A N D S I

Association Nationale des Dirigeants en Sciences de l'Information
www.andsi.fr

Intelligence Économique avec Alain Juillet ; actions et protections des DSI.

Compte rendu rédigé par ANDSI & Pierre Delort

En bref…

Alain JUILLET proposera un exposé relatif à l'Intelligence Économique et analysera les différentes composantes que cette notion revêt. Cette présentation sera suivie d'un débat, portant notamment sur les actions et protections que les DSI peuvent mettre en œuvre dans le cadre de leurs fonctions.

L'Association Nationale des Directeurs des Systèmes d'Information organise des débats et en diffuse des comptes-rendus, les idées restant de la seule responsabilité de leurs auteurs. Elle peut également diffuser les commentaires que suscitent ces documents.

Introduction

Alain JUILLET évoque la crise sanitaire actuelle. Les trois vagues successives laissent apparaître des facteurs communs :

- impréparation totale ;
- pilotage à vue ;
- organisation dépassée ;
- gestion erratique des moyens.

En matière d'Intelligence Economique (IE), l'impréparation conduit toujours à des situations non maîtrisables et à de la sur réaction, dont les conséquences sont coûteuses sur le long terme.

L'intelligence économique ?

Il apparaît indispensable d'anticiper les menaces et les opportunités qui pèsent sur l'environnement. L'IE consiste alors à mieux savoir afin de mieux anticiper. Elle repose sur la recherche, la collecte et le traitement d'informations pour détecter des tendances, des attentes et de nouveaux besoins, les actions et l'état de la concurrence, mais également l'évolution de l'environnement. L'IE permet de réduire la marge d'erreur dans les choix et les actions entreprises.

Dans un monde hyperconcurrentiel, il est apparu que les méthodes utilisées par l'IE fonctionnaient dans de très nombreux domaines d'activité : miliaire, politique, économie, juridique ou sportif. L'IE n'est plus l'apanage du seul secteur économique.

La veille

La veille correspond à la surveillance de ce qui se passe dans un cadre défini. Elle peut être thématique, globale ou ciblée. Elle permettra, en permanence, de détecter toutes les modifications du « dossier de base » qui a été constitué en amont.

La constitution d'un dossier de base, la pratique de la veille et le croisement des deux conduisent à la détection de « signaux faibles », ce qui donnera un avantage compétitif, concurrentiel.

Le monde est complexe et regorge d'informations. Dans l'univers numérique actuel, entre 90 et 95 % des informations sont disponibles par des moyens légaux, dans tous les domaines.

Le vrai problème actuel n'est plus de collecter les données, mais de sélectionner les plus utiles pour en faire une synthèse diffusée très rapidement à ceux qui en ont besoin. Plus le volume de données traitées est significatif, plus la marge d'incertitude est réduite. Dans les grands laboratoires de recherche sur le numérique, à l'instar de Google, l'incertitude a été réduite à environ 10 %. L'IE correspond à un atout considérable pour la compétitivité des entreprises dans la mesure où cela leur permet d'accroître leur efficacité.

Un préalable indispensable consiste à se connaître parfaitement pour bâtir des stratégies gagnantes. Cette connaissance suppose un bilan de l'existant et une analyse contradictoire qui passe par l'identification de ses défauts. Dans les années 1980, le *benchmarking* importé des États-Unis mettait en oeuvre ce premier principe de l'IE.

L'IE permet de comprendre toutes les spécificités de chacun des environnements, d'identifier les tendances et de regarder ce qui se passe. Mais le risque permanent est de se laisser piéger par des biais cognitifs, c'est-à-dire de nier la réalité, et ce, pour des raisons idéologiques, morales, politiques ou d'égo. A titre d'illustration, un biais cognitif renvoie actuellement au refus du monde occidental de reconnaître la valeur de vaccin russe « Spoutnik » contre le Covid-19. L'IE apporte de nombreuses informations que nous ne pourrions pas voir.

A ce jour, 20 % des informations lues ou entendues quotidiennement sont fausses du fait du mode de fonctionnement du système médiatique. Il apparaît alors indispensable d'apprendre à éviter les *fake news* en recoupant les informations. Le recours à des réseaux permet aussi de résoudre cette difficulté. Les Asiatiques, les Allemands ou les Américains utilisent cette méthode qui correspond à leurs gènes, contrairement aux Européens du sud et plus généralement aux Méditerranéens en raison de leur caractère individualiste.

L'IE doit inclure une vision à moyen et long terme. Une entreprise ne peut pas être gérée sur un seul horizon de court terme. L'IE permet alors de détecter les évolutions, ce qui permettra aux entreprises de bâtir leur vision du futur et leurs adaptations aux évolutions permanentes.

La Sécurité

Le combat concurrentiel moderne oblige les acteurs à développer des stratégies offensives ou défensives en fonction de la situation. Une réflexion doit être conduite à propos de la sécurité des informations. Cela pose la question de la diffusion des informations à l'extérieur de l'entreprise et donc du concept du secret d'entreprise. Par exemple et selon les lois américaines, toute information passant par une entité américaine (serveur, dollar, banque, société, etc) peut être récupérée et utilisée. Il est nécessaire de collecter et de conserver les datas en Europe.

Avec l'arrivée du numérique, les possibilités d'acquisition d'informations de tous genres, d'actions de déstabilisation des personnes et des entreprises, de détournement ou de pillage de données sensibles, ou simplement d'opérations criminelles sont devenues faciles à réaliser. Il est possible de poser des barrières, mais jusqu'à un certain point. Face à un attaquant qui maîtrise les meilleures techniques, le défenseur doit savoir évoluer du *firewall* au SOC, et maintenant du VPN à l'*Endpoint Detection and Response* s'il veut éviter d'être victime. Il incombe en permanence de réaliser des investissements qui sont onéreux tandis qu'il est parfois complexe de convaincre les dirigeants de cette nécessité.

La communication d'influence

L'IE ne se limite pas au traitement de l'information et à la sécurité économique. Un autre élément essentiel se rapporte à l'influence. Dans les années 2000, il est apparu possible d'influencer une population donnée pour créer un environnement favorable ou défavorable. Attaquer l'image d'une entreprise peut s'avérer extrêmement négatif pour cette dernière. L'exemple de la campagne de déstabilisation à l'encontre de Total en Birmanie constitue un exemple pertinent.

Des acteurs sont spécialisés dans l'influence, et ce, afin de détruire ou déstabiliser des entreprises. La surveillance des réseaux sociaux en permanence devient alors une nécessité.

Conclusion

Les principes de l'IE ont toujours existé. Il est possible de les retrouver chez Sun Tzu. La puissance de Venise sur la méditerranée au Moyen-Âge provient de la pratique de l'IE. Enfin, les Japonais et les Russes ont développé leur économie après la Guerre grâce à l'IE. L'IE représente un réel potentiel pour les entreprises et les États.

Débat

Int : L'idée de se regarder soi-même est intéressante. Un DSI pourrait éventuellement avoir un côté réflexif.
AJ : En effet. Votre métier évolue en lien avec le numérique. Votre domaine devient le cœur d'une entreprise. Par ailleurs, de nombreux acteurs souhaitent uniquement obtenir des résultats et de l'efficacité. A titre d'illustration, Saint-Gobain avait toujours considéré qu'il ne représentait pas une cible. L'attaque subie par cette société a notamment conduit à un blocage du Siège pendant deux semaines et à la fermeture de trois usines. Le problème est que les dirigeants d'entreprises n'ont pas été formés à ces problématiques. Dans le passé les entreprises travaillaient avec des plans à cinq ou trois ans. Cet horizon s'est réduit, ce qui empêche une vision de long terme et au final s'avère dangereux.

Int : Il n'est pas évident d'amener le management à ouvrir les yeux. Sur quel type de ressource les DSI pourraient-ils s'appuyer afin de faire passer des messages auprès du Comex ou du Conseil d'administration ?
AJ : L'ANSSI est un acteur intéressant qui délivre des messages. Ces informations sont françaises, vraies et suffisamment précises pour interpeller. Pour convaincre, il faut utiliser des informations sûres, ce qui suppose de les chercher. Ensuite, il importe d'éclairer les décideurs. Dans les grandes entreprises, la peur apparaît lorsqu'un concurrent ou un partenaire s'est fait piéger en matière de sécurité. Il apparaît indispensable de fournir des informations ciblées qui renvoient à des exemples concrets.

Int : Le fait d'être confronté à une attaque suppose de faire preuve d'humilité. Pour autant, il s'agit d'un moyen d'obtenir une écoute de la part de la Direction et des ressources supplémentaires. Dans le domaine de l'automobile, le management n'est pas réceptif aux messages ayant trait à la sécurité informatique.
AJ : J'ai évoqué cette question de l'IE auprès de l'ancien Président de PSA. Ce dernier ignorait qu'une telle entreprise pouvait se faire pirater. Les dirigeants n'écoutent pas les experts, mais leurs pairs.
Int : Nous pouvons sensibiliser les dirigeants à partir des outils qu'ils comprennent.
AJ : Le numérique est un outil à double face. Les jeunes générations commencent à être formées en la matière.
Int : Que pouvons-nous dire à propos de la maturité des pays sur ces sujets ? Des *benchmarks* sont-ils effectués en termes de maturité concernant la thématique de l'IE ?
AJ : Des *benchmarks* sont effectivement réalisés. En matière d'agressivité, il convient de retenir que les Etats-Unis, par l'intermédiaire de la CIA et de la NSA sont mobilisés pour aider leurs entreprises. Il importe ensuite

de mentionner la Chine dont les systèmes sont moins sophistiqués. Pour autant, elle apprend rapidement et espionne beaucoup. Les Chinois estiment ne pas avoir à se justifier dans la mesure où l'espionnage ne leur pose pas de problème moral. Enfin, les Israéliens correspondent à un autre acteur très agressif.

La Russie est un acteur agressif, mais différent. Elle dispose d'équipes de hackers qui sont majoritairement en dehors des organismes d'État. Ce sont des groupes criminels privés qui réalisent des actions pour le compte de l'État russe, mais également pour eux-mêmes.

Int : Des sociétés œuvrent afin d'aller chercher l'empreinte numérique d'autres entreprise. Disposer d'information à propos de cette empreinte est important et participe à ce travail de connaissance de soi évoqué précédemment. Les dirigeants d'entreprises doivent-ils être sensibilisés à propos de cette thématique ?
AJ : L'ANSSI vient de publier un guide sur la sécurité informatique des PME, très adapté à ces acteurs. S'agissant de l'empreinte numérique, la plupart des entreprises n'ont pas la capacité de réaliser ce type d'étude. Il est souhaitable de solliciter des sociétés extérieures. Toutefois, peu d'entreprises spécialisées peuvent mener ce travail. En outre, il est indispensable de bien choisir la société qui réalise l'enquête dans la mesure où elle disposera d'informations qu'elle pourrait mal utiliser. Sur le plan contractuel, il convient de vérifier que toutes les informations communiquées seront effectivement restituées à l'issue de la mission. L'empreinte numérique n'en demeure pas moins un excellent moyen de vérifier les failles.

Int : J'ai constaté que les spécialistes de l'IE n'abordaient pas ces questions de sécurité il y a une dizaine d'années dans le cadre des formations en IE.
AJ : En effet, les rares écoles qui formaient les spécialistes en IE ne s'intéressaient pas à la sécurité. La situation a évolué.
Int : C'est rassurant.

Int : Aujourd'hui, il s'avère encore délicat de convaincre la hiérarchie à propos de ces problématiques de sécurité.
AJ : Avec les nouveaux moyens techniques, nous pouvons bloquer une très grande quantité d'attaques. L'utilisation des outils nomades implique de sécuriser chaque poste, et non plus le réseau. En face les hackers qui travaillent sur des gros réseaux se retrouvent sur des systèmes décentralisés, ce qui leur pose un problème. Leur modèle de fonctionnement est confronté à des difficultés. De toutes manières il convient d'apprendre à vivre avec des outils qui ne sont pas complètement fiables.

Int : Que pensez-vous de la maturité des politiques sur ces sujets ?
AJ : Le politique n'a pas conscience des outils qu'il utilise. A titre d'illustration, Nicolas Sarkozy utilisait un portable banal non crypté lorsqu'il était Président de la République. L'ambassade américaine, située à 200 mètres de l'Élysée, était en mesure d'écouter toutes ses conversations. Certains politiques sont sensibles à cette problématique, mais ils représentent une infime minorité.

Présentation des orateurs

Alain JUILLET est Président de l'Académie d'Intelligence Économique après une expérience incluant le renseignement (DGSE), la direction et le redressement d'entreprises (Suchard...), l'administration de l'État (responsabilité de l'Intelligence Économique auprès du Premier Ministre...)…