La sécurité en service géré

Pour bien fonctionner, les PME sont devenues très dépendantes de leur IT et de sa sécurité. Mais, faute de ressources internes suffisantes, elles doivent souvent se contenter d'une protection partielle ou inégalement gérée. Appliqué à la sécurité, le modèle de l'infogérance peut offrir une réponse convaincante à cette situation.

« Aujourd'hui, quasi tout le monde sait à quoi sert un anti-virus. Malheureusement, souvent, il n'est pas mis à jour ou est désactivé car il peut ralentir le fonctionnement des applications. Ceci montre que la plupart des PME sont sensibles à leur sécurité mais n'y consacrent pas toujours les moyens nécessaires car elles ont d'autres priorités ou ne perçoivent pas le risque complet », observe **Pierre Lechat**, Business Line Manager chez **Trasys**. Les PME sont conscientes des risques de base du type virus mais peu sont informées des autres types de risques et des possibilités de protection qui y sont liées, notamment en matière d'authentification et d'autorisation des accès. Elles manquent souvent d'une vision globale sur leur infrastructure de sécurité et évaluent mal le niveau critique d'applications courantes et vulnérables comme l'e-mail. Par manque de connaissances pointues en sécurité, elles peuvent prendre des risques sans toujours s'en rendre compte comme placer des serveurs critiques sur le même réseau que les postes PC ou mettre en place une connexion permanente mais non sécurisée avec l'extérieur. « La majorité des PME ne sont tout simplement pas en règle avec les bonnes pratiques pour gérer leur sécurité IT en bon père de famille », note **Pierre Focant**, directeur des ventes de la division Global Solutions de **Systemat**.

Pour obtenir une sécurité optimale de son environnement IT, la PME va devoir sélectionner et combiner plusieurs composantes. Cela comporte pas mal d'exigences, difficiles à satisfaire pour une majorité d'entre elles. Il faut faire appel à un expert capable de paramétrer correctement la solution et d'en assurer le suivi. La solution doit être mise à jour presque quotidiennement, compte tenu de l'évolution très rapide des menaces. Il faut aussi s'assurer que les différents outils spécialisés communiquent entre eux. Bref, pour être correctement mise en place et gérée, la sécurité IT de la PME requiert non seulement un investissement financier mais aussi des compétences spécialisées. « Le seuil d'entrée pour assurer efficacement une protection de l'IT demeure assez élevé. Pour les PME, la possibilité de faire appel à un spécialiste en sécurité paraît d'autant plus justifiée », rappelle **Dirk Laurijssen**, Senior Security Consultant chez **MSP**.

Audit préalable

Avant de proposer ses services, le prestataire effectue généralement un premier audit de l'infrastructure et des procédures sécurité de la PME. Chez la plupart des fournisseurs, cet audit est gratuit si par la suite le client lui commande les prestations associées aux recommandations. Quelle que soit la situation de la PME en matière de sécurité IT, cet état des lieux reste un passage obligé. « Vous devez savoir où vous êtes vulnérable et vous protéger en conséquence. C'est là notre principale valeur ajoutée : nous intervenons d'abord comme un consultant sécurité qui vous recommande la meilleure stratégie de sécurité ICT à suivre par votre PME », souligne Dirk Laurijssen. « La protection va plus loin que la seule infrastructure technique. Il faut

aussi informer le personnel de l'entreprise des risques spécifiques », ajoute-t-il. Après analyse du risque et en fonction des besoins de la PME et de son budget, un contrat spécifique est adapté au niveau de sécurité demandé.

De l'anti-virus au BCRS

Les offres de services sécurité comprennent généralement une partie hardware (système de protection, système de récupération/sauvegarde,...), une partie software (installation des logiciels au niveau des postes de travail,...) et une partie maintenance proactive par télémaintenance. Pour couvrir les multiples risques auxquels la PME peut être confrontée, les prestataires proposent de plus en plus un service global. « Chaque PME peut avoir des besoins bien spécifiques au niveau de sa sécurité. Il s'agit donc plutôt d'une approche au cas par cas. Néanmoins, le concept de l'offre globale reste valable pour couvrir les aspects les plus courants de la sécurité IT », explique Pierre Focant. Les solutions packagées en sécurité comprennent au minimum la protection du mail (anti-spam et anti-virus), la protection réseau (pare-feu), un monitoring à distance du système de sécurité et enfin un service de visite sur site assuré par un informaticien professionnel. Certaines offres incluent aussi l'authentification de l'accès (via *tokens*) et une solution de BCRS (Business Continuity and Recovery Services) pour la récupération des données après sinistre. Ceci étant, même dotée d'un tel service, la PME doit veiller à continuellement mettre à jour sa sécurité. Pour éviter toute surprise, autant s'assurer que ce processus de mise à jour, du moins pour les fonctionnalités de base, est inclus dans le coût initial du service. Sur le plan tarifaire, le service peut être proposée en régie selon des tarifs standards, en mode prépayé, sous forme ASP ou encore intégré dans un contrat.

> « La majorité des PME ne sont tout simplement pas en règle avec les bonnes pratiques pour gérer leur sécurité IT en bon père de famille.

Plate-forme web

Pour certains de ses aspects, la sécurité IT peut aussi être assurée directement depuis une plate-forme en ligne. C'est l'approche qu'a suivie Flexos, avec l'aide de deux partenaires technologiques (ScanSafe et Postini-Google). Accessible via le web, la plate-forme de sécurité de Flexos propose l'essentiel des services pour se protéger contre les menaces véhiculées par internet. Le principe de fonctionnement du service sécurité de Flexos est simple : avant d'atteindre le réseau de la PME, le flux de données qui transite par internet est dévié vers le centre de données de ScanSafe ou Postini où il est soigneusement filtré. Une fois nettoyé de son contenu malicieux, le flux de données est ensuite redirigé vers sa destination finale. « Ce processus constitue un bon moyen d'empêcher les pièces jointes malveillantes, du type *spyware*, usurpation d'identité ou *spam* de pénétrer sur le réseau de la PME. Les avantages pour la PME sont assez évidents : pas d'équipement et de logiciel complexe à installer et à configurer, pas de mise à jour à prévoir, pas de recrutement d'un spécialiste sécurité », souligne **Joyce Proot**, Sales & Marketing Manager de **Flexos**. Le responsable IT de la PME dispose d'une interface (via le portail de Flexos) qui lui permet de définir des mesures de protection spécifiques, de suivre des indicateurs de performance et de créer des rapports sur la sécurité web de la PME. Le coût du service est de 2500 euros par an pour un parc de 25 PC.

Quel que soit le modèle d'infogérance en sécurité choisi par la PME, celle-ci doit en tout premier lieu éviter les pertes de données. Pour ce faire, elle veillera à s'équiper d'un système de sauvegarde pour garantir la continuité de ses activités, à mettre en place un contrôle de l'activité réseau en entrée et en sortie aux moyens de filtres qui tiennent compte de son organisation interne, à s'équiper de logiciels anti-virus et anti-spyware sur toutes les stations de travail et sur les serveurs, et enfin, à s'assurer d'une mise à jour régulière de ses procédures de sécurité pour retrouver une situation stable après sinistre.

PhdB

Appliances de sécurité pour la PME

La sécurité figurant désormais en tête des priorités des PME (Forrester : The State of European SMB IT, janvier 2007), IBM a également décidé de développer une offre de sécurité adaptée à ce segment du marché. Davantage orientée produit que service, l'offre sécurité d'IBM pour les PME (à partir de 50 postes) applique le principe de l'appliance (solution combinant équipement et logiciel). L'offre sécurité d'IBM pour la PME comprend un appliance pour des services de restauration après désastre, trois appliances multifonctionnels pour la sécurité web (anti-virus, anti-spam, VPN, prévention d'intrusion, pare-feu et web filtering) et deux appliances mono-fonctionnels (scanning des codes malveillants présent sur le réseau et sécurisation de l'e-mail). La solution peut être installée et gérée par le client lui-même ou à distance par IBM ou l'un de ses partenaires. Il faut prévoir un coût de base de 2000 euros pour la protection de 100 postes durant la première année.