Extrait du Spyworld Actu

https://www.spyworld-actu.com/spip.php?article5065

Henri Samier : la protection des entreprises est protéiforme

- Intelligence économique -

Date de mise en ligne : dimanche 15 juillet 2007

Spyworld Actu

Dépôt de brevets, secret, mais aussi sécurisation des données informatiques... La protection des entreprises revêt différentes formes, souvent complémentaires. Des pratiques essentielles parfois oubliées voire méconnues des PME, et pourtant gages de leur pérennité comme l'explique Henri Samier, directeur du Master Innovation à l'ISTIA d'Angers.

Pourquoi les entreprises doivent-elles se protéger ?

"Tout simplement parce que les innovations technologiques développées par les entreprises, quelles que soient leur taille et leur activité, constituent des investissements non négligeables. Si ces innovations ne sont pas protégées, le risque est grand de voir leurs productions copiées. In fine, la pérennité de l'entreprise peut être remise en cause."

Comment se protéger ? Y a-t-il différentes formes de protection ?

"Je distingue en fait trois degrés de protection possibles. Le premier, le plus évident peut-être, consiste à mener une politique de dépôts de titre de protection industrielle auprès de l'INPI (brevets, marques, dessins et modèles). Dans certains cas, lorsque l'entreprise a des productions saisonnières, c'est finalement le renouvellement rapide des gammes qui assurera de fait la meilleure des protections face aux contrefacteurs. Intéressant aussi le procédé du secret lorsque le produit est difficile à copier en raison de son fonctionnement ou de sa formulation. Chacun pensera à un fameux soda américain, mais le secret concerne bien sûr d'autres secteurs tels que l'aéronautique, la plasturgie... Le secret consiste donc à ne pas diffuser les connaissances élaborées ou acquises par l'entreprise qui doit veiller, en interne, au respect de cette règle."

La maîtrise de la communication apparaît donc essentielle...

"Effectivement, ce que j'appelle 2ème niveau de protection concerne les mentalités et la culture d'entreprise. Cela implique que chaque acteur de l'entreprise sache très clairement ce qu'il convient de communiquer à l'extérieur. Si l'entreprise ne sensibilise pas ses personnels, il y a un risque important de fuites d'informations, sans pour autant volonté de malveillance."

Mais il peut y avoir malveillance...

"Bien sûr. Les actes de malveillance concernent de plus en plus les données informatiques des entreprises qui restent vulnérables. Défendre le capital immatériel des entreprises constitue selon moi le 3ème niveau de protection à mettre en oeuvre. Or, les PME sous-estiment beaucoup la facilité avec laquelle les hackers peuvent s'introduire dans leurs systèmes. À ce titre, il est intéressant de se rapprocher du CLUSIF (Club de la Sécurité de l'Information Français), cette association regroupant des chefs d'entreprises et des collectivités s'intéresse de près aux bonnes pratiques en matière de sécurité des données informatiques."

Piratage, actes de malveillance pour obtenir des informations confidentielles : peut-on parler d'espionnage industriel ?

"Certaines pratiques s'apparentent effectivement à de l'espionnage industriel. Les entreprises peuvent d'ailleurs saisir le correspondant régional de la DST (1) pour une information sur ces pratiques et les moyens de les prévenir.

Sans sombrer dans la paranoïa !"

(1) Service du Ministère de l'Intérieur, la Direction de la Surveillance du Territoire (DST) est notamment compétente en matière de protection du patrimoine économique et scientifique.

Pour en savoir plus : istia.univ-angers.fr/innovation Pour en savoir plus : clusif.asso.fr

Post-scriptum :

http://www.anjou.org/DetailArt_Art....