

gestion

Pouvez-vous vous permettre de perdre votre réputation en plus de vos données ?

MICHEL PLANTE

EST VICE-PRÉSIDENT, SOLUTIONS CLIENTS, CHEZ FUSEPOINT.

SÉCURITÉ La mise en œuvre d'un bon dispositif de sécurité et de maintien des activités est essentielle pour préserver la réputation d'une entreprise, ses succès commerciaux et la qualité de ses relations avec ses clients.

Des disques durs se volatilisent dans des locaux prétendument sécuritaires. Des serveurs contenant des données financières confidentielles se retrouvent sur Internet. Des virus et une interruption de courant majeur causent des panes de réseau, paralysant les activités de nombreuses entreprises et les forçant même à fermer leurs portes pendant plusieurs jours.

De plus en plus, la sécurité et le maintien des activités étant désormais régulièrement au menu des pages économiques, de nombreuses entreprises s'aperçoivent maintenant qu'elles avaient un faux sentiment de sécurité. Selon les études, elles sont nettement plus conscientes des risques, mais encore mal préparées à réagir en cas d'attaque mettant la sécurité en péril ou en cas de perturbation de leurs activités.

Selon une étude de la firme Gartner, 62 % des chefs d'entreprise et des responsables de l'informatique disent que leur entreprise dépend en partie ou largement du Web pour son fonctionnement (y compris 26 % qui disent vendre des produits ou des services en ligne). Mais malgré tout, la plupart de ces dirigeants sont d'avis qu'il faudrait plus qu'une journée complète pour remettre leurs systèmes en service si jamais se produisait une défaillance. Dans la même étude, Gartner estime que deux entreprises sur cinq ayant été victimes d'un désastre ferment leurs portes dans les cinq années qui suivent. De quoi faire réfléchir sérieusement.

Ernst & Young estime, en outre, que plus du tiers des entreprises canadiennes ne sont pas préparées pour une interruption de leurs activités et qu'une attaque d'envergure, un désastre ou une interruption des activités forcerait 36 % d'entre elles à fermer leurs portes. La firme croit

aussi que 26 % de ces entreprises n'ont pas de plan de maintien des activités et que 25 % n'ont pas de plan de reprise après sinistre pour leurs systèmes informatiques.

Conséquences coûteuses

Voilà pour les extrêmes, mais les gestionnaires commencent à comprendre que les conséquences des brèches de sécurité et des interruptions de service ne se limitent pas aux baisses du chiffre d'affaires et aux occasions perdues. De tels événements ternissent l'image de l'entreprise et entament sérieusement sa crédibilité. Les conséquences peuvent donc s'avérer nettement plus coûteuses à court, moyen et long termes que les seules évaluations de dommage matériel. Ainsi, à titre de fiduciaire respectueux des règles, chaque entreprise est responsable de demeurer opérationnelle et de continuer à servir ses clients.

Pour qu'une entreprise soit vraiment bien préparée au chapitre de la sécurité et du maintien des activités, la planification à cet égard ne doit pas se faire en vase clos, au sein du service d'informatique, mais plutôt être prise en charge par les cadres supérieurs et le conseil d'administration. En fait, la capacité de l'entreprise à réagir en cas d'urgence devrait être aussi importante que les prévisions de ventes, le prix des actions et le bilan de l'entreprise. De plus, pour cerner les risques et leurs effets potentiels sur l'entreprise et pour qu'un programme efficace intégrant technologies, méthodes et ressources humaines puisse être mis sur pied, il est essentiel qu'une évaluation honnête et complète soit réalisée par la direction de l'entreprise.

Mais si la sensibilisation de la direction pour obtenir son adhésion est un passage obligé, qu'en est-il de l'évaluation et de la mise en œuvre du plan par des experts ? De nombreuses entreprises, en particulier celles qui occupent une position intermédiaire sur le marché, ne disposent pas des installations sécurisées, de l'expertise technique ou des ressources humaines pour lutter de manière préventive contre les risques dont elles sont conscientes.

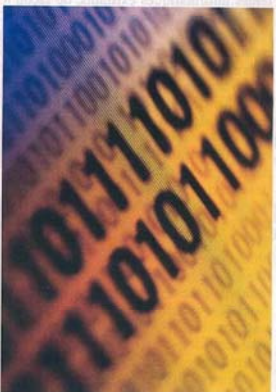
La gestion des rustines applicables aux logiciels constitue une manifestation tout à fait actuelle de ce problème. La société Trend Micro, spécialisée dans les antivirus, estime qu'il y a plus de 70 000 virus infor-

matiques en circulation dans le monde. Comment une entreprise de taille moyenne peut-elle se doter des ressources humaines et financières lui permettant d'appliquer des centaines de rustines par mois, sans compter les mises à jour de son système de détection d'intrusion et de ses coupe-feu ?

Devant un pareil dilemme, la question incontournable consiste à se demander par où commencer.

Une question de confiance

Dans nombre de cas, le recours aux services d'infogérance d'un fournisseur externe à titre de partenaire peut constituer la solution la plus sécuritaire et la moins



chère. Grâce aux économies d'échelle qu'il est en mesure de réaliser, le fournisseur de services d'infogérance est capable d'offrir des installations et une infrastructure sécuritaires, une expertise technique ainsi que des services de planification préventive dont nombre d'entreprises seraient incapables de se doter par leurs propres moyens. Mais à qui peut-on faire confiance ?

Comme dans le cas de bien des partenariats commerciaux du genre, il s'agit essentiellement de choisir un fournisseur qui fera systématiquement preuve de la rigueur et de la minutie nécessaires dans la totalité de ses services. Vous allez payer le fournisseur pour qu'il gère de façon préventive votre infrastructure informatique, y compris vos données et vos applications essentielles, de manière à ce qu'il vous en garantisse la fiabilité, la performance et la disponibilité.

Voici quelques conseils qui devraient vous aider à faire le bon choix.

1 Le centre informatique du fournisseur est-il conçu spécialement pour garantir une disponibilité de 99,999 % ? Les panes de courant et les ruptures de

connexion Internet sont toujours les principales causes d'interruption des activités des entreprises. Par conséquent, il est primordial que le fournisseur pressenti ait une stratégie éprouvée en vue de maintenir l'alimentation électrique et les connexions Internet.

2 Demandez directement au fournisseur si des panes de courant ont déjà interrompu le fonctionnement de ses installations ou les activités de ses clients. Assurez-vous que le centre informatique du fournisseur est relié à au moins deux postes électriques distincts et qu'il est muni de plusieurs génératrices sur place permettant de pallier une panne de courant de plusieurs jours. Veillez à ce que le fournisseur soit relié à l'Internet par l'intermédiaire de plusieurs entreprises de télécommunications, de manière à diversifier ses voies de communication.

3 Le fournisseur offre-t-il de solides accords sur les niveaux de services, et son personnel possède-t-il de solides qualifications dûment attestées ? Bien que l'alimentation électrique et la bande passante constituent l'essentiel, vous devez également prendre le temps d'examiner attentivement les politiques et les ressources humaines sur lesquelles le fournisseur s'appuiera pour protéger votre entreprise contre toute attaque ou toute interruption importante de vos activités.

Prenez connaissance en détail des accords sur les niveaux de service offerts par le fournisseur pour bien comprendre quelles garanties il offre en plus de l'alimentation électrique et de la bande passante. Examinez de près les qualifications du personnel qui serait directement chargé de la mise en œuvre et du soutien de votre système. Demandez au fournisseur de voir les résultats des vérifications de sécurité et de disponibilité réalisées par des tiers.

4 Le fournisseur compte-t-il parmi ses clients des entreprises de votre secteur ? Exigez de parler à des clients du fournisseur pressenti qui, idéalement, seraient des entreprises de votre secteur. Demandez aux clients si les services, l'expertise technique et le degré de professionnalisme sont conformes à ce qui leur avait été promis.

S'il y a un aspect positif aux menaces et désastres, c'est que les cadres supérieurs sont de plus en plus sensibilisés au fait que les systèmes informatiques constituent la pierre angulaire des activités de leurs entreprises et souvent de leurs activités commerciales essentielles. En vue de protéger les actifs et la réputation d'une entreprise, il incombe à la direction, et non uniquement au service informatique, de veiller à ce que l'entreprise se soit dotée bien à l'avance de l'infrastructure, des services et des ressources qui lui éviteront de devoir recourir, au beau milieu d'une crise, des décisions onéreuses risquant de lui nuire.