Mise en conformité : encourager la culture de ‘l’excellence IT’

Une étude menée par un « institut » californien, le « IT Policy Compliance Group « , intitulée *« Pourquoi la conformité paie : Réputations et revenus en danger. »* montre que, neuf sociétés sur dix sont exposées au risque financier dû à la perte et aux vols de données.

Selon le document, les entreprises qui ne disposent pas d’un système permettant de vérifier la conformité de l’infrastructure IT prennent des risques inconsidérés. La principale menace qui pèse sur elles, est bien entendu le vol de données sensibles. Et l’on sait, avec la multiplication des témoignages et des affaires qu’un tel hold-up peut coûter très cher. (lire notre article sur le cas Monster.com)

D’après ce même document, il est désormais impératif que les entreprises comprennent l’importance de la mise en place de procédures de sécurité, de contrôles techniques et de surveillance. Il conseille de lancer ces vérifications au moins deux fois par semaine. Un point de vue intéressant, mais qui dans bien des cas reste difficile à mettre en place, par manque de moyens et ou de personnel.

Parmi les grands groupes, l’étude distingue deux types de risques. D’abord pour les sociétés qui sont à la traîne technologiquement et qui ne se penchent pas sur les solutions de mise en conformité, le risque de vol de données et d’une fois tous les trois ans. Par contre pour les grandes organisations à la pointe technologique, le risque de pertes de données et d’une fois tous les 42 ans.

D’après cette analyse, les sociétés qui excellent dans la mise en conformité sont celles qui sont le moins victimes de vol de données ou d’attaques de cybercriminels.

Le coût de la perte de données

Selon le site Attrition.org, les États-Unis ont une moyenne de 280 incidents par an.

Toujours d’après le site associatif, il y a fort à parier pour que ce mauvais résultat continue de progresser, car les entreprises n’aiment pas révéler ce genre d’affaires.

Reste qu’elles sont de plus en plus souvent obligées de le faire sous la pression des gouvernements, des régulateurs, mais aussi des consommateurs, et des actionnaires.

Si ces sociétés cachent la vérité, c’est tout simplement parce que cela s’apparente à de la mauvaise publicité, et que généralement l’annonce d’une intrusion ou de la perte d’un ordinateur contenant des fichiers sensibles, va de pair avec une perte de client et une baisse de revenu, d’une moyenne de 8%.

Les conseils de l’IT Policy Compliance Group

En marge de la publication de cette étude, l’institut américain en profite pour donner quelques conseils aux sociétés qui souhaitent mieux se protéger.

Voici les six étapes à suivre pour mieux se protéger

1 -Introduire des contrôles plus fréquents et appropriés de l'infrastructure IT

2 -Faciliter et simplifier la communication avec les utilisateurs, publier régulièrement les résultats des contrôles, en un mot jouer la carte de la transparence…

3 -Etablir des standards de sécurité plus élevés.

4 -Encourager la culture de « l'excellence IT »

5 -Procéder à un contrôle global toutes les deux semaines

6 -Donner plus de moyens aux équipes en charge des contrôles, et faciliter l'automatisation de ces processus