BYOD : la sécurité divise employeurs et employés

L'**impact du BYOD** (Bring Your Own Device) sur la sécurité des systèmes d'information et la confidentialité des données est diversement appréhendé par les salariés et les employeurs, indique **Webroot** dans un rapport. Le fournisseur américain de solutions de sécurité informatique fait référence à deux enquêtes en ligne réalisées aux États-Unis par **Harris Poll**. La première a été menée en décembre 2013 auprès d'un échantillon de **2 129 employés**, la seconde, en avril 2014, auprès de **205 professionnels IT** actifs dans des entreprises de 500 salariés et plus.

Mobile et sécurité

41% des employés interrogés ont déclaré utiliser un smartphone ou une tablette dans le cadre professionnel pour accéder à leur messagerie ou à d'autres données de leur entreprise. Parmi eux, **78% utilisent leur propre terminal mobile**. Bien que 67% des salariés assurent que leur dispositif est équipé d'une application de sécurité, une majorité se contente des logiciels dédiés préinstallés en usine. Si 86% des collaborateurs affirment utiliser des mesures de protection de base (mots de passe, accès WiFi sécurisé…), seuls 19% des terminaux concernés seraient équipés d'une suite de sécurité.

Autre point sensible : les politiques internes de BYOD. **Une stratégie qui imposerait l'installation d'applications de sécurité spécifiques divise**. 54% des collaborateurs seraient prêts à accepter l'installation de ces logiciels, alors que 46% des employés cesseraient d'utiliser leurs terminaux personnels pour le travail. Ils craignent en priorité (55%) l'accès d'un tiers à leurs données personnelles. L'effacement de données et la géolocalisation par l'employeur sont d'autres sujets d'inquiétude.

En la matière, les femmes (57%) sont davantage préoccupées que les hommes (41%). Elles sont également plus nombreuses (**81% de femmes contre 66% d'hommes**) à estimer que les employés devraient contribuer à la décision portant sur le choix d'une application de sécurité. Mais les employeurs rechignent encore à les consulter et plus de 60% ne prennent pas vraiment en considération les préférences de leurs employés en ce qui concerne la sécurité des terminaux.

La gestion du risque

L'heure est au management du risque. 98% des employeurs déclarent avoir fixé **une politique en matière de sécurité mobile**. Et 73% autorisent l'accès aux données de l'entreprise via un terminal personnel. Parmi ces dirigeants : 33% requièrent l'installation d'une application spécifique sélectionnée par leurs soins, 21% permettent l'accès sans consigne de sécurité et 19% demandent à ce que le terminal soit équipé d'une solution de sécurité avant d'autoriser l'accès *corporate*.

Sans surprise, 95% des entreprises interrogées s'inquiètent des risques que font peser le BYOD sur la sécurité de leurs systèmes, réseaux et données. Et **96% des employeurs redoutent la faille**

critique. Webroot, qui prêche pour sa paroisse, avertit : *« Si l'entreprise ne respecte pas les droits de ses employés en matière de BYOD, ces derniers cesseront d'utiliser leurs terminaux personnels à des fins professionnelles. Chacun perdrait alors la productivité et l'équilibre entre travail et vie privée qu'apporte la mobilité »*.

crédit photo © watcharakun – Shutterstock

Lire aussi

Mobilité : le juteux marché du BYOD

Sécurité : cher, très cher BYOD