

# UN COURRIEL SÉCURISÉ DE L'ÉMETTEUR AU DESTINATAIRE

La protection des données, la garantie de leur intégrité et l'authentification de l'émetteur ne font pas encore partie des politiques de sécurité dans de nombreuses sociétés.

**L**a protection contre les virus, les spam et les phishing n'est aujourd'hui plus une question pour les entreprises. Celles-ci ont, durant ces dernières années, investi beaucoup d'argent et de temps pour se protéger contre des attaques provenant de l'extérieur. Néanmoins, elles n'ont pas encore vraiment pris conscience qu'il existe également des risques importants lorsqu'elles transmettent des informations en utilisant le courriel électronique comme moyen d'échange. Pour les hackers (pirates informatiques), le courriel électronique est une proie facile à attraper pour récolter de nombreuses données sans grande difficulté, ou mieux encore, pour modifier le contenu d'un courriel ou remplacer l'émetteur par eux-mêmes afin de recevoir des informations confidentielles en retour.

## Des produits novateurs adaptés aux besoins

Fort de ce constat, la société e-Xpert Solutions a présenté dernièrement de nouvelles applications à ses clients qui garantissent la

sécurité de bout en bout des courriels électroniques, en proposant les produits Tomtemo TrustMail, ClearSwift et Websense. Ces applications s'articulent principalement autour de deux axes que sont l'intégrité des données et la garantie que la politique de sécurité de l'entreprise est bien respectée.

Les besoins et les critères de sécurité n'étant pas les mêmes d'une entreprise à l'autre, plusieurs configurations et scénarios sont possibles en combinant l'ensemble des produits. L'entreprise qui ne veut pas compliquer la réception d'un courriel choisira une solution de Webmail. Celle-ci consiste à déposer le message à transmettre sur un serveur se trouvant dans une zone démili-

*LES BESOINS ET LES CRITÈRES DE SÉCURITÉ N'ÉTANT PAS LES MÊMES D'UNE ENTREPRISE À L'AUTRE, PLUSIEURS CONFIGURATIONS ET SCÉNARIOS SONT POSSIBLES EN COMBINANT L'ENSEMBLE DES PRODUITS.*

tarisée et à envoyer simplement une notification au destinataire lui demandant d'aller chercher son courriel au moyen de son navigateur en mode protégé (méthode du tunnel). Une entreprise qui souhaite que son courriel sorte de son réseau et soit clairement envoyé au destinataire choisira une solution de chiffrement des données par un échange de clés publiques et privées ou par

la création d'un PDF chiffré et protégé par mot de passe, ou encore par un chiffrement de bout en bout du courriel en utilisant la méthode du certificat.

## Un contrôle total des courriers sortants

En parallèle, pour garantir la politique de sécurité, une solution « DLP Data Leak ou Lost Prevention » pourra être mise en place. Avec une telle application, tous les courriels sortant seront soit contrôlés automatiquement selon certaines règles de sécurité pré-établies, soit validés par un supérieur hiérarchique avant l'envoi définitif selon la méthode appelée « les 4 yeux ». Ainsi, l'entreprise se prémunit d'un envoi accidentel ou intentionnel de données confidentielles et offre la possibilité au supérieur hiérarchique de valider tout envoi jugé « sensible ».

Démonstrations faites en direct, ces différentes techniques fonctionnent parfaitement et répondent à un réel besoin du marché.

## e-Xpert Solutions en quelques mots

e-Xpert Solutions S.A. ([www.e-xpertsolutions.com](http://www.e-xpertsolutions.com)) est une société suisse de services spécialisée en sécurité informatique, dont les fondateurs ont fait de leur passion leur métier. Fort de leurs convictions et de leur expérience, leurs ingénieurs conçoivent, déploient et maintiennent au quotidien des architectures de sécurité au moyen de solutions pragmatiques, basées sur des technologies fondamentales et novatrices, adaptées aux exigences de la clientèle.

Jean-Daniel Faessler