Cybercriminalité: un risque surtout interne

Les conséquences de la cybercriminalité commencent à prendre une ampleur considérable. Selon une récente étude d'IBM, menée auprès de 3.000 entreprises dans le monde, dont 150 en France, le coût du cybercrime dépasse désormais celui des vols et agressions physiques.

Selon les responsables informatiques, la diminution du chiffre d'affaires (79% en France et 72% pour la moyenne des autres pays) et la perte de clients (60% et 67%) seraient les deux plus grandes sources de coût en cas de cyber-attaque. En revanche, seulement 2% des entreprises françaises craignent la perte de prospects, chiffre peu élevé en comparaison avec la moyenne des autres pays (33%). Enfin, 74% des entreprises françaises pensent que la cybercriminalité pourrait porter atteinte à la marque et la réputation de leur entreprise, contre 63% des entreprises du reste du monde. 84% des responsables informatiques pensent que des organisations liées au crime organisé et disposant de technologies sophistiquées ont remplacé les cyberdélinquants isolés. Cependant, ils sont presque **deux tiers à être persuadés que les menaces sécuritaires proviennent désormais essentiellement de l'intérieur de l'entreprise**. Ce taux atteint 54% en France. Pour permettre de réduire l'impact de la cybercriminalité sur leurs affaires, 59% d'entre elles affirment être suffisamment protégées. Cependant, c'est la simple mise à niveau d'un logiciel anti-virus ou d'un pare-feu qui reste en tête du classement des actions prioritaires des responsables informatiques interrogés. Selon IBM, si ces priorités n'évoluent pas, nombre d'entreprises ne seront pas assez équipées pour combattre les menaces sécuritaires quotidiennes, la méthode « pansement » ou « patch » ne suffisant pas. *« Les résultats de cette étude montrent que les entreprises sont conscientes de l'impact de cybercriminalité sur leurs affaires »*, observe Cyrille Nicolas, responsable de l'offre Sécurité d'IBM pour la France, l'Afrique du Nord et de l'Ouest. *« En réalité, c'est une lutte permanente et les protections technologiques que les entreprises ont mises en oeuvre comme les antivirus et les pare-feu ne sont pas suffisantes. Elles doivent aussi prendre en compte le facteur humain, et envisager la sécurité en termes de processus et pas seulement en termes de produits »*, alerte-t-il.