

PGP crypte les données de bout en bout

Infosecurity Europe, Londres. Occupant l'un des plus gros stands de ce salon londonien, PGP, éditeur américain de solutions de sécurité, se lance à la conquête du marché européen.

Le cryptage reste la méthode la plus sûre pour éviter de voir ses données confidentielles et sensibles se propager sur le Web à la suite d'un vol d'ordinateurs portables ou de terminaux mobiles.

PGP présente une plate-forme de cryptage permettant de traiter l'ensemble des besoins des entreprises avec une seule application: PGP Encryption Platform.

Répondant aux sociétés qui souhaitent en priorité protéger leurs e-mails, PGP a imaginé Desktop Email 9.5. Il s'agit d'un outil automatisé et simplifié de cryptage des courriels ; il sécurise les contenus sensibles présents à la fois sur les portables et sur les ordinateurs de bureau.

Desktop Email 9.5 protège les communications entrantes et sortantes et supporte la majorité des standards de sécurité en matière d'e-mails ; il est compatible avec la plupart des applications de messagerie.

Notons que pour les destinataires qui ne disposent pas de solutions de sécurité, l'expéditeur peut choisir d'envoyer le document en mode encrypté à l'aide de PGP Zip ou de PGP Self-Decrypting Archive. Une fois cette procédure terminée, l'e-mail est envoyé de façon standard.

Une méthode d'encryptage simplifiée

PGP Desktop Email et PGP Universal Server sont des solutions dont la philosophie réside dans l'automatisation du processus. Elles disposent d'une console de management unifiée permettant de mettre à jour les règles de sécurité d'un groupe en temps réel. En outre, cette solution est compatible avec la majorité des infrastructures e-mails, et des protocoles. Des outils sont intégrés à Desktop Email 9.5 pour faciliter son déploiement au sein de l'entreprise et parmi les employés que la direction souhaite protéger. Enfin, l'application peut être personnalisée en utilisant Windows MSI Installer. Les règles de sécurité du groupe sont mises en place à partir de la console de management de l'application.

Une fois le logiciel installé correctement sur les ordinateurs des collaborateurs, ces derniers peuvent immédiatement poursuivre leur activité. Les messages sont automatiquement encryptés, décryptés et signés numériquement. Le contenu du courriel est également vérifié selon les critères préétablis dans les règles de sécurité du groupe procédant à l'installation.

De cette façon, la charge de travail du service informatique est allégée ; la solution garantit que tous les messages et les pièces jointes associées ont bien été vérifiés. Cela permet d'éviter de confier cette tâche délicate aux salariés du groupe qui ne sont pas formés pour cela.

Cette simplicité d'utilisation que revendique PGP est à l'origine de la grande popularité de ce logiciel aux États-Unis.

Philip M Dunkelberger, p-dg de PGP, explique : « Avec la plate-forme Encryption Platform, nous

proposons une solution complète de cryptage des données qui doit répondre à l'ensemble des besoins de nos clients en protégeant les disques durs, les terminaux Blackberry, les e-mails, la messagerie instantanée, etc. Les règles de cryptage des données doivent être simples et automatisées. Par exemple, le cryptage des e-mails est fait de façon totalement invisible, l'utilisateur ne s'en rend pas compte. »

