

Données personnelles : Les salariés se méfient de leur employeur

Sécurité

Posté par : JerryG

Publié le : 4/7/2013 15:00:00

Un rapport de la société **Aruba** montre que les **salariés sont inquiets à l'idée de perdre leurs données personnelles**, une inquiétude qui pousse nombre d'entre eux à utiliser leurs terminaux personnels à l'insu de leur employeur

Aruba Networks, l'un des leaders de l'accès réseau pour l'entreprise mobile, vient de publier une étude mondiale révélant que les salariés qui utilisent leur propre terminal mobile au bureau sont inquiets à l'idée que leur employeur puisse accéder à leurs informations personnelles.

Le rapport de l'étude « Employees tell the truth about your company's data », menée auprès de plus de 3 000 salariés dans le monde, révèle que près de la moitié des salariés européens (45 %) redoutent la perte de données personnelles, une crainte que partagent 40 % des personnes interrogées au Moyen-Orient et 66 % aux Etats-Unis.



Par ailleurs, ils sont 34 % en Europe, 35 % au Moyen-Orient et 51 % aux Etats-Unis à déclarer que leur service informatique ne prend aucune mesure pour assurer la protection des dossiers et applications professionnels se trouvant sur leurs terminaux personnels.

Ces inquiétudes font que de nombreux salariés rechignent à mettre leur terminal personnel entre les mains du service informatique, mettant ainsi en danger les données de leur entreprise. Près d'un salarié européen sur six (soit 15 %) déclare n'avoir même pas prévenu son employeur qu'il utilise un terminal personnel au travail. Ils sont 17 % dans ce cas au Moyen-Orient et en Amérique.

Encore plus inquiétant pour les entreprises : 13 % des salariés européens, 26 % au Moyen-Orient et 11 % aux Etats-Unis avouent qu'ils n'informeront pas leur employeur si leur

terminal était corrompu, même si cela entraînait une fuite de données professionnelles. Ils sont par ailleurs 40 % en Europe, 41 % au Moyen-Orient et 36 % en Asie à affirmer qu'ils ne signaleraient pas immédiatement une fuite de données.

Cette réticence s'explique par la perception négative que les salariés ont du service informatique de leur entreprise. Ils s'inquiètent plus particulièrement de ce que le personnel informatique pourrait faire de leur terminal et des données qu'il contient. 25 % des salariés européens interrogés, 31 % au Moyen-Orient et 45 % aux Etats-Unis sont inquiets à l'idée que le personnel informatique accède à leurs données personnelles, et ils sont 18 % en Europe et 26 % au Moyen-Orient à craindre que leur service informatique ne fouille dans leurs données privées s'ils lui confiaient leur terminal.

Lorsqu'on leur demande comment elles réagiraient si le personnel informatique de l'entreprise accédait à leurs données personnelles, près de la moitié des personnes interrogées en Europe et au Moyen-Orient répondent qu'elles seraient en colère, tandis qu'elles seraient 41 % en Europe, 47 % au Moyen-Orient et 46 % aux Etats-Unis à percevoir cela comme une violation.

Ben Gibson, directeur marketing chez Aruba Networks, a déclaré : « *L'attitude menée des deux côtés de l'Atlantique montre que les employés et les services informatiques jouent avec la sécurité des données, mais cela n'est pas uniquement le fait du hasard. Pour résumer : autant les salariés acceptent mal le pouvoir que les employeurs exercent aujourd'hui sur leurs données personnelles, autant ils sont indifférents à la sécurité des données de l'entreprise.* »

« *L'utilisation de terminaux électroniques personnels pour un usage professionnel (BYOD) est devenue aujourd'hui une réalité face à laquelle les entreprises doivent adopter des solutions pour, d'un côté, garantir le caractère privé des données des employés et, de l'autre, exercer un contrôle plus strict sur le réseau afin de s'assurer qu'aucune information sensible ne puisse être divulguée, le tout sans perturber l'expérience de l'utilisateur* », a-t-il conclu.

Il existe clairement un fossé entre ce que les employés veulent et ce dont les services informatiques des entreprises ont besoin. Créer une véritable séparation entre données personnelles et données de l'entreprise contribuerait fortement à résoudre ces problèmes et à tranquilliser les salariés.

Pour gérer l'utilisation des appareils mobiles personnels, l'application mobile Aruba Workspace provisionne une zone cryptée distincte sur les terminaux afin d'y stocker les applications et les contenus à caractère professionnel. Cette technique assure aux services informatiques une maîtrise totale des informations de l'entreprise enregistrées dans cet espace chiffré et ce, sans la moindre visibilité des zones personnelles du terminal, protégeant ainsi la vie privée des employés.

Pour obtenir de plus amples informations et accéder au contenu détaillé de l'attitude ([Employees tell the truth about your company's data](#)).