

LE BULLETIN *d'information sur* *l'intelligence économique stratégique pour les PME-PMI*

ÉDITO

La sécurisation des locaux

Au cœur de ses différentes stratégies d'intelligence économique se pose la question de la sécurité. La précédente newsletter abordait le thème de la sécurité informatique. Il n'est pas le seul.

L'information circule essentiellement au sein de l'entreprise, plus particulièrement dans ses locaux et c'est la sécurisation de ces derniers que nous allons aborder aujourd'hui.

Identifier les menaces

Dès que l'on parle de sécurisation de locaux, on pense immédiatement système d'alarme, vidéosurveillance ou surveillance humaine. Mais ces outils ne sont que la conséquence d'une réflexion plus large, qui doit toujours être engagée. Quelles sont les valeurs à protéger au sein de l'entreprise ? Quelles sont les menaces auxquelles nous allons avoir à faire face, pour chacune de ces cibles ? La menace doit être étudiée selon ses trois angles caractéristiques : l'objectif qu'elle vise, l'agresseur qui va agir et ses méthodes et moyens d'action.

Les schémas d'infiltration, faiblesses de l'entreprise

Un audit préalable de sûreté apporte une vision globale sur la sécurisation des locaux d'une entreprise. Il porte sur plusieurs points : les forces et les faiblesses de l'entreprise, l'analyse de ses flux

(humains, matières et produits, informations, financiers, fluides et énergies) et la détermination des valeurs, qui sont les cibles d'éventuels agresseurs. La bonne connaissance de l'entreprise, acquise par l'auditeur et son expérience dans le domaine, permettent d'identifier les schémas d'infiltration. Ces derniers sont d'autant plus dangereux que la motivation des attaquants est grande, la facilité d'accès établie et l'impunité ressentie.

Trouver la bonne méthode de sécurisation

La sécurisation des locaux se fait par cercles concentriques des abords des bâtiments, aux limites du bâtiment vers l'intérieur des locaux. Plusieurs outils sont disponibles. Les protections mécaniques servent à dissuader, retarder et parfois empêcher les intrusions. Ces protections (clôtures, murs, portes, fenêtres, serrures) font l'objet de normalisation, ainsi que les sociétés qui les fabriquent et les installent. Ces sociétés, reconnues, sont à sélectionner en priorité.

Alarmes : des outils, des principes

Sont ensuite pris en considération les moyens d'alarme électroniques, (détecteurs de mouvements, d'ouverture, de bris de vitres, barrières hyper fréquences, etc...), ainsi que les systèmes de vidéo surveillance, essentiels quant à la dissuasion et la détection des intrusions.

Un grand principe à respecter est de veiller à ce que la durée de la résistance mécanique des bâtiments



soit supérieure à l'addition des temps de détection, de transmission d'alarme et d'intervention. De même, dans les bâtiments d'une certaine importance (en général plus de 800 m²), il est important d'adopter le principe de deux moyens de détection pour chaque scénario d'infiltration identifié. Une installation

d'alarme ne se conçoit pas sans l'appui d'une société de télésurveillance, qui assurera les interventions éventuelles.

Sociétés prestataires : privilégiez la certification

L'adoption d'une solution de prestations humaines permanentes ou temporaires se fait sur la base de l'importance des valeurs à protéger et des capacités financières de l'entreprise, ces solutions étant très efficaces, mais d'un coût élevé

Comme pour les protections mécaniques, le monde de l'assurance a mis en place des certifications et des règles dans les domaines de l'alarme intrusion et de la vidéo surveillance. Les sociétés référencées dans ces domaines sont à préférer à celles qui n'ont pas fourni l'effort de s'y conformer, ceci étant un gage de sérieux et de qualité.

Enfin, et ce n'est pas le plus coûteux, une bonne organisation et des procédures efficaces sont essentielles pour assurer une bonne politique de sûreté. Il ne faut pas oublier que cette politique, qui doit être engagée et soutenue par la direction de l'entreprise, n'est pas uniquement du ressort du chargé de sécurité et de son service, mais de l'ensemble du personnel qui doit être conscient et informé de la nécessité d'une telle politique et y adhérer.

M. Jean Lucat, ACONIT

POINT CLÉ

Le premier rempart contre les sinistres : la protection des locaux.

Lorsque l'on évoque les risques de vol d'information ou d'atteinte au patrimoine informationnel de l'entreprise, on imagine volontiers des attaques sophistiquées contre le système d'information, des pénétrations de firewall, la mise en place de chevaux de Troie voire l'interception de communications. Ces menaces existent et doivent être combattues mais il convient de ne pas oublier qu'il est en général plus facile d'entrer dans une entreprise par la porte que par la connexion Internet.

L'entreprise reçoit de nombreux visiteurs : clients, prospects, fournisseurs, sous-traitants, prestataires, etc, qui ne devront pas être mis au contact de l'information sensible sans avoir le « besoin d'en connaître ». Pour un visiteur expert, il suffit parfois d'un coup d'œil à un document ou à un dessin pour deviner la stratégie de l'entreprise, déceler une innovation, repérer un problème. La première règle de protection sera d'organiser les locaux de l'entreprise de telle façon que les visiteurs restent cantonnés en des lieux qui ne contiennent pas d'information sensible. Une salle de réunion excentrée par rapport à l'activité remplira ce rôle à condition de prendre le soin de la laisser vide de tous documents et d'effacer les tableaux.

Prévoyez un « circuit de notoriété » qui permettra de faire visiter votre entreprise, d'en donner une image concrète et valorisante tout en évitant les locaux sensibles.

Il arrive aussi que des visiteurs indésirables s'invitent aux heures de fermeture, le plus souvent à la recherche de matériel directement monnayable mais parfois à la recherche d'informations.

Vous aurez mis vos informations sensibles à l'abri : bureaux nets, documents rangés dans des armoires fermant à clé, voire dans des coffres. Votre informatique centrale aura été placée dans une salle spécifique à accès très restreint et à contrôle renforcé. Vos données informatiques auront été sauvegardées sur des supports dont un exemplaire aura été placé à l'extérieur.

Il ne reste plus qu'à placer des obstacles successifs sur la route de l'intrus. C'est ce que l'on appelle la défense en profondeur : grillages, barreaux aux fenêtres, portes blindées, accès par code ou badge, seront autant de freinages qui ralentiront l'intrus et donneront le temps aux services de sécurité d'intervenir. Il va de soi que des détecteurs appropriés auront déclenché l'alarme dès le premier franchissement des limites.

On n'oubliera pas de compléter tout ceci par une alarme incendie éventuellement couplée à un dispositif d'extinction automatique ni de mettre en avant ces investissements lorsqu'il s'agira de négocier la prime d'assurance.

Michel LE PIMPEC

Secrétaire du GITSIS (Groupement Interprofessionnel pour le Traitement de Sécurité des Informations Sensibles)

L'intelligence économique : une démarche au service de son développement

Retour sur les enjeux de l'intelligence économique avec Brice De Gliame, Président de la Société ITB (Intelligence and Technology for Business), spécialisée dans l'intelligence collaborative et l'accompagnement des cadres et dirigeants d'entreprises, à l'élaboration et à la conduite de leur stratégie.

L'intelligence économique passe aussi par la sécurisation des locaux. En quoi un dirigeant de PME est-il aussi concerné ?

Brice De Gliame : Sous pression, un dirigeant d'entreprise n'a pas toujours le temps ou le recul nécessaire pour s'intéresser à la sécurisation des locaux. Pourtant, c'est un des moyens pour préserver son activité.

Un exemple ? En cas d'incendie ou de pertes de données, le dirigeant a-t-il prévu un stockage de secours de ses archives et un lieu de protection de ses informations importantes ? Ce type de question simple renvoie à l'organisation de la protection et la sécurité de l'information au sein de son l'entreprise, donc à un aspect « défensif » de la stratégie définie par le dirigeant. Il s'agit là non pas d'actions isolées à réaliser, mais bien d'une démarche globale à mettre en œuvre.

Cette démarche peut-elle apporter des avantages concrets pour l'activité d'une entreprise ?

Brice De Gliame : Cette démarche est un moyen pour renforcer et développer son activité, en fonction d'objectifs clairement définis. Souvent l'intelligence économique est associée à une logique limitée à la protection hors s'il est indispensable de s'assurer de la sécurisation de ses locaux, ces actions défensives demeurent totalement insuffisantes pour assurer la croissance de son activité.

L'intelligence économique apporte des méthodes et des outils nouveaux au service du développement de l'entreprise et de sa compétitivité : c'est donc aussi une démarche offensive au service de l'entreprise.

Une PME qui met en place en interne de bonnes pratiques de recueil et d'analyse de l'information collectée par ses collaborateurs et un dispositif de veille stratégique et compétitive fondé sur la surveillance d'un bouquet pertinent de sources (documentaire, presse, web) disposera d'atouts supplémentaires pour conquérir de nouveaux marchés.

De nombreuses PME travaillent aujourd'hui avec des grands groupes ou des donneurs d'ordre – comme l'Etat – qui sont sensibles à la capacité de leurs fournisseurs à se doter des bons outils de veille et d'analyse dans un climat concurrentiel croissant. Il faut ensuite savoir « vendre » auprès de ses clients cette démarche engagée, expliquer sa stratégie et ses objectifs fixés. Ce sont de réels arguments différenciant qui valorisent l'entreprise auprès de ses partenaires extérieurs.

L'intelligence économique
est aussi une démarche
offensive au service de
l'entreprise... qui pourra ainsi
rassurer ses partenaires
extérieurs...

Comment un dirigeant de PME peut-il s'engager dans une telle démarche « offensive » ?

Brice De Gliame : Il doit d'abord avoir une vision claire de ce qu'il cherche à atteindre ou à obtenir et ensuite le dirigeant pourra s'appuyer sur des méthodes simples et efficaces.

Dans un premier temps, il s'agira d'utiliser les 4 phases de la méthode du cycle du renseignement :

- élaborer un plan de recherche des informations lui paraissant utiles,
- identifier les sources légales auprès desquelles il pourra collecter ces informations,
- analyser puis synthétiser les informations collectées,
- et enfin planifier ces informations à des fins de décisions et de planification des actions.

Après cette étape d'acquisition de la connaissance et d'aide à la décision, le dirigeant et ses collaborateurs pourront utiliser une seconde méthode pour anticiper et planifier leurs actions :

- définir (ou re-définir au regard des informations précédemment collectées) leur (s) objectif (s) à atteindre,
- renforcer leurs centres de gravités (les zones de vulnérabilités)
- déterminer le chemin à suivre pour atteindre leur (s) objectif (s) tout en évitant les principaux écueils,
- planifier les actions en fonction des capacités et des ressources disponibles.

Cette approche est un moyen de se poser les bonnes questions et de cibler les points essentiels en vue d'une mise en œuvre rapide de la stratégie de l'entreprise.

L'intelligence économique contribuerait donc aussi à concevoir et à conduire la stratégie de sa PME ?

Brice De Gliame : Oui, cela va permettre au dirigeant de « construire » l'information stratégique et compétitive dont il a besoin pour décider et qui n'existe nulle part sous une forme formalisée.

Avec l'aide d'outils et de méthodes efficaces, le dirigeant et ses collaborateurs pourront ainsi concevoir de manière collective et partagée, la stratégie gagnante de l'entreprise, c'est-à-dire les objectifs à réaliser, la planification opérationnelle et la conduite des actions nécessaires pour atteindre les objectifs.

C'est aussi dans l'optique d'aider les PME à s'approprier ces méthodes, que nous mettons gratuitement à la disposition des entreprises des outils méthodologiques (mémento sur le cycle du renseignement, la planification opérationnelle) conçus en coopération avec une pluralité d'acteurs publics et privés, civils et militaires avec notamment la sortie prochaine d'un nouveau mémento consacré à la protection et à la sécurité de l'information.

ITB

171, avenue Victor Hugo 75116 PARIS

Tél. 01 45 04 95 16

www.itb.fr

FOCUS SUR

Pour la sécurité des entreprises artisanales : mobilisation générale et actions concrètes !

La lutte contre toutes les formes de violence, et notamment celles qui frappent le monde économique, constitue une priorité pour l'action des services de l'Etat dans les Hauts-de-Seine.

A ce titre, la Chambre de Métiers et de l'Artisanat des Hauts-de-Seine a organisé le mardi 8 avril dernier dans ses locaux une réunion-débat ayant pour thème la sécurité des entreprises artisanales. Cette réunion a mobilisé un grand nombre de participants : chefs d'entreprise et collectivités.

Lors de cette réunion, le protocole associant les services de la Préfecture, la Direction Départementale de la Sécurité Publique des Hauts-de-Seine et de la CMA92 a été signé. Ce protocole tripartite mentionne les axes d'intervention développés pour favoriser la sécurité des entreprises artisanales dans notre Département :

- Des rencontres régulières au cours desquelles seront évoqués tous les thèmes intéressant les entreprises artisanales : phénomènes délinquants (vols d'outillage, de métaux, vols avec violences...), infractions impliquant certains secteurs artisanaux (travail dissimulé, emploi d'étrangers en situation régulière...), sécurité routière (campagnes d'éclairage, informations pratiques et préventives concernant les

comportements dangereux dans la conduite des véhicules professionnels...)

- Des correspondants désignés : la Direction départementale de la Sécurité Publique et la CMA92 ont nommé des correspondants dans chaque institution afin de centraliser les demandes ou informations. Pour la CMA92, Jean Auboiroux, vice-président de la CMA92 est le correspondant désigné.
- Des actions de sensibilisation à la sécurité (protection des personnes et des biens), à la vidéoprotection, à la sécurité routière (catégories d'infraction, conduite à tenir lors d'une agression...) sont prévues.
- Des actions d'information par le biais du journal de la CMA92 « Atouts92 » et d'une plaquette de prévention réalisée par la CMA92 en collaboration avec les services de Police sera diffusée courant septembre. Les thèmes : comment se protéger ? Comment protéger ses biens ? Comment réagir en cas d'agression ? Comment déposer plainte ou comment ne pas être victime du travail illégal ? ... seront développés dans un but de prévention et de sensibilisation.

« Il n'y a pas de liberté d'entreprendre sans le respect de la loi et des règlements. La mobilisation de chacun d'entre nous est déterminante pour faire reculer la délinquance. La mobilisation de chacune des communes des Hauts-de-Seine est une nécessité pour combattre toutes les formes de violences et sécuriser nos professions ! Aidez-nous à le faire savoir... Ce combat est aussi le vôtre. »
Daniel Goupilat, Président de la CMA92.

CONTACT

Chambre de Métiers et de l'Artisanat
des Hauts-de-Seine

Elisabeth Auffray, Responsable de la Communication
Tél. : 01 47 29 43 93 - eauffray@cma-nanterre.fr

ACONIT

Contact : Jean LUCAT

Mail : jean.lucat@aconit.eu

115, rue Saint-Dominique - 75007 Paris

Site Internet : <http://www.aconit.eu>

La Confédération Générale des Petites et Moyennes Entreprises Ile-de-France (CGPME IDF).

Contact : Cyril Pattegay - Chargé de mission

Mail : c.pattegay@cgpme-idf.fr

10, Terrasse Bellini - 92806 Puteaux Cedex

Site Internet : <http://www.cgpme-idf.fr/>

Chambre des Métiers et de l'Artisanat des Hauts-de-Seine

Contact : Gérard DANSAC - Vice Président

Mail : mlognon@cma-nanterre.fr

17 bis, rue des Venêts - BP 1410

92014 Nanterre Cedex

Site Internet : <http://www.cma92.fr>

EN SAVOIR PLUS

GITSIS

**(Groupement Interprofessionnel pour le Traitement
de Sécurité des Informations Sensibles)**

Contact : Michel LE PIMPEC

GITSIS - c/o Intertechnique - BP1

78373 Plaisir Cedex

Mail : mlepimpec@intertechnique.zodiac.com

Site Internet : <http://www.gitsis.asso.fr>

ITB

Contact : Brice de Gliame - Président

Mail : bdg@itb.fr

171, avenue Victor Hugo - 75116 Paris

Site Internet : <http://www.itb.fr>

CONTACT

I.E.S Le Bulletin est édité en complément du Guide "Le dirigeant de PME-PMI & l'intelligence économique", projet régional en partenariat avec Agefos PME Ile-de-France, le Conseil Régional d'Ile-de-France et la CGPME Ile-de-France. Tél. : 01 47 78 78 35 - Mail : contact@cgpme-idf.fr

Secrétaire Général de la CGPME Ile-de-France : Abdellah MEZZIOUANE

Ont participé à ce numéro : Brice De Gliame, président ITB - Jean Lucat, Aconit - Michel Le Pimpec, secrétaire du GITSIS - Karine LAYMOND, chargée de communication à la CGPME Ile-de-France - Conception, réalisation : CHALLENGE'R - 43, rue Raspail 92300 Levallois