

# Emmanuel Obadia : « Aucun système n'est protégé à 100 % »

*Le directeur pour l'Europe du Technology Group de Lotus donne des conseils pour assurer la sécurité.*

→ protocole SMTP (Simple Mail Transfer Protocol), utilisé pour l'acheminement des messages électroniques, fonde sa rapidité sur un code extrêmement simple, dépourvu de toute sécurité.

Les messages sont lisibles par quiconque infiltre un des ordinateurs hébergeant un routeur de courrier électronique, ou tout simplement les serveurs de l'expéditeur ou du destinataire. Et le risque augmente encore avec les services de courrier sur le web.

C'est pourquoi les expéditeurs de données sensibles emploient des programmes de chiffrement permettant de crypter les messages. Une réponse partielle au risque d'interception du courrier électronique par un pirate.

**Antoine BLONDEAU**

– Aucun système n'est protégé à 100 %. Si un pirate spécialisé et expérimenté a décidé de pénétrer dans un système, il y a peu de chance qu'il n'y parvienne pas. Toutefois, dans le cas de l'échange de courrier électronique, l'utilisation de clés chiffrées partagées entre deux correspondants et connues d'eux seuls permet d'assurer une sécurité maximale pour envoyer des informations.

– Pour une entreprise, quel est l'enjeu de la sécurité du courrier électronique ?

– L'enjeu est stratégique.



Emmanuel Obadia. (DR.)

pié collé près de l'écran d'un micro-ordinateur.

Propos recueillis par C. H.

des e-mail et l'infrastructure