>L'INTELLIGENCE ÉCONOMIQUE : METTRE EN ŒUVRE DE BONNES PRATIQUES, PROTÉGER SES RICHESSES

La DCRI, Direction Central du Renseignement Intérieure, a organisé une conférence sur le thème "l'intelligence économique" le jeudi 21 mars 2013 afin de sensibiliser les organisations professionnelles et, à travers elles, leurs adhérents sur des risques méconnus. La Fédération de la Plasturgie n'a pas manqué d'y participer et se doit d'être le relais de l'information

Les richesses de nos entreprises sont multiples : des matières innovantes, des procédés techniques efficients, une réputation, des processus de financement performants sont quelques exemples. Elles se traduisent bien souvent sous la forme d'informations qui relèvent du domaine public ou du périmètre stratégique dont la divulgation est directement préjudiciable à l'entreprise.

Vos concurrents, des administrations de certains pays et de plus en plus souvent des officines privées scrutent l'abondant flux d'informations rendues publiques volontairement ou non : publication, communiqué de presse, dépôt de brevets, entretien commercial, demande de certification.

Ils pratiquent l'intelligence économique, activité légale, afin d'y trouver de l'information stratégique ou vous cibler pour des actions illicites, l'espionnage, le vol, le chantage. Les exemples de transferts d'informations stratégiques dans le domaine public n'ont pas manqué lors de cette conférence :

• Photos de matériels sensibles de l'aérospatiale sur la page Facebook d'un collaborateur.
• Maquette fidèle d'un prototype sur un salon professionnel.
• Trame de TGV transformée en salle de réunion par des commerciaux.
• Conception d'une stratégie de rachat d'un groupe pétrolier dans un bar.

Mais également, des vidéos, des témoignages et des démonstrations d'activités illicites : vol de portable (plus de 800 sur les lignes TGV à destination de nos principaux complexes industriels), piratage de téléphone réalisable en mois de 5 minutes, chantage et ses conséquences graves, voire catastrophiques pour les entreprises ciblées, ont retenu toute l'attention des participants.

La prise de conscience de l'existence de cette menace et des conséquences potentielles pour votre entreprise est une première étape qui doit se poursuivre par un plan d'action adapté à votre contexte.

Les principaux jalons proposés par les spécialistes de la sécurité de l'information sont :

• Identification des informations selon 3 catégories :
- L'information blanche, c'est-à-dire sans impact sur votre activité,
- L'information tactique, sa communication permet d'en déduire de l'information stratégique,
- L'information stratégique, sa communication est rédhibitoire à la bonne poursuite de votre activité.

• Identification des collaborateurs manipulant ces informations et leurs outils de travail : PC, Smartphone, bloc note.
• Mise en œuvre de mesures personnalisées aux risques et aux acteurs.

Il ne s'agit pas de surprotéger toutes les informations et tous les acteurs de votre entreprise, le coût serait prohibitif et les mesures sécuritaires trop contraignantes à sa bonne marche. Il est nécessaire de doter les acteurs concernés d'outils sécurisés et d'amener les collaborateurs à mettre en pratique une « hygiène digitale ».

Les principaux outils et attitudes sont très simples à mettre en œuvre :

• Des disques durs cryptés, des clés USB différentes pour les données personnelles et les données professionnelles et une clé pour les échanges de document en réunion.
• Un anti-virus et autre parade contre les logiciels malveillants.
• Un film protecteur sur le PC portable pour restreindre la lecture.
• Un mot de passe de 6 caractères et plus sur tous vos équipements.
• Pas de données personnelles ou d'informations trop précises sur les réseaux sociaux.
• Pas de réunion de travail dans les lieux publics.
• Toujours garder un lien physique avec son équipement mobile.

Contact :
Olivier Roecker
Directeur Systèmes d'Information
o.roecker@fed-plasturgie.fr