Websense mesure l'usage du Web 2.0 au bureau

Jugés utiles, les **outils du Web 2.0 demeurent parfois interdits au sein d'une entreprise**. Un constat que rapporte l'éditeur de protection de messages électroniques Websense. A l'appui, un rapport établi auprès de **1.300 responsables du secteur IT de 10 pays en février 2009.**

Constat : des incohérences se font jour lorsque le rapport explique que 62% des responsables IT s'accordent à dire que : « *les outils Web 2.0 sont nécessaires à leur activité*« , néanmoins, **9% d'entre eux confirment ensuite avoir le niveau de sécurité requis** pour se prémunir contre les risques.

Dominique Loiselet, Directeur général France et Afrique du Nord de Websense commente : « *En France, les responsables ont le sentiment de disposer d'éléments de sécurité suffisants afin de se prémunir contre des attaques ou pertes venant des outils 2.0. Il y a, à mon sens,* ***une véritable méconnaissance des risques*****« .**

A la loupe, les outils 2.0 les plus utilisés sont les ***webmail*** (messageries), les portails de **type iGoogle, les wikis mais aussi les sites dits de réseaux sociaux.** Ces derniers rassemblent les sites communautaires tels que Facebook, LinkedIn, Viadeo, Twitter… sont les plus souvent interdits en entreprise. L'étude explique ainsi que dans presque la moitié des cas (**48% des personnes interrogées), l'accès à Facebook n'est pas autorisé**. Dans 22% des cas, ce sont les webmails dont l'accès est interdit durant le travail.

Dominique Loiselet commente ce constat : « ***Désormais Facebook a remplacé la machine à café.*** *Il faut donc que les responsables s'accordent pour autoriser les outils 2.0 mais en intégrant leur utilisation dans leur politique de sécurité*« . Car si des mesures trop restrictives sont prises au sein des sociétés, le rapport explique que « ***47% des répondants indiquent que les utilisateurs au sein de leur entreprise essaient de contourner les règles de sécurité Internet***« . Constat logique démontrant l'utilité de disposer d'une politique de sécurité flexible.

Dès lors si les sites Web 2.0, peuvent permettre de créer et de publier leur propre contenu, ils fournissent aussi aux cybercriminels des moyens de mener des attaques sur une cible beaucoup plus large. Il s'agit donc d'**équilibrer le risque d'une perte de données, ou d'informations voire de rendement avec une utilisation utile des réseaux sociaux.**

Si la prudence reste mère de sûreté, force est de constater que l'usage des réseaux sociaux s'est fortement développé. Il s'agit donc aux responsables informatique et de sécurité de savoir qui va où et pourquoi. Un peu comme sur Facebook en somme.