Optimiser le budget informatique en temps de crise économique

Par Franck Trognee, Country Manager SonicWALL France

Les services informatiques face à la crise actuelle

Dans un contexte de crise économique, même si le budget informatique diminue, les attentes en matière de technologies, elles, continuent d'augmenter. Pour le bien de leur entreprise, les responsables informatiques optimisent les opérations, réduisent les coûts, anticipent et abordent les problèmes avant qu'ils ne surviennent et règlent rapidement les difficultés rencontrées. Rationaliser les processus et gérer activement l'infrastructure informatique devient impératif.

Voici donc quelques règles de base à ne pas oublier :

- ✓ **Garantir la sécurité** : les fonctionnalités informatiques les plus avancées ne sont d'aucune utilité sans la protection du réseau, condition sine qua non à toute activité.
- ✓ **Etre proactif** : planifiez des restrictions budgétaires, ou prévoyez de les intensifier, avant que cela ne vous soit demandé. Echelonnez ces réductions, de sorte que votre entreprise soit prête à diminuer davantage ses dépenses au cas où la situation économique continuerait de s'aggraver.
- ✓ **Agir plus habilement :** une stratégie classique consisterait à repousser les achats de matériel. Au contraire, développez de nouvelles capacités de récupération. Supprimez les équipements superflus pour réduire les frais d'exploitation. Regroupez les centres de données.
- ✓ **Redéployer les ressources informatiques :** donnez la priorité aux initiatives lucratives. La mise en œuvre de nouveaux systèmes de veille stratégique peut, par exemple, aider à analyser de nouveaux segments du marché, ou à hiérarchiser les réductions budgétaires internes.
- ✓ **Simplifier les structures :** de nombreuses entreprises virtualisent leur infrastructure (serveurs, stockage, parfois même les postes de travail) afin de simplifier la gestion informatique. Certaines cependant, notamment les PME, doutent encore des avantages de la virtualisation.

Optimiser les dépenses informatiques en temps de crise

- ✓ **Maîtrisez les chiffres**

En période de crise, il est absolument indispensable de pouvoir justifier toute dépense informatique. Le retour sur investissement (ROI), la réduction du coût total de possession (TCO) et la brièveté des délais de récupération des investissements en nouvelles technologies sont des facteurs de plus en plus déterminants. Les responsables d'achats informatiques devront éventuellement remettre en cause leur préférence pour les grandes marques ou du moins se demander si la supériorité de leurs prix est vraiment justifiée. Les chiffres comptent énormément, non seulement dans l'acquisition d'un nouveau logiciel ou matériel, mais aussi pour légitimer les opérations informatiques régulières.

- ✓ **Utilisez des appliances matérielles**

Les appliances matérielles sont des appareils spécialisés comportant un programme d'application spécifique. Ce type d'appareils limite le temps consacré à la gestion, dans la mesure où les appliances sont généralement prêtes à l'emploi et contiennent leur propre infrastructure. Ces appliances peuvent également se révéler plus fiables car elles fonctionnent sur des systèmes d'exploitation très simples. Certains fournisseurs proposent de gérer les appliances de leurs clients, ou leur offrent une interface de gestion permettant d'administrer plusieurs appliances sur leur propre réseau. Comparables aux appliances matérielles, les appliances virtuelles ou logicielles sont des applications autonomes qui fonctionnent comme des machines virtuelles dans un environnement virtuel.

- ✓ **Utilisez des appareils multifonctions**

Les appareils multifonction, qui supportent plusieurs applications en un seul boîtier spécialisé, se rapprochent des appliances matérielles. Ils permettent de régler le problème de la prolifération de matériel dans l'entreprise. Car si les appliances présentent de nombreux avantages, leur utilisation massive peut rapidement conduire à un encombrement du centre de données.

Pour réduire les coûts de gestion et d'exploitation, un matériel polyvalent, par exemple de gestion unifiée des menaces (UTM), peut être un précieux allié. Les solutions UTM concentrent plusieurs applications de sécurité – comme une combinaison d'antivirus, anti-spam, pare-feu, réseau privé virtuel (VPN), prévention des intrusions, blocage des programmes malveillants, pare-feu applicatif et filtrage de contenu – en un seul boîtier. En mars 2008, le spécialiste de l'étude des marchés IDC annonçait même que les appareils UTM étaient en passe de remplacer les routeurs sur le marché d'entrée de gamme. Il prévoyait également une intensification du phénomène sur ce segment du marché.

- ✓ **Télétravaillez !**

Les entreprises considèrent de moins en moins le télétravail comme un problème, mais plutôt comme une opportunité. Les bénéfices que les entreprises retirent du télétravail, ainsi que les avantages d'ordre écologique sont vecteurs de croissance. A commencer par les améliorations des nouvelles embauches et de taux de rétention des employés. Chez certains éditeurs, la possibilité de travailler à distance serait un facteur déterminant pour les télétravailleurs. En développant le télétravail, l'entreprise réduit ses dépenses en matière de TI, d'installations et de coûts d'exploitation, et encourage la productivité de ses employés.
Cependant, le télétravail peut aussi alourdir la tâche du service informatique. La priorité étant évidemment de garantir un accès distant sécurisé afin de protéger les données entre le bureau à domicile et l'entreprise. Les webconférences sont pratiques dans la mesure où elles permettent aux télétravailleurs de rester en contact avec leurs collègues, tout en réduisant les besoins en déplacements, en particulier des équipes de vente et de marketing. La voix sur IP (VoIP) peut également aider à limiter les dépenses téléphoniques.

- ✓ **Automatisez le contrôle des terminaux**

En raison du nombre croissant d'utilisateurs distants, y compris des télétravailleurs, les entreprises doivent pouvoir réguler l'accès aux ressources sur leur réseau. Pour commencer, établissez une règle exigeant que les appareils d'accès possèdent les versions les plus récentes des logiciels de sécurité, antivirus et anti-spam, afin de protéger le réseau des programmes malveillants. Automatisez ensuite l'exécution de cette règle en recourant à une technologie qui ne permette la connexion qu'aux terminaux correctement protégés.

- ✓ **Réduisez le nombre de fournisseurs informatiques**

L'exploitation d'équipements matériels et logiciels provenant de différents fournisseurs complique la gestion informatique et alourdit les dépenses. Trop souvent, le service informatique doit sacrifier une partie de ses ressources internes ou externes à l'intégration d'appareils ou d'applications

incompatibles. Eliminez les redondances pour réduire les frais de licences et de support. Dans la sélection de vos fournisseurs, négociez fermement et n'hésitez pas à aller voir ailleurs, surtout en temps de ralentissement de la demande. N'ayez pas peur du changement.

- ✓ **Considérez les offres hébergées**

Les contraintes financières augmentent l'attrait des offres hébergées (ou basées sur les services). Contrairement aux applications traditionnelles sur site, les logiciels-services (SaaS) et les services gérés n'entraînent pas, en général, de frais initiaux élevés en matière de licences, avantage non négligeable quand l'argent se fait rare. Le service informatique doit voir les SaaS non pas comme une menace, mais comme un moyen de réduire sa charge de travail.

- ✓ **Passez à l'Internet pour le stockage et le traitement**

Le « cloud computing » est un phénomène d'actualité que les entreprises utilisent, entre autres, pour confier le stockage et le traitement de tâches intensives à des fournisseurs de services Internet. De nombreux revendeurs informatiques locaux et régionaux offrent également des applications basées sur Internet et se sont parfois spécialisés dans un domaine, comme la continuité des activités.

- ✓ **Exploitez les applications du Web 2.0**

Profitez des applications grand public et des technologies Web 2.0 pour accroître la productivité des employés et optimiser la communication. Vos employés utilisent ces applications chez eux ou sur leurs portables, elles leur sont donc familières et ne nécessitent guère de formation. Grâce à elles, les employés bénéficient des mêmes possibilités au travail qu'à la maison. Les services informatiques gagneraient beaucoup à intégrer les technologies Web 2.0 orientées consommateur aux interfaces de leurs applications propriétaires internes.
Comme elles s'adressent aux consommateurs, les technologies Web 2.0 sont souvent peu coûteuses, parfois gratuites. Les services marketing utilisent de plus en plus ce genre d'applications pour fidéliser la clientèle et atteindre de nouveaux cercles d'intéressés, un enjeu décisif en temps de récession. Les services informatiques doivent être prêts à s'ouvrir au Web 2.0 si ça n'est pas encore le cas.

Crise et Sécurité : conclusion

Au-delà des aspects soulevés plus haut, aucun service informatique ne peut risquer de compromettre la sécurité d'un réseau, crise ou pas. Si la protection n'est pas garantie, ce sont toutes les autres installations informatiques qui sont menacées.
Une bonne partie des stratégies esquissées dans ce livre blanc défient le modèle traditionnel de la sécurité réseau, appelé à s'adapter pour intégrer le télétravail, le cloud computing, les logiciels-services, tout comme le Web 2.0 et les services gérés. Il est donc temps de revoir notre conception de la sécurité.
Un nouveau modèle de sécurité émerge, prenant acte des nouvelles tendances et de la nature distribuée des entreprises de toutes tailles. L'enjeu présent est parfaitement résumé par le terme « dépérimétrisation ». En effet, les périmètres de sécurité, qui constituaient autrefois des remparts solides contre les attaques, ne suffisent plus.
Les sites distants, sites de clients et partenaires d'externalisation se situent tous en dehors du périmètre de sécurité traditionnel, tout comme les appareils mobiles et sans fil, ainsi que les ordinateurs portables Wi-Fi. Il en découle de nouveaux risques de brèches dans la sécurité. Pour protéger tous ces éléments, ainsi que le cœur du réseau et les centres de données eux-mêmes, il faut mettre en œuvre plusieurs couches de défense, ou encore un modèle de « défense en profondeur ». L'objectif : sécuriser les ressources par utilisateur et par terminal au-delà du périmètre, ainsi que sécuriser le trafic de données traversant le périmètre.
De plus, certaines applications Web 2.0 récentes dévorent littéralement la bande passante au détriment d'applications vitales. Les experts informatiques doivent donc être capables de

hiérarchiser la consommation de la bande passante réseau en fonction de l'application, du type de fichier ou du profil d'utilisateur.
Les applications poste à poste, notamment, apportent un bénéfice restreint, voire nul, à l'entreprise, mais sont susceptibles de monopoliser une part colossale de la bande passante. Les responsables informatiques doivent donc bannir ce type d'applications ou les restreindre au moyen de limitations de bande passante. En temps de crise, acheter plus de bande pour les amateurs de YouTube n'est sans doute pas la première priorité d'une entreprise.

A propos de SonicWALL, Inc.

SonicWALL s'engage à améliorer les performances et la productivité des petites et des grandes entreprises, ainsi qu'à diminuer les coûts et la complexité d'un réseau sécurisé. SonicWALL a déjà vendu plus d'un million d'applications via un réseau international de dix mille partenaires. Ainsi, des dizaines de millions d'utilisateurs du monde entier peuvent contrôler et sécuriser leurs données professionnelles. SonicWALL conçoit, développe et produit des solutions étendues de sécurisation des réseaux, d'accès distant sécurisé, de sécurisation de messagerie, de protection et restauration permanente des données et de gestion et reporting centralisés. Pour plus d'informations rendez-vous sur http://www.sonicwall.com/

Safe Harbor Regarding Forward-Looking Statements

Certain statements in this press release are "forward-looking statements" within the meaning of the Private Securities Litigation Reform Act of 1995. The forward-looking statements include but are not limited to statements regarding the benefits associated with the Universal Management Appliance, the ability of the EM5000 to reduce administrative costs and the pre-installation of required operational elements into the EM5000. These forward-looking statements are based on the opinions and estimates of management at the time the statements are made and are subject to certain risks and uncertainties that could cause actual results to differ materially from those anticipated in the forward-looking statements. In addition, please see the "Risk Factors" described in our Securities and Exchange Commission filings, including our Annual Report on Form 10-K for the year ended December 31, 2007, for a more detailed description of the risks facing our business. All forward-looking statements included in this release are based upon information available to SonicWALL as of the date of the release, and we assume no obligation to update any such forward-looking statement.

Contact Presse :
Pauline Marguet
Open2Europe
01.55.02.14.52
p.marguet@open2europe.com