Entreprises : le BYOD, un danger pour la sécurité informatique

Votre voisin de bureau vient travailler avec son ordinateur, sa tablette et son smartphone. Il est donc ce qu'on appelle un adepte du Bring Your Own Device (BYOD), une tendance qui pourrait mettre à mal la sécurité informatique de l'entreprise, comme le rappellent plusieurs études.

Les salariés connectés, un danger pour l'entreprise

Depuis quelque temps, on voyait les salariés connectés, ces adeptes du BYOD, comme un vrai plus pour l'entreprise de matière de productivité, de réactivité. On ne les voyait peut-être pas assez comme une source d'ennuis informatiques. Selon une étude de l'équipementier informatique Aruba Networks, les salariés connectés représenteraient un danger pour l'entreprise en matière de sécurité, mais pourraient également ne pas être si productif qu'on voulait le croire.

Informatique : 41 % des Français utilisent un appareil personnel pour un travail professionnel

Ces salariés ,dit #GenMobile (génération mobile), qui ont en général entre 18 et 35 ans, et qui sont autorisés à pratiquer le BYOD, représenteraient donc un danger pour l'entreprise. Une étude complémentaire du Club de la Sécurité de l'Information Français (Clusif), estime que 41 % des Français utiliseraient un équipement personnel pour traiter des données professionnelles. La cause logique du BYOD. Seulement il n'y a pas que le travail qui semble primer dans le BYOD.

Vers l'interdiction du BYOD en entreprise ?

Or on estime aujourd'hui que le BYOD entraînerait de grosses failles de sécurité du fait du manque de services informatiques sur ces appareils (les DSI des entreprises ne s'en occupent pas), et des pratiques qui y sont liées : surf personnel sur Internet au travail, téléchargement de jeux, pornographie etc On estime aujourd'hui que 44 % du temps passé sur Internet au travail l'est pour raisons personnelles. De quoi faire réfléchir les entreprises quant aux pratiques informatiques qu'elle tolèrent, ou pas.