



LES CONFÉRENCES DU MARTROI

Espionnage et pratiques déloyales... votre entreprise est-elle à l'abri ? Tel était le sujet d'actualité abordé lors de la conférence du jeudi 26 mars 2009 organisée par la CCI du Loiret et la Jeune Chambre Économique d'Orléans.

Une conférence réussie !

Ce ne sont pas moins de 130 personnes, représentant 96 entreprises qui ont participé jeudi 26 mars à la conférence « Espionnage et pratiques déloyales... votre entreprise est-elle à l'abri ? ».

A cette occasion, un collaborateur de la Direction Départementale du Renseignement Intérieur (DDRI) a dévoilé les nombreuses failles des entreprises quant à la sécurité de leur système d'information.

Résumé de la rencontre

Après les mots d'accueil successifs de Yves BROUSSOUX, Président de la CCI du Loiret, de Sébastien MARQUANT, Président de la Jeune Chambre Économique d'Orléans et de Christian Martinez, Directeur Régional du Renseignement Intérieur, l'agent de la DDRI a animé une conférence de 2h sur les menaces et les vulnérabilités méconnues des entreprises quant à la sécurité économique. Après avoir fait une présentation des acteurs du Renseignement en France, il a présenté les nouvelles missions de la DDRI ainsi que les différentes cibles dans l'entreprise tout en précisant les vecteurs de la menace. Il a également démontré au travers de chiffres clés et par des exemples concrets en quoi les systèmes d'information pouvaient être vulnérables et quelles en sont les différentes parades.



La synthèse de la présentation

Les missions de la DCRI

La DCRI est née de la fusion entre la Direction de Surveillance du Territoire (DST) et la Direction Centrale des Renseignements Généraux. Ses nouvelles missions relèvent du contre-espionnage, du contre-terrorisme, de la protection du patrimoine et de la lutte contre les proliférations ainsi que de la lutte contre les violences subversives.

Jusqu'à aujourd'hui les acteurs du renseignement connus se limitaient aux Services de Renseignement d'État et aux sociétés de renseignement privées.

Au delà de ces acteurs « visibles », on trouve désormais de nouveaux commanditaires :

- Les États, les nations,
- Les concurrents,
- Les groupes de pression,
- Les groupes terroristes et autres crimes organisés.

Une menace est un danger qui existe dans l'environnement d'un système indépendamment de celui-ci et peut être défini en fonction de son origine (interne ou externe), de son caractère (intentionnel ou accidentel) et enfin de sa nature (physique ou logique).

Chiffres clés

Sur les 3 dernières années, la DCRI a recensé

- 150 secteurs d'activités touchés
- représentant 2637 entreprises
- 4339 atteintes ou mises en danger
- 3400 auteurs ont été identifiés avec 91 nationalités différentes

Dans ce laps de temps, la Région Centre se situe en 7^{ème} position des régions françaises en termes d'attaques d'entreprises, phénomène dont la tendance est à la hausse.

Dans l'entreprise, les cibles sont multiples et variées

- L'image de marque de l'entreprise est continuellement exposée aux attaques extérieures
 - ⇒ Une modification dommageable de la présentation et du contenu du site de l'entreprise peut engendrer une perte de confiance de certains clients et une diminution de sa crédibilité...
- Le patrimoine
 - ⇒ Un incendie ou un dégât des eaux suffit pour détruire ordinateurs, fichiers et archives.
- L'information stratégique
 - ⇒ Un ordinateur portable volé peut contenir des informations stratégiques (des données financières de l'entreprise, des informations sur la R&D, des informations commerciales, les fichiers clients, les brevets...).
- Les systèmes de communication et d'information
 - ⇒ Ils constituent le système nerveux de l'entreprise mais aussi son talon d'Achille : piratages et virus sont capables de paralyser l'ensemble du réseau informatique.

- Les cadres-dirigeants, les employés...
 - ⇒ leurs bavardages dans les transports en commun peuvent tomber dans l'oreille d'un concurrent ou d'une personne malintentionnée. A fortiori, il existe des prises d'otages de salariés pour extorsion d'informations.

L'origine de la menace peut être interne, externe ou concerner l'environnement proche de l'entreprise.

- On estime que 80% des menaces ont une origine interne à l'entreprise, souvent dues à des employés indécidés ou en conflit avec leur hiérarchie, des collaborateurs désireux de créer leur propre société, ou encore ceux sollicités par la concurrence...
- En externe, on situe les attaques au niveau des concurrents directs mais apparaissent de nouveaux acteurs malveillants que sont les pirates informatiques ou « hackers ». En général, le but est ludique ou pour acquérir une certaine reconnaissance mais parfois il s'agit de personnes recrutées par la concurrence, le grand banditisme ou bien par des sociétés de renseignements privés pour le compte de commanditaires.
- Dans l'environnement proche de l'entreprise on retrouve également des acteurs externes : prestataires de services, auditeurs, stagiaires, intérimaires... qui peuvent en menacer la pérennité.

Les parades

Pour réduire le risque d'attaque, une démarche de management globale est nécessaire. Il s'agit avant tout de recenser les menaces et d'établir la liste des données sensibles à protéger.

Au niveau de l'entreprise, il est utile de :

- Mettre en place une organisation adaptée, un plan de sécurité interne par exemple,
- Sensibiliser les collaborateurs et les impliquer dans la démarche de mise en place d'une politique de sécurité en communiquant sur les comportements et les bonnes pratiques à adopter,
- Mettre en place des produits de sécurité en adéquation avec les besoins identifiés (antivirus, pare-feu, chiffrement ou cryptage de données, sauvegardes internes et externes...),
- Contrôler les accès aux ressources informatiques (charte informatique, engagement de confidentialité...),
- Surveiller son réseau et mettre en place des correctifs,
- Etre vigilant sur les contrats d'externalisation : les prestataires de services de nettoyage, d'audit, de conseil venant régulièrement dans l'entreprise...

Au niveau de l'individu, il est approprié de :

- A l'intérieur de l'entreprise :
 - ⇒ Faire « bureau net » et le fermer,
 - ⇒ Utiliser avec prudence téléphone, GSM, fax, visioconférence,
 - ⇒ Porter un badge,
 - ⇒ Accompagner les visiteurs.
- A l'extérieur de l'entreprise :
 - ⇒ Etre attentif à ne pas bavarder n'importe où (lieux publics : salons, conférences, transports en commun...)
 - ⇒ Etre vigilant lors des voyages à l'étranger, résister aux tentations trop visibles ...

La sécurité économique active procède d'un état d'esprit, d'une prise de conscience et relève du rôle de chacun ce qui implique la mobilisation et l'adhésion de tous.

Elle est une affaire de bon sens, de logique mais surtout de vigilance à tous les niveaux.