Accès restreint aux applications professionnelles depuis son mobile
Mobilité
Posté par : JulieM
Publiée le : 25/10/2012 13:30:00

Une étude indépendante, commandée par Ping Identity, leader de la sécurité d'identification Cloud, révèle que **les entreprises restreignent l'accès des employés aux applications** nécessaires à leur travail en raison de leurs craintes liées à la sécurité et à la sauvegarde de l'intégrité des données.

Les employés français utilisent en moyenne cinq applications de travail chaque jour, mais près d'un tiers (23%) affirment qu'ils ne sont pas autorisés à accéder à ces applications via leurs appareils mobiles. Beaucoup indiquent qu'ils pourraient avoir accès à certaines applications critiques de travail (43%), mais seulement 26 % peuvent parfaitement travailler à partir de leur appareil mobile de la même façon que sur leur lieu de travail et bénéficier ainsi d'un accès à toutes les applications.

Les applications liées aux données financières sont en tête de la liste des accès restreints (42%). 38% des employés ne pouvant pas accéder aux applications via leurs mobiles ont des accès limités concernant les applications de type Salesforce (38%) ou les applications partenaires (13%).

En outre, plus de la moitié des répondants (52%) déclarent que le besoin de sécurité est la principale raison pour laquelle l'accès à certaines applications est restreint. Alors que 18% des employés pensent que cet accès limité est lié à un problème majeur de gestion des accès par l'entreprise.

Reconnaissant la nécessité de créer un environnement transparent pour le personnel au travail, un tiers des entreprises ont permis l'accès de leurs employés aux applications internes et externes avec les mêmes identifiants et mots de passe. Utiliser Single-Sign-On (SSO) est un moyen de contrôler les points d'accès et d'éviter la multiplication des mots de passe.

« *Les employés deviennent de plus en plus mobiles et les applications professionnelles sont de plus en plus utilisées notamment via le Cloud. Les mesures de sécurité doivent donc commencer par la*

gestion de l'identité de l'individu, et non pas de ses applications ou périphériques. Il faut offrir aux employés un accès transparent aux applications critiques tant à l'intérieur qu'à l'extérieur de l'entreprise, ainsi qu'à la gestion des connexions. C'est essentiel pour assurer la réussite de l'entreprise dans des délais extrêmement compétitifs. » commente **Jason Goode**, Directeur EMEA de Ping Identity « *Restreindre l'accès aux applications via des appareils mobiles est une réaction réflexe liée aux craintes de fuite et de sécurité des données. Toutefois, ce contrôle verrouillé ne sera pas nécessairement adapté à une génération de plus en plus mobile.* »

D'où et quand se connectent les employés Français ?

Tandis que seulement 16% des Français interrogés affirment accéder à leurs applications professionnelles depuis leurs salles de bains, 31% des Britanniques indiquent le faire. En outre, près de 40% des Français interrogés admettent accéder à des applications professionnelles depuis leur chambre (contre un tiers des Britanniques).

Autres moments et lieux étranges depuis lesquels les employés se connectent à leurs applications professionnelles : pendant un rendez-vous amoureux (17%) ou un événement sportif (15%) ou à partir d'un établissement médical (20%) ou d'un hangar. 7% des salariés révèlent que leur cabane de jardin est l'endroit le plus étrange depuis lequel ils se sont connectés .