La protection des données numériques, un sujet à prendre au sérieux dans les entreprises

jeudi 13 décembre 2012, par lpe

Le 10 décembre, Eric Gallot, chef d'escadron de la gendarmerie de Poitiers, et Jérôme Moreau, Gendarme à Poitiers, ont donné une conférence dans les locaux de l'IAE de Poitiers, sur une initiative des étudiants de l'ICOMTEC sur l'importance de la protection des données numériques pour une entreprise dans le contexte de concurrence actuel.

La conférence s'est organisée en trois temps. Tout d'abord, les gendarmes ont donné une définition de l'Intelligence Economique, ensuite ils ont expliqué pourquoi les entreprises devaient absolument être prudentes avec l'ensemble de leurs données numériques pour conclure dans un dernier temps en donnant des exemples de l'actions de la gendarmerie dans ce domaine.

Selon Alain Juillet, ancien Haut Responsable chargé d'Intelligence Economique, « *l'Intelligence Economique consiste en la maîtrise et la protection de l'information stratégique pour tout acteur économique. Elle a pour triple finalité la compétitivité du tissu industriel, la sécurité de l'économie et des entreprises et le renforcement de l'influence de notre pays* ».
Afin d'assurer une présence effective à ce niveau, l'Etat se doit d'intervenir selon trois axes principaux, à savoir la veille stratégique, le soutien à la compétitivité des entreprises et à la capacité de transfert des établissements de recherche publics ainsi qu'à la sécurité économique.

Pour une entreprise, les menaces concernant le vol de données numériques peuvent être internes, externes ou mixtes. En effet, tant les facteurs organisationnels et informatiques que ceux stratégiques, économiques, humains ou encore sociaux doivent être pris en compte.
La prise de contrôle par un fond d'investissement (affaire GEM Plus), les OPA hostiles (affaire Perrier), les

atteintes à l'image (affaire du saumon) ou encore les abus de confiance (affaire Valeo) prouvent que les entreprises françaises ont été et peuvent encore être touchées par des actions en interne ou en externe afin d'accéder à leurs données confidentielles.

La « guerre économique » existe bel et bien en Europe.

1 entreprise française sur 4 est victime d'attaques, et 1 entreprise sur 2 en Allemagne pour un préjudice de 15 à 20 milliards d'euros par an.
Il faut savoir que ce sont les PME les plus touchées, car disposant de moins de moyens que les multinationales, leurs protections ne sont pas optimales et il est facile de les duper.
Les trois principaux risques pour les entreprises sont :
- Les risques humains : au niveau des collaborateurs avec les débauchages opportuns, les faux entretiens d'embauche, les salariés espions et l'exploitation des faiblesses d'employés malléables (les protestataires ou les démotivés par exemple).
- Les risques informatiques : ces risques sont très importants car il est relativement simple de mettre en place des attaques informations, avec tous les livres disponibles à ce sujet dans le commerce notamment, et c'est peu couteux. Ces actions visent à voler, exploiter, détruire ou encore corrompre des données stratégiques ou encore à perturber voire à bloquer le bon fonctionnement du réseau interne de l'entreprise (exemple du virus Stuxnet).
- Les risques terrains : les attaques physiques d'une entreprise sont loin d'être négligeables ; de nombreux sabotages conduisent à des vols importants de données.

Pour contrer cette menace de vol de données confidentielles pour les entreprises, la Gendarmerie Nationale travaille en partenariat avec les CCI régionales. Le maillage territorial est très important car la proximité permet la mise en place d'actions de sensibilisation et l'élaboration d'un bilan de vulnérabilité. Ce dernier évalue le degré de risque des entreprises face à ce piratage de données.
En effet, la Gendarmerie de Poitiers propose aux PME d'établir pour elles des diagnostics, afin d'évaluer leur niveau de protection et de leur fournir des solutions.
Neuf points critiques sont développés afin de permettre une prévention efficace :
- Risques liés aux fournisseurs et sous-traitants,
- Risques liés aux clients,
- Risques liés au facteur humain (interne et externe),
- Risques liés à l'activité de Recherche & Développement,
- Risques liés à la protection physique du site,
- Risques liés au système informatique,
- Risques liés aux outils numériques,
- Risques capitalistiques,
- Risques liés aux prestataires extérieurs.

La Gendarmerie Nationale procure des recommandations autour de trois principales thématiques.
La première concerne l'environnement de l'entreprise, son site et ses locaux. Au niveau du site, les gardiens sont primordiaux par exemple, au niveau des locaux les portes et fenêtres doivent être bien verrouillées et les déplacements sur le site doivent être supervisés grâce à l'utilisation de badges ou des registres de visite par exemple.
La seconde concerne les risques liés aux systèmes d'informations des entreprises. Les outils, à savoir les mots de passe et l'utilisation d'antivirus sont primordiaux. Sécuriser les informations au niveau du serveur de l'entreprise est également une précaution à prendre. Le réseau intranet et le site web doivent également être sous vigilance constante.
La troisième thématique concerne le facteur humain. L'entreprise doit toujours être vigilante avec ses employés et ses prestataires extérieurs afin de garantir l'opacité de ses informations confidentielles.

La conclusion de cette conférence pourrait être la suivante : il ne faut pas que les entreprises cèdent à la paranoïa mais il faut cependant qu'elles soient extrêmement vigilantes dans le contexte de concurrence actuel.

Cette conférence était organisée par Cellie (la cellule d’intelligence économique de l’IAE de Poitiers), JEIC (la Junior-Entreprise IAE Consultants) et le Service Communication de l’IAE de Poitiers.