.rnu.tn

Salah BENABDALLAH

Directeur Technique

Agence Nationale de Certification Électronique

3, bis Rue de l'Angleterre 1000 Tunis

(216) 71 35 94 07

Sba@certification.tn

Humbert LESCA

Professeur des Universités

ESA Université Pierre Mendès France

BP47-38040 GRENOBLE Cedex 9-France

(33) 04 76 82 54 85

humbert.lesca@esa.upmf-grenoble.fr

□ Résumé

La veille stratégique est un processus d'apprentissage et d'intelligence collective visant à réduire l'incertitude et à développer la capacité d'anticipation de l'entreprise face à son environnement changeant et imprévisible. La technologie Internet offre un support efficace et réactif à ce processus. Le présent papier discute des apports différentiels de l'Internet et traite le cas particulier de la réponse aux incidents de sécurité, activité qui répond à une démarche explicitée par ce processus.

Mots clés :

Veille anticipative, Intelligence collective, Technologie Internet, Attaque numérique, Réponse aux incidents de sécurité.

□ Abstract

Environmental scanning is an intelligent and adaptive process that helps companies to reduce business uncertainty and cope with unstable and unpredictable external events. The Internet technologies can provide an efficient and reactive support to this process. This paper addresses this issue and develops the particular case of security incident response, where the application of this process represents an appropriate activity.

Key-words :

Learning environmental scanning, Collective intelligence, Internet technology, Network security, Incident response.

Introduction

La veille stratégique est un système d'information permettant à l'entreprise de détecter et d'interpréter les événements de l'environnement extérieur susceptibles d'influer sa pérennité. En effet, l'écoute anticipative de l'environnement permet d'avoir un avantage informationnel important et nécessaire pour une action rapide au bon moment. Le processus de la veille stratégique implique la mise en place d'un dispositif d'intelligence collective au sein de l'entreprise qui englobe la veille anticipative et, en plus, comprend un processus de création de connaissances et de sens.

Par ailleurs, les développements relativement récents en matière des technologies de l'information et de la communication ont permis aux entreprises de se doter de nouveaux moyens et supports pour rechercher, structurer, échanger et diffuser de l'information en réduisant les contraintes en termes de temps et d'espace.

Dans ce cadre, l'Internet offre de multiples utilités pour soutenir et perfectionner les différentes phases du processus de la veille stratégique.

L'objectif de ce papier est de discuter et d'analyser les apports potentiels de l'Internet pour supporter et perfectionner les activités de veille anticipative et d'intelligence collective. L'accent sera mis particulièrement sur l'utilisation de la recherche approchée dans le processus d'intelligence collective tel que décrit par le modèle de (Lesca, 1997). Dans ce modèle, les phases de la mémorisation, l'accès/diffusion et la création de sens seront d'un intérêt particulier pour approuver l'approche préconisée dans ce papier.

Pour valider ce travail, une étude de cas sera développée autour du travail des équipes de réponse aux incidents (ERI) de sécurité des réseaux d'entreprise, domaine dans lequel le dispositif de veille anticipatif et intelligence collective serait d'un apport certain.

Ce papier est organisé comme suit. La première section est consacrée à la présentation du modèle de Veille Anticipative et Intelligence Collective (Lesca, 1997). Dans la deuxième section, les apports potentiels de l'Internet dans le processus de l'intelligence compétitive sont, d'abord, explicités à travers une revue de la littérature récente pour signaler, ensuite, certaines lacunes dans ce domaine de recherche. La troisième section identifie les objectifs et les apports de la recherche approchée dans le processus de l'intelligence collective particulièrement pour la phase de création de sens. La quatrième section traite une étude de cas portant sur les mécanismes de réponse aux incidents de sécurité des réseaux, pour valider empiriquement le dispositif de veille anticipatif et intelligence collective supporté par Internet. La

conclusion résume l'essentiel de ce papier avec une discussion de certaines voies futures de recherche.

1. Présentation du modèle Veille Anticipative et Intelligence Collective (VA-IC)

La veille stratégique, re-qualifiée aujourd'hui d'intelligence stratégique ou d'intelligence compétitive, désigne le processus informationnel par lequel l'entreprise se met à l'écoute anticipative des signaux faibles de son environnement socio-économique dans le but créatif de découvrir des opportunités et de réduire son incertitude (Lesca et Schuler, 1998).

Le processus de la Veille Stratégique apparaît comme étant un processus d'apprentissage collectif, itératif et créatif de connaissances et de sens face aux stimuli que l'entreprise reçoit de son environnement externe.

Au sein de l'entreprise, l'intelligence collective traduit la capacité des individus à se procurer des informations à caractère anticipatif concernant l'environnement externe, à sélectionner certaines d'entre elles selon des critères, à relier ces informations entre elles et à établir des combinaisons selon certaines règles en vue de créer du sens pour la prise de décision.

Ainsi, un dispositif de «Veille Anticipative et Intelligence Collective» doit permettre aux preneurs de décision d'agir au bon moment, rapidement et efficacement en assurant la traçabilité des informations depuis leur captage jusqu'à leur exploitation pour l'action.

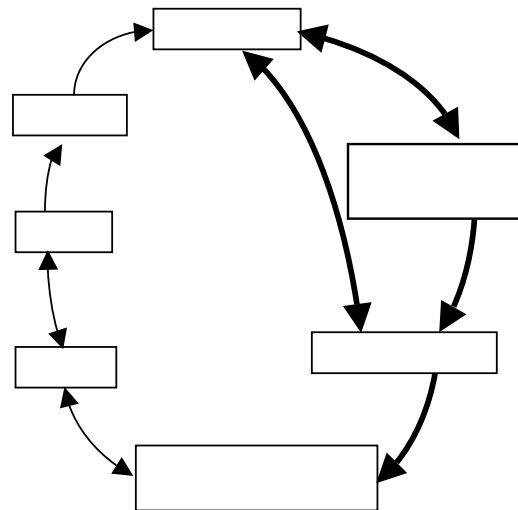


Figure 1 : Veille Anticipative et Intelligence Collective
© Lesca

Le Ciblage : C'est l'opération qui vise à définir et à délimiter la partie de l'environnement externe de l'entreprise sur laquelle il faut cibler les efforts de la veille stratégique.

La phase du ciblage s'apparente également à définir les besoins en information et donc l'identification des sources (formelles et informelles) à scruter susceptibles de fournir les informations ciblées.

La Traque : C'est l'opération par laquelle les informations de la veille anticipative sont procurées. Le traqueur ou le capteur « gatekeeper » est la personne qui a pour rôle d'aller au devant de ces informations et de les rendre disponibles dans l'entreprise.

La Remontée : c'est l'opération par laquelle un traqueur fait parvenir les informations recueillies à la personne chargée de les stocker. Le dispositif de remontée nécessite que le traqueur dispose d'un moyen matériel approprié pour transmettre les informations, facile d'accès et d'utilisation.

La Mémorisation : La mémorisation qualifiée également par le stockage intelligent est nécessaire pour valoriser et exploiter les informations collectées de la veille anticipative. Le stockage intelligent permet la mise en forme des informations et leur classement dans des bases de données pour pouvoir les retrouver à tout moment prêtes à être utilisées. Le plan de classement reprend les thèmes et les acteurs, qui sont les mots clés principaux, et affine les détails. L'affinage se fait en fonction de la liste des mots clés résultant du ciblage de la veille stratégique. Cependant, la liste des mots clés n'est pas définitive ou statique et elle peut évoluer en relation avec l'évolution du ciblage.

La Création de sens : C'est la phase cruciale du processus qui consiste à traiter et à interpréter d'une façon inductive les informations de veille stratégique ou encore à créer des liens significatifs entre informations fragmentaires, ambiguës et incertaines au cours d'interactions avec des mémoires individuelles et collectives.

Il s'agit de l'opération collective au cours de laquelle sont créées de la connaissance et du « sens ajouté » de façon à créer des champs possibles pour l'entreprise.

Diffusion /Accès : La diffusion est l'opération qui consiste à mettre les informations élaborées, résultant des séances de création de sens, à la disposition des utilisateurs finals autorisés, souvent des responsables opérationnels. De même, un utilisateur potentiel peut prendre l'initiative d'aller vers l'information s'il éprouve le besoin de disposer de certaines informations qu'il est capable de désigner ou bien qui lui ont été recommandées par d'autres utilisateurs. Dans ce cas de figure, il s'agit de la phase d'accès aux informations.

Action : Si les informations traitées sont suffisamment significatives, elles peuvent être intégrées dans le

processus décisionnel. Si par contre, les informations traitées ne permettent pas une vision assez claire, elles peuvent être complétées en relançant une nouvelle requête des informations manquantes.

2. Utilisation de l'Internet pour l'Intelligence Compétitive :

2.1 État de l'art :

L'intérêt de la littérature pour une utilisation des potentialités techniques de l'Internet dans le processus de l'intelligence compétitive est relativement récent. En effet, l'Internet est de plus en plus considéré comme étant une source riche et variée d'informations qui peuvent concerner plusieurs domaines (Brabston et McNamara, 1998) et par la suite un véritable accélérateur de l'intelligence stratégique définie comme étant la mise en œuvre "des dispositifs efficaces afin de collecter, traiter et diffuser les informations pertinentes et fiables indispensables à la prise de décision" (Reveli, 1998).

Cependant, son utilisation comme outil de recherche ou de collecte est relativement plus appropriée à l'acquisition de l'information concernant l'environnement général plutôt que l'environnement spécifique. Ceci est expliqué par le fait que l'information disponible sur Internet est obtenue de sources secondaires comme la presse, les revues et certaines publications et rapports spécialisés (Pawar et Sharda, 1997).

Aguilar (1967) distingue entre quatre modes de recherche de l'information dans le cadre d'une activité de scanning : la recherche non directive, la recherche conditionnée, la recherche informelle et la recherche formelle. Pawar et Sharda (1997) associent à chacun de ces modes un service Internet approprié. Ainsi, les Gophers et le WWW sont utilisés pour une recherche exploratoire, accéder à un site spécifique, et par la suite ils conviennent aux quatre modes de recherche mentionnés par Aguilar (1967).

Par ailleurs, Teo (2000) et Teo & Choo (2001) ont proposé un modèle décrivant l'impact de l'Internet sur l'efficacité et la qualité des différentes phases d'un dispositif d'intelligence compétitive composé de trois étapes : la recherche primaire et secondaire de l'information externe, la collaboration interne et externe, et la diffusion d'intelligence interne et externe.

Les résultats empiriques de leurs études ont prouvé une relation positive entre la qualité de chacune de ces phases et les fonctionnalités de l'Internet. En effet, les utilités et les fonctionnalités de l'Internet semblent améliorer la qualité de l'information qui est mesurée à travers dix dimensions : la précision, le contenu, la perfection, l'actualité, l'importance, la pertinence, la fiabilité, l'utilité, l'opportunité, understandability. L'amélioration de la qualité de l'information nécessaire à l'intelligence compétitive permet d'avoir un avantage

concurrentiel en générant plus de revenus, en réduisant les coûts et en permettant une meilleure efficacité du management.

Chen et al. (2002) proposent un outil qui supporte certaines phases du processus de l'intelligence compétitive appelé, Competitive Intelligence Spider, et qui dépasse les insuffisances des moteurs logiques disponibles sur Internet en offrant des possibilités plus importantes pour une collecte en temps réel des pages Web spécifiées par l'utilisateur, une structuration et une indexation des documents collectés utiles pour l'analyse des sites Web dont le contenu et l'évolution intéressent le veilleur.

Plusieurs autres études se sont intéressés aux avantages des agents intelligents (Maes, 1994 ; Liu, 1998) pour les activités de scanning liées particulièrement à la recherche et à la diffusion des informations.

Ces travaux théoriques et empiriques mettent en évidence le rôle de plus en plus important que peut jouer l'Internet dans le processus de veille stratégique. Cependant, son utilisation reste encore limitée et surtout liée à la recherche et à la collecte des informations. La proposition d'outils pratiques d'utilisation de l'Internet pour supporter le processus d'intelligence collective afin de développer une capacité d'anticipation reste limitée. Notre principal objectif à travers ce travail est de proposer un modèle basé sur la technologie Internet permettant la constitution et l'exploitation d'une mémoire organisationnelle en explicitant le fonctionnement du processus d'intelligence collective qui permet de synthétiser et de mettre en relation des informations éparses.

2.2 Les apports différentiels de l'Internet pour le processus de VA-IC :

D'une façon générale, la technologie Internet est caractérisée par quatre principaux concepts qui peuvent être utiles aux différentes étapes d'un processus d'intelligence collective :

1. un outil d'accès à une information interne et/ou externe distante (en termes de temps et d'espace) et quel que soit son support (texte, son, image)
2. un mécanisme de structuration des informations (collectées et/ou déduites) dans des bases de données en utilisant des liens d'hierarchisation et de dépendance ainsi que des critères de regroupement et ce par la création de liens hypertexte et d'adresses URL.
3. un mécanisme de recherche d'informations grâce à des moteurs de recherche (comme les opérateurs logiques) fonctionnant par mots clés ou des expressions et en opérant des liens sémantiques
4. un mécanisme de contrôle d'accès qui permet de mettre en œuvre des politiques d'accès, d'authentification et d'autorisation aux ressources

de l'entreprise et qui garantit la traçabilité des accès, des actions opérées sur les ressources et de l'évolution des actions opérées sur les ressources.

Ainsi, ces services contribuent d'une façon efficace et rapide à un stockage intelligent et dynamique des informations collectées avec la création de liens utiles à une structuration et une hiérarchisation significatives de celles-ci. Ils permettent également la définition d'une politique d'accès, en fonction de la contingence de la tâche du veilleur, aux informations et connaissances stockées ainsi que la recherche de certaines informations en cas de besoin. Cette approche permet également une capitalisation des connaissances lorsque, en plus des informations proprement dites sont stockés également les commentaires exprimés par les experts, ainsi que les validations éventuelles remontant des opérationnels. Ceci permet la traçabilité de l'évolution de la base des connaissances et par la suite la constitution d'un véritable catalyseur de l'apprentissage organisationnel.

Il nous paraît aussi que la technologie Internet peut contribuer à la création de valeur ajoutée à l'information capable de contribuer à la prise de décision. L'utilisation de la technologie Internet comme support au processus d'intelligence collective répond aux besoins des preneurs de décision de disposer d'outils efficaces et rapides en permettant :

- une structuration systématique et dynamique des informations. En effet, la section suivante montre l'apport d'une base de connaissances associée aux procédures de structuration et dont le rôle est de mémoriser les liens dynamiques pouvant être créés lors du processus d'Intelligence Collective et en traçant l'évolution du processus d'induction.
- un traitement significatif des informations. En effet, un certain nombre de règles de recherche (de nature exacte, probabiliste, ou approchée) seront développées dans la suite permettant de créer des liens dynamiques, sémantiques et/ou probabilistes pour assister la phase de création de sens en aidant à une meilleure compréhension des problèmes posés.

Par ailleurs, l'intégration du processus de VA-IC supporté par Internet présente des qualités capables d'intéresser les entreprises désireuses de développer une capacité d'anticipation. Ces qualités incluent la fiabilité, la flexibilité et la généralité. En effet, ce processus garantit une fiabilité acceptable dans la mesure où il permet une traçabilité de l'information et une réactivité importante. La flexibilité se traduit en termes d'adaptabilité aux aspects structurels et organisationnels de l'entreprise, d'adaptabilité aux modifications structurelles de l'information et d'adaptabilité aux modifications observées dans règles de prise de décision. En fin, ce processus vérifie les conditions de généralité en termes d'applicabilité à des types d'activités et/ou de problèmes traités différents.

3. L'apport différentiel des mécanismes de recherche approchée pour la phase de création de sens

3.1 Structuration de l'information

Le stockage des informations suppose la disposition d'un plan de classement multicritère ainsi que la définition d'un certain nombre de liens entre les informations stockées au sein d'un regroupement donné. Le regroupement permet d'avoir un stock informationnel plus riche, plus synthétique et/ou plus générique.

Le classement d'une nouvelle information dans un regroupement déjà existant autour d'un thème se fait, généralement, selon trois types de critères (Lesca et Caron, 1995) :

- Critère de similitude : les informations peuvent être regroupées par similitude lorsqu'elles expriment la même idée ou lorsqu'elles traitent d'un même thème.
- Critère de proximité : qui signifie que l'information est proche du thème auquel on va la rattacher comme le fait d'avoir une caractéristique commune.
- Critère d'analogie : les informations peuvent être regroupées par analogie (directe ou symbolique) lorsqu'elles sont associées sur la base de ressemblances constatées.

L'instrumentation de ces critères de regroupement en vue de les rendre opérationnels est une opération nécessaire et importante pour un stockage intelligent.

Dans ce cadre, la structuration classique des informations dans des bases de données présente plusieurs insuffisances. En effet, cette structuration se caractérise par l'existence de liens statiques et déterministes ce qui implique des possibilités limitées de recoupement et d'enrichissement des informations nécessaires pour générer de la signification. De plus, les mécanismes de recherche de type recherche exacte ne satisfont qu'à un pourcentage faible les critères de similitude, de proximité et/ou d'analogie entre les informations stockées.

Cependant, la diversité et la complexité du contexte des entreprises exige la formulation de liens dynamiques et variables en fonction d'un certain nombre de paramètres non figés. Ces liens doivent tenir compte du contexte temporel et de l'évolution des problèmes traités liés à l'évolution du ciblage ou aux contraintes. En effet, la veille anticipative est un système d'information particulier de l'entreprise, dédié à l'aide à la décision d'un certain type : de nature non répétitive, non programmable (heuristique au sens de Simon), dont l'enjeu peut être grand pour l'entreprise et prise dans un contexte d'incertitude.

Prenons l'exemple d'un lien d'influence entre deux informations, ce lien peut évoluer dans le temps pour devenir un lien d'opposition ou de causalité si l'acteur ciblé change de stratégie ou le thème objet de ciblage connaît d'autres contraintes. L'instrumentation des liens de regroupement doit être capable d'appréhender et de tracer cette évolution avec la mise en œuvre d'une typologie de liens de raisonnement pour organiser les informations disponibles sous forme d'une connaissance signifiante. Ceci peut être accompli par la séparation entre la mémorisation des informations et le traitement des liens. Ainsi, une base de données peut être utilisée pour stocker les informations regroupées selon des liens statiques et une base de connaissances opérant sur des liens dynamiques, des outils de représentation des liens et des outils heuristiques permettant la recherche des liens optimisés et la traçabilité de leur évolution.

La technologie Internet permet de répondre à ces besoins par l'emploi de mécanismes de stockage de l'information en hypertexte (liens statiques, recherche exacte et approchée), la manipulation de liens dynamiques à travers des moteurs d'inférence qui sont des outils qui permettent de faire de la déduction automatique à partir d'hypothèses et de règles de déduction approchée à travers la création de liens sémantiques et/ou probabilistes. Elle permet aussi la gestion de bases de connaissances implémentant des heuristiques de raisonnement appropriées aux liens stockés.

Ainsi, grâce aux capacités et possibilités étendues de stockage, de recherche et de traçabilité, l'Internet permet non seulement la gestion d'une base de données mais également la constitution et l'exploitation d'une base de connaissances qui témoigne de l'évolution de l'apprentissage organisationnel.

3.2 Création de valeur ajoutée à l'information

La phase de création de sens fait nécessairement intervenir plusieurs acteurs (experts et responsables de l'entreprise) et traduit leur capacité à créer et à manipuler des liens d'influence et/ou des relations d'opposition entre informations éparses stockées à un moment donné et sélectionnées (Lesca et Caron, 1995) afin de créer des champs possibles pour l'action ultérieure des opérationnels. La création et la manipulation des liens entre les informations peuvent être induites soit d'une façon automatique suite à une consultation de la base de connaissances et à travers des interactions de mémoires individuelles et collectives, soit par des raisonnements collectifs et créatifs sur les liens.

Par analogie, ce processus peut être comparé à un jeu de puzzle consistant à regrouper des pièces incomplètes et en désordre avec la différence qu'il ne s'agit pas de reconstituer quelque chose qui existerait déjà et la non

disposition de toutes les pièces. L'output de la co-construction du puzzle dépend de la capacité des acteurs d'ajouter du sens aux informations éparses, fragmentaires et incertaines. Pour assister cette phase, un système de création de valeur ajoutée supporté par la technologie Internet appelé ,e-puzzle, et composé de cinq modules se présentant comme suit :

- **Module « mémorisation des informations »** : il est utilisé pour la mémorisation des informations collectées et des liens intermédiaires.
- **Module « sélection multicritère des informations »** : cette sélection est multicritère en utilisant des opérateurs de recherche exacte/approchée permettant progressivement de construire des requêtes et de les affiner jusqu'à ce que les acteurs du processus soient satisfaits du lien généré.
- **Module « construction des puzzles »** : c'est la phase de raisonnement sur les liens. L'utilisateur peut travailler soit sur un lien déjà construit extrait de la mémoire afin de le mettre à jour ou de l'affiner, soit établir un nouveau lien. Dans le cadre d'une nouvelle création de liens, les acteurs peuvent procéder à une association d'informations automatiquement proposée par l'outil et obtenue en association avec les liens stockés suite à l'emploi de moteurs de recherche approchée, soit ils le construisent eux-mêmes en fonction de leur propre raisonnement.
- **Module « gestion du processus »** : il permet de gérer en temps réel les différentes données présentes dans la base ainsi que les liens créés. Le gestionnaire du processus peut ajouter, réduire ou supprimer des liens déjà construits, des sélections et des informations.
- **Module « recherche exacte/approchée »** : les mécanismes de recherche permettent d'extraire l'information (locale ou externe) selon des liens d'influence, d'opposition, sémantiques, et/ou probabilistes.

Le déroulement du processus de création de valeur peut se faire virtuellement en abolissant les contraintes temporelles et spatiales.

La figure 2 représente les liens d'interopérabilité entre les cinq modules de l'e-puzzle.

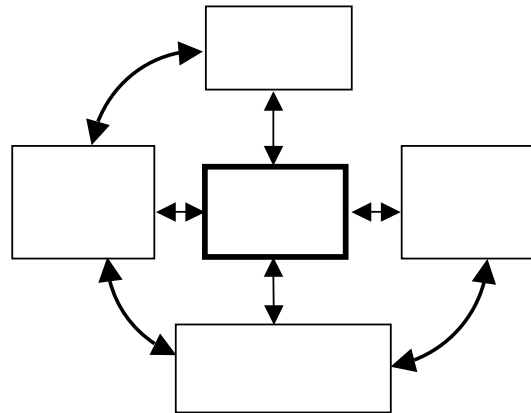


Figure 2 : les relations d'interopérabilité entre les modules de l'e-puzzle

4. Étude de cas : Application du dispositif de VA-IC dans la réponse aux incidents de sécurité des réseaux d'entreprise

4.1 La sécurité des réseaux d'entreprise

Dans une optique de mesure d'efficacité du processus VA-IC en termes de fiabilité, flexibilité et généralité, nous proposons de faire une application dans le cadre de la réponse aux incidents de sécurité (atteintes à la sécurité) observés sur un réseau propre à une entreprise.

La veille anticipative, dans ce domaine, est un système d'information dédié à l'aide à la protection des ressources de l'entreprise. Elle permet la détection automatique des attaques numériques qui ont été préalablement répertoriées et la prise de décision relative à la réponse à ces attaques compte tenu de leur impact sur l'activité de l'entreprise. Ce même processus permet de caractériser les attaques non répertoriées à travers l'analyse de certains signaux faibles collectés par des systèmes de détection (tels que les systèmes de détection d'intrusion), d'évaluer les dégâts potentiels occasionnés et de préparer une réponse appropriée et rapide à ces attaques.

Les attaques non répertoriées sont essentiellement de nature à générer des décisions d'un certain type : de nature non répétitives, non programmables, dont l'enjeu peut être grand pour l'entreprise et prises dans un contexte d'incertitude.

En effet, une attaque est toute action compromettant la sécurité de l'information d'une organisation (Stallings, 2000). Certaines propriétés des systèmes de communication rendent les attaques numériques plus dévastatrices que les attaques usuelles dans la mesure

où elles sont difficiles à détecter. Ces propriétés incluent :

- le caractère automatique des activités de la chaîne de valeur,
- la possibilité d'effectuer des actions à distance,
- la possibilité de faire propager les effets d'attaques,
- la facilité de dissimuler l'identité de l'attaquant

D'après le rapport annuel 2002 de CSI/FBI (Power, 2002), 74% des sociétés consultées ont rapporté que l'Internet est le point d'attaque le plus fréquent alors que 33% des sociétés ont signalé que les attaques sont de l'intérieur tandis que 12% des sociétés ont identifié des attaques qui ont transitées à travers des connexions distantes.

D'après ce même rapport, les types d'attaques détectées les plus sévères sont :

- Déni de service : 40 % des entreprises.
- Accès non autorisé par des utilisateurs internes : 38 % des entreprises.
- Virus : 85 % des entreprises.
- Accès réseau et abus de service Internet: 78 % des entreprises.
- Pénétration des Systèmes d'information de l'entreprise : 40 % des entreprises.

Ces attaques ont engendré des pertes financières énormes pour les entreprises consultées. En effet, la perte financière totale est estimée à 456 millions de dollars pour l'année 2002. Ces enjeux financiers importants ajoutés au nombre croissant et complexe des attaques, obligent les entreprises à développer des politiques puissantes et efficaces de sécurité basées en particulier sur la réactivité d'une équipe de réponse aux incidents de sécurité (ERI).

4.2 Rôle des ERI

Les ERI de sécurité sont chargées d'identifier les attaques (à travers la collecte de signaux faibles émis par les systèmes de détection d'anomalies), agir de façon à réduire l'impact des attaques en évaluant les dégâts et en prenant les décisions relatives à la protection des ressources sensibles de l'entreprise ainsi que d'anticiper la propagation de leurs effets. Le travail des ERI est complémentaire à celui des équipes qui administrent les réseaux de communication et qui y implémentent les mécanismes de sécurité. Les ERI doivent agir conformément à une politique de sécurité claire et définie et qui peut s'intégrer dans le cadre d'un processus de VA-IC.

En effet, les tâches essentielles accomplies par les ERI sont :

- La notification (mémorisation temporaire) : tout incident doit être notifié à temps et communiqué aux personnes et/ou aux départements concernés.

- L'analyse dont l'objectif est d'étudier les causes de l'incident et les conséquences de son avènement ainsi que l'étude des liens éventuels avec les incidents antérieurs.
- La réaction des ERI qui doivent prendre des actions concrètes et de stopper ou limiter l'impact de tout incident détecté en tenant compte de la spécificité de l'entreprise. Cette réaction doit être rapide, efficace et réalisée collectivement.
- La documentation et la traçabilité (mémorisation) : chaque incident de sécurité doit être documenté d'une façon convenable et publié dans des sites de telle façon que l'étude de son impact et des conditions de sa réalisation soient possibles à tout moment (West-Brown, Stikvoort et Kossakowski, 1998).

Pour soutenir cette activité des ERI, une base d'informations pour accompagner la génération de liens est nécessaire à l'analyse des attaques et aux choix de réponse aux incidents de sécurité. Cette base comporte une première composante, géographiquement répartie, fournissant une information complète sur les attaques répertoriées dans des sites génériques (i.e. Allen, 2001) ou dans des sites internes à l'entreprise. La deuxième composante est une base de liens entre les attaques, les informations utiles à l'analyse des signaux faibles pouvant représenter des attaques, des ressources de l'entreprise et les choix en matière de prise de décision. Dans la suite, nous donnons deux exemples de liens :

- Le premier exemple décrit le cas d'un Déni de Service probable qui consiste à la détection de trois signaux faibles qui indiquent trois types de tentatives d'accès au réseau de l'entreprise répétées (dans un intervalle de temps réduit) vers trois ressources différentes et provenant de la même adresse. Il y a dans ce cas une forte probabilité d'attaque distribuée visant le blocage d'un service offert par l'entreprise. Une solution de résolution de cette attaque est d'ordonner au firewall l'arrêt temporaire (ou définitif) de tout trafic provenant de la source en question (même s'il s'agit d'une source appartenant à un partenaire économique).
- Le deuxième exemple décrit le cas d'une intrusion non autorisée en constatant des accès non autorisés vers des services sensibles de l'entreprise. L'étude du trafic montre que ces accès sont internes et que le traçage des fichiers d'accès montre que des éléments nécessaires à l'authentification des utilisateurs d'un autre service de l'entreprise ont été lus. Une décision possible serait d'arrêter le service cible momentanément jusqu'à ce que les éléments d'authentification soient changés, et ceci quelque soit la perte occasionnée par l'arrêt (qui peut être partiel ou total) du service.

Conclusion

La technologie Internet présente un intérêt certain pour supporter les différentes phases d'un processus de VA-IC et ce à plusieurs niveaux. D'abord, la constitution d'une mémoire organisationnelle à travers la traçabilité de l'apprentissage collectif lors des traitements des informations de veille anticipative, ensuite l'aide à la décision en permettant de développer des heuristiques et d'établir des liens de raisonnement dynamiques.

Références

- Aguilar F. J. (1967), *Scanning the business environment*, New York, Macmillan.
- Allen J. H. (2001), *The CERT guide to system and network security practices*, Addison Wisley.
- Brabston M-E. et McNamara G. (1998), « The Internet as a competitive knowledge tool for top managers », *Industrial Management & Data Systems*, Vol. 4.
- Chen H., Chau M. et Zeng D. (2002), "CI Spider : a tool for competitive intelligence on the Web", *Decision Support systems*, vol. 34.
- Lesca H. (1997), *veille stratégique : concepts et démarche de mise en place dans l'entreprise*, DISTNB.
- Lesca H. et Caron M-L. (1995), « Veille stratégique : créer une intelligence collective au sein de l'entreprise », *Revue Française de Gestion*, Septembre-Octobre.
- Lesca H. et Schuler M. (1998), « Veille stratégique : comment ne pas être noyé sous les informations », *In Economies et Sociétés*, Série Sciences de Gestion, n°2.
- Liu S. (1998), « Strategic scanning and interpretation revisiting: foundations for a software agent support system-Part 2 : scanning the business environment with software agents », *Industrial Management & Data Systems*, Vol. 4.
- Maes P. (1994), « Agents that reduce work and information overload », *Communications of the ACM*, n°7, vol. 37, july, pp. 31-40.
- Pawar B. S. et Sharda R. (1997), « Obtaining business intelligence on the Internet », *Long Range Planning*, Vol. 30 (1).
- Power R. (2002), « 2002 CSI/FBI Computer Crime and Security Survey », *Computer Security Issues & Trends*, Vol. VIII, No. 1, Spring.
- Revelli C. (1998), *Intelligence stratégique sur Internet*, Dunod.
- Stallings W. (2000), *Network Security Essentials : Applications and Standards*, Prentice Hall.
- Teo T.S.H. (2000), « Using the Internet for competitive intelligence in Singapore », *Competitive Intelligence Review*, Vol. 11(2).
- Teo T.S.H. et Choo W. Y. (2001), « Assessing the impact of using Internet for competitive intelligence », *Information Management*, Vol. 39.
- West-Brown M. J., Stikvoort D. et Kossakowski K. P (1998), *Handbook for Computer Security Incident Response Teams (CSIRTs)*, Carnegie Mellon University/Software Engineering Institute, December.