

Internet : PME et réseaux sociaux, vers une interdiction ?

Internet

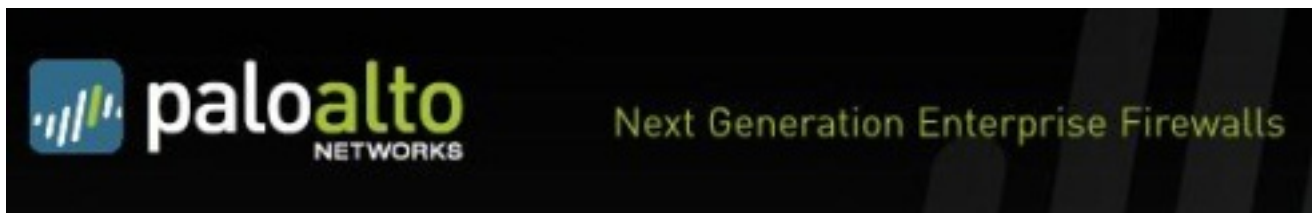
Posté par : JulieM

Publiée le : 7/4/2010 0:00:00

Une étude révèle que les industries fortement réglementées **n'ont pas la maîtrise des applications de réseaux sociaux** et des risques associés

Une récente étude de **Palo Alto Networks** révèle qu'en dépit des problèmes de conformité, les sociétés de services financiers et les établissements de santé utilisent en moyenne 28 applications de réseaux sociaux.

Selon la dernière étude réalisée par Palo Alto Networks™, spécialiste de la sécurité des réseaux, l'utilisation d'applications Entreprise 2.0 s'intensifie partout dans le monde, tout particulièrement dans les secteurs d'activité les plus réglementés. Tandis que les médias sociaux ont envahi les entreprises du monde entier, leur utilisation a très largement devancé leur contrôle. Le degré de risques associés varie considérablement selon les secteurs et les lieux, en fonction de facteurs tels que les réglementations et la cybercriminalité. Les professionnels de l'informatique doivent tenir compte de la diversité des risques dans le cadre de leurs politiques d'utilisation des applications, leurs besoins en termes de conformité et leurs profils de sécurité.



Disponible dès aujourd'hui, le rapport sur l'utilisation des applications et les risques associés (Application Usage and Risk Report, 5e édition, printemps 2010) de Palo Alto Networks est une étude semestrielle qui évalue le trafic applicatif du monde réel à travers plusieurs centaines d'entreprises dans le monde. Cette nouvelle édition du rapport révèle qu'il n'a jamais été aussi facile d'accéder à des applications, ce qui accélère leur adoption indépendamment de la géographie ou du secteur vertical. Alors que les employés du secteur médical ou financier utilisent de plus en plus les médias sociaux pour la collaboration professionnelle, ils ignorent souvent les risques associés tels que la non conformité, la perte de données et la propagation des menaces. Ces risques peuvent compromettre la sécurité du réseau de l'entreprise, ainsi que son intégrité dans son ensemble.

Le rapport montre par exemple que **94 %** des sociétés de services financiers et des établissements de santé inclus dans l'étude utilisent en moyenne 28 applications de réseaux sociaux, dont Facebook, Twitter et LinkedIn. Dans ces deux secteurs, des réglementations (telles que HIPAA et FINRA) exigent que les entreprises contrôlent et surveillent les flux d'informations à travers les applications de réseaux sociaux afin de protéger les données confidentielles qu'elles gèrent. Cependant, tout le trafic est considéré comme du trafic Web car les applications de réseaux sociaux utilisent les ports 80 ou 443. Cette visibilité réduite du trafic généré par les réseaux sociaux pourrait constituer une violation, ou entraîner des violations, de la conformité vis-à-vis des réglementations

de l'industrie.

Par conséquent, bon nombre de responsables informatiques se voient obligés d'interdire complètement les applications de médias sociaux. Mais est-ce vraiment réalisable ?

« Les responsables informatiques ne peuvent pas se contenter de bloquer les applications Entreprise 2.0 étant donné leur utilité professionnelle évidente. Ils ne peuvent pas non plus permettre à ces applications de proliférer sur leurs réseaux. Le service informatique doit mettre en œuvre les applications Entreprise 2.0 de manière sécurisée », a déclaré René Bonvanie, vice-président du marketing mondial de Palo Alto Networks. « En définissant et en appliquant des politiques permettant la mise en œuvre sécurisée de ces applications, le service informatique peut améliorer la productivité de l'entreprise tout en réduisant les risques de sécurité et les violations de conformité. »

Autres constats de cette étude :

- **Parmi les 41 applications de messagerie électronique** rencontrées, 26 variantes Web ont été détectées dans les secteurs des services de santé et financiers, utilisant respectivement 220 Go et 152 Go. L'utilisation répandue de la messagerie Web présage de nombreux risques pour l'entreprise et la sécurité, notamment des violations de conformité, la fuite de données et la propagation de logiciels malveillants.

- **Deux tiers des 750 applications** ayant été suivies dans le cadre de cette étude, y compris les applications client-serveur et peer-to-peer (P2P), peuvent passer pour du trafic Web grâce au "port hopping" (saut de ports), en utilisant le port 80 ou en dissimulé dans un tunnel SSL. Cela réfute le mythe selon lequel les ports 80 et 443 sont uniquement réservés au trafic Web. Si les applications de partage de fichiers P2P ressemblent à du trafic Web, elles sont par conséquent difficiles à détecter et à contrôler. Cela augmente considérablement le risque de fuite de données accidentelle.

- **L'utilisation d'applications Web** de partage de fichiers consomme 399 Go de bande passante dans les sociétés de services financiers et 143 Go dans les établissements de santé. La mise à disposition de ces applications étant sur une base 1:1, le risque de perte ou de fuite de données accidentelle est réduit, mais cela n'empêche pas la transmission délibérée de données confidentielles, à moins que des contrôles de politique stricts soient en place.

- **La bande passante consommée** par les applications de réseaux sociaux a doublé au cours des 18 derniers mois pour atteindre 9 Go par entreprise.

Les informations sur plus de 950 applications identifiées par Palo Alto Networks ont été publiées dans Applopedia, qui fait partie du centre de recherche sur les applications et les menaces de la société. Pour connaître l'actualité, les commentaires et les [dernières découvertes sur les applications et les menaces](#)