



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DÉLÉGATION
INTERMINISTÉRIELLE
À L'INTELLIGENCE
ÉCONOMIQUE

SECO

LA LETTRE DE LA SÉCURITÉ ÉCONOMIQUE

N°1 - juillet 2012

L'éditorial

Olivier BUQUEN,
Préfet, Délégué Interministériel à l'Intelligence Economique

Les entreprises et les établissements de recherche français exercent leur activité dans le cadre d'une économie mondialisée, ouverte, dont l'intensité concurrentielle ne cesse de progresser. Cette ouverture et cette concurrence sont porteuses de croissance et offrent de nouvelles opportunités de développement aux entreprises françaises. Pour autant, elles engendrent un certain nombre de risques pour les entreprises, les établissements de recherche et globalement pour l'économie française. Il est donc primordial d'identifier et de prévenir ces menaces qui peuvent cibler de multiples domaines :

- la captation de l'innovation, de la R&D ou d'autres actifs stratégiques, via des intrusions dans les locaux ou les systèmes informatiques;
- l'atteinte à l'image et la réputation : celles-ci peuvent notamment être entachées par des campagnes de désinformation ou des tentatives de déstabilisation ;
- les attaques sur le capital des entreprises, cible de prises de participation, voire de prises de contrôle par certains investisseurs non souhaités ou masqués, aux intentions prédatrices, profitant de faiblesses des entreprises en période de crise.

Dans chacun de ces domaines, l'Etat contribue à limiter la vulnérabilité des entreprises et des établissements de recherche. Un des axes forts de cette politique publique de sécurité économique repose sur la sensibilisation de tous les acteurs, pour que de simples mesures de précaution élémentaires soient adoptées, rendant plus difficiles et donc plus dissuasives les tentatives indues d'acquisition d'information.

L'important est de trouver un équilibre entre une naïveté excessive, qui laisserait nos entreprises trop vulnérables,



Olivier BUQUEN

© Credit: MINISTÈRE PRÉFET

et une paranoïa stérile incompatible avec une économie ouverte. Cet équilibre s'appelle la vigilance.

La Lettre de la Sécurité économique de la D2IE contribue à cette vigilance. Diffusée tous les deux mois, elle s'appuiera sur des témoignages et sur des exemples de faits réels récents. Vous retrouverez également, sur une thématique donnée, quelques conseils simples à mettre en œuvre pour rendre l'action des agresseurs plus difficile. Enfin, elle présentera succinctement l'action de la D2IE dans les autres volets de la politique publique d'Intelligence économique que sont la veille et le soutien à la compétitivité de nos entreprises et de nos établissements de recherche.

Nous comptons sur vous pour la diffuser largement !

Et dans votre entreprise ?

Pierre MOUSTIAL,
Directeur Général des Laboratoires URGO, témoigne.

D2IE : Votre entreprise a demandé à la Direction Centrale du Renseignement Intérieur (DCRI) de réaliser un audit de sécurité de son établissement principal. Pourquoi une telle démarche ?

Pierre MOUSTIAL : Chez les Laboratoires URGO, nous menons une démarche permanente d'amélioration



Pierre MOUSTIAL

continue et nous ne croyons qu'à l'efficacité validée de façon indépendante, que ce soit dans le développement de nos produits ou pour nos procédures de protection de nos acquis scientifiques. J'ajouterais que, pour entraîner les collaborateurs d'une entreprise, dans une démarche de sécurité économique, il faut des faits tangibles remontés de façon

incontestable par des experts de la sécurité comme ceux de la DCRI.

(suite de l'interview en page 4)

Délégation Interministérielle à l'Intelligence Economique

ATRIUM—5 place des Vins-de-France—75573 Paris CEDEX 12

☎ 01.53.44.26.22

Vous souhaitez recevoir les prochains numéros de SECO ? Abonnez-vous en nous envoyant un e-mail avec ABONNEMENT en objet à : contact@ie.gouv.fr

(Vous souhaitez vous désabonner ? Envoyez DESABONNEMENT en objet)

Toute ressemblance avec un fait réel ...

A chaque numéro, la D2IE présente des cas récents d'ingérence économique, afin de vous aider à anticiper et à vous protéger. Récits d'événements réellement survenus au cours des derniers mois, les cas présentés constituent une illustration de la diversité des atteintes susceptibles de viser les entreprises françaises.

Une entreprise déjoue les manœuvres intrusives d'une délégation étrangère

Spécialisée dans une nouvelle technique très innovante, une entreprise en pleine expansion, et bénéficiant notamment de l'évolution d'une nouvelle réglementation adoptée par un pays étranger, cherche depuis quelques années à se développer à l'international en tissant des partenariats. Elle a lancé le projet d'une joint-venture avec une entreprise étrangère, dont les dirigeants ont été invités en France afin de faire avancer les négociations. Lors de la visite, les représentants de ce pays ont demandé à accéder à l'un des ordinateurs de l'entreprise, en prétendant ne pas disposer du matériel informatique nécessaire pour présenter leur structure. Les ordinateurs se trouvant dans les locaux dédiés à la recherche et développement, les dirigeants français ont alors proposé un ordinateur portable vierge de tout document interne, qu'ils avaient justement prévu d'utiliser en cas de demande de leurs hôtes. Les émissaires étrangers ont alors décliné l'offre et ont effectué leur présentation sur leur propre ordinateur, qu'ils venaient soudainement de retrouver...

Commentaire : délégations étrangères, « bienvenue » mais vigilance de tous les instants.

La délégation étrangère manifestait visiblement un intérêt très marqué pour l'entreprise française. Dès lors, la tentative de connexion à un ordinateur de la salle de R&D peut apparaître suspecte. Il est évidemment indispensable pour une entreprise de recevoir régulièrement des visiteurs. Mais il convient d'organiser ces visites. La peur de déplaire à d'éventuels clients, fournisseurs, partenaires ou actionnaires ne doit pas conduire à l'oubli des règles minimales de sécurité et de confidentialité. Dans le cas présent, on peut se féliciter de l'attitude des dirigeants qui ont su préserver leur intérêt malgré l'insistance et le subterfuge de la délégation. L'entreprise française n'a pas donné de suite favorable à ce projet de collaboration.

Les employés d'une entreprise rappellent à l'ordre un visiteur ayant tendance à se perdre...

Une grande entreprise française accueille fréquemment, en son siège, des partenaires pour des réunions de travail. Sur un des projets en développement, un visiteur, à la fin de la réunion, n'a pas rejoint directement la sortie et a été surpris, par une employée, en train d'errer dans les couloirs. Cette dernière l'a alors pris en charge et lui a proposé de le raccompagner à la salle de réunion ou auprès du contact au sein de l'entreprise qui était affiché sur son badge. Quelques semaines plus tard, à l'occasion d'une autre réunion, le même individu est de nouveau aperçu dans un espace où il n'avait pas à se trouver. Il est également intercepté par un employé qui adopte la même position et lui propose la même alternative de raccompagnement. Lors de sa troisième venue, il est accueilli, non seulement par l'hôtesse qui lui délivre son badge habituel, mais également par le responsable de la sécurité du site qui lui fait remarquer les deux précédents égarements et lui conseille aimablement mais fermement de ne pas se perdre une nouvelle fois, sous peine d'être raccompagné définitivement à la porte de l'entreprise...

Commentaire : la sécurité économique de l'entreprise, c'est l'affaire de tous.

Les égarements répétés du futur partenaire, en visite dans les locaux de l'entreprise, suscite une interrogation sur ses motivations réelles. Si elles n'ont pu être établies, le comportement adopté ne semble pas des plus innocents.

Les éventuelles difficultés liées à cette *intrusion consentie* ont pu être évitées grâce à la politique de sûreté / sécurité mise en place par l'entreprise et au comportement exemplaire des salariés.

Différents enseignements peuvent être tirés de ce cas :

- * l'entreprise a mis en place un système efficace de badge pour les visiteurs avec le nom de la personne visitée et le numéro de la salle de réunion, ce qui permet aux employés de guider lesdits visiteurs,
- * l'ensemble du personnel de l'établissement a été sensibilisé à la détection des comportements inadaptés,
- * enfin, la mise en place de rapport d'étonnement a porté ses fruits puisque le responsable de la sécurité du site a été alerté des faits précédents et a pu intervenir de façon adaptée en appui de l'hôtesse d'accueil.

A chaque numéro, la D2IE vous propose une fiche synthétique. Elle présente succinctement les risques potentiels sur un sujet précis et suggère des mesures de prévention et des parades simples à mettre en place.

Fiche n°1 : Encadrer les visiteurs et les délégations

Les risques

La plupart des vols de données sensibles sont commis sans effraction par des personnes qui ont eu libre accès au site. On parle alors « d'intrusion consentie ». Des stratagèmes visant à tromper l'attention des personnels d'accueil peuvent être élaborés.

Si les visites sont d'abord des opportunités, elles peuvent parfois masquer des intentions malveillantes. Aussi, la volonté de montrer son savoir-faire et ses compétences ne doit pas conduire à dévoiler des informations confidentielles.

Les parades

- * Contrôler les accès par des moyens adaptés à la zone protégée : personnel d'accueil, registre de visite, badges, interphone, digicode, vidéo protection
- * Limiter les accès à contrôler (accès fournisseurs, visiteurs, personnel), en assurer le filtrage et verrouiller les autres accès.
- * Définir les zones ou pièces sensibles et fermer les accès lorsqu'elles sont inoccupées
- * Définir une zone d'attente pour faire patienter les visiteurs
- * Prévoir une procédure d'accueil des visiteurs
- * Faire porter un badge bien identifié et spécifique aux visiteurs
- * Recevoir les visiteurs dans une salle de réunion neutre
- * Accompagner les visiteurs constamment
- * Définir un circuit de visite préservant la confidentialité de certaines zones sensibles
- * Ne pas permettre l'accès au réseau de l'entreprise (attention aux faux prétextes : consultations d'e-mails, lecture ou impression d'un document sur clé USB, etc.)
- * Pour une visite de nouveaux partenaires, notamment étrangers, vérifier les motivations et le profil des visiteurs. Organiser la visite en conséquence.
- * Ne pas hésiter pas à refuser de répondre à une question indiscrète, hors sujet ou hors de votre compétence



Sensibiliser les personnels au respect des consignes (port du badge, etc.) et à la vigilance

A votre service...

***Vous avez des questions sur la sécurité économique.
Vous faites face à une situation atypique et vous ne savez pas avec qui l'évoquer.
Vous souhaitez signaler un fait, une atteinte que vous avez subie.***

***Sans entrer dans le détail, laissez-nous vos coordonnées.
Vous serez rapidement recontactés par le service de l'Etat compétent.***



securite-economique@interieur.gouv.fr

Vous avez mis en place des bonnes pratiques en matière de sécurité ? Vous avez fait face avec succès à une menace ou à une agression économique ? Si vous souhaitez partager votre expérience, cette rubrique est la vôtre.

Ecrivez-nous à contact@ie.gouv.fr

(suite de l'interview de la page 1)

D2IE : Que vous a apporté l'audit de la DCRI ?

Pierre MOUSTIAL : En l'absence de procédures claires et d'instructions précises, les données stratégiques de l'entreprise sont facilement accessibles à des tiers malintentionnés. Le point essentiel de faiblesse est l'absence de conscience des risques de la part des salariés de l'entreprise. Les auditeurs de la DCRI nous ont transmis un état des lieux précis de nos points forts et de nos vulnérabilités, accompagné d'un ensemble de recommandations concrètes pour nous améliorer. Cette aide fut donc très précieuse pour embrayer sur des mesures opérationnelles de protection.

D2IE : Pensez-vous que ces efforts réalisés constituent un investissement pour l'avenir de l'entreprise ?

Pierre MOUSTIAL : Une démarche d'intelligence économique et de protection des informations pour une entreprise comme la nôtre, c'est comme une assurance : c'est l'assurance de ne pas voir les investissements lourds consacrés à la recherche et au développement, vecteurs de notre croissance et de notre prospérité future, gâchés de façon brutale car nous n'aurions pas su préserver nos innovations .



L'actualité de la D2IE

Publication d'un Guide de l'intelligence économique pour la recherche

Le 14 mars 2012, la D2IE lançait au Ministère de l'Enseignement Supérieur et de la Recherche, **le guide de l'intelligence économique pour la recherche**. Dans un contexte où l'innovation est le moteur de la croissance, les établissements de recherche, sont en effet des acteurs majeurs du paysage économique français. Le patrimoine scientifique de la recherche est donc un bien commun qu'il s'agit de protéger et de valoriser le plus efficacement possible, pour qu'il profite en priorité au développement du tissu industriel national ou communautaire. A travers cinq thématiques (veille stratégique, gestion du patrimoine immatériel, politique de sécurité des systèmes d'information, développement de l'interface entre la recherche et le monde socio-économique, politique internationale), ce guide énonce des préconisations concrètes et permet de mettre en lumière les problématiques que les établissements de recherche seront le plus souvent amenés à gérer.

Signatures de conventions de partenariat avec des acteurs majeurs de l'IE

Matière transversale par essence, l'intelligence économique, telle qu'elle est promue par la D2IE, nécessite l'action commune des différents partenaires participant aux trois piliers de celle-ci : veille stratégique, soutien à la compétitivité, sécurité économique.

A cet effet, la D2IE a conclu des conventions de partenariats avec des institutions importantes, relais stratégiques de l'intelligence économique. Ainsi, le 20 mars 2012, la D2IE, **l'Institut National de la Propriété Industrielle (INPI)** et **l'Agence Française de Normalisation (AFNOR)**, conscients que la normalisation et la propriété industrielle constituent deux axes stratégiques de la politique publique d'intelligence économique, ont signé trois conventions de partenariat bilatérales.

Les rôles d'accompagnement des avocats dans le développement des entreprises et de sensibilisation des ces dernières à la protection de leur patrimoine matériel ou immatériel, informationnel ou technologique, ont également conduit la D2IE, le **Conseil National des Barreaux (CNB)** et le **Barreau de Paris** à signer deux autres conventions de partenariat le 18 avril 2012. Le 4 juin 2012, a été signée une convention de partenariat entre la D2IE et le **Conseil Supérieur de l'Ordre des Experts-Comptables (CSOEC)**, le réseau des professionnels de l'expertise comptable, acteur clef de l'économie régionale et de l'accompagnement au développement des entreprises. Enfin, le 21 juin 2012, la D2IE a conclu un partenariat avec le **Syndicat Français de l'Intelligence Economique (SYNFIE)** pour renforcer leur coopération au service des entreprises.