

PRA : l'assurance vie du SI et de l'entreprise

Il faut voir le système d'information comme l'organe principal d'une organisation. Interconnecté, il est le socle de l'ensemble des logiciels de l'entreprise, de la gestion des ressources humaines au suivi client, achats, ventes et stocks, logistique, comptabilité, en passant par l'ensemble des activités de production... Il collecte, il stocke, il traite, il distribue l'information et rassemble l'ensemble des ressources de l'entreprise. Il représente les technologies de l'entreprise, induit les processus et devient au fil du temps, valeur et modèle économique.

Sa préservation et sa sécurité sont indéniablement liées à la progression de l'entreprise sur son marché. Elles le sont d'autant qu'une part toujours plus importante de l'activité économique se fonde sur la stabilité, la continuité du système d'information. Pourtant, sites e-commerce, applications, traitement de la donnée, temps réel ont surtout concentré l'attention sur la recherche de performance, d'agilité et de scalabilité.

La sécurité en outre est généralement perçue par le prisme des cyberattaques. Sensibilisation, analyse des vulnérabilités, déploiement de technologies de sécurité variées représentent à eux seuls un pan important de la stratégie de sauvegarde d'une entreprise. Mais aucune de ces mesures n'est efficace face à une panne matérielle, une panne logicielle, la défaillance d'une sauvegarde, une erreur humaine, un accident ou une catastrophe naturelle.

Prendre la mesure de la diversité des risques

Les causes d'incidents sur l'infrastructure d'un système d'information sont multiples et leurs conséquences, parfois très lourdes. Dans l'hypothèse grave d'un incendie, les entreprises qui en sont victimes doivent simultanément faire face à des situations touchant aussi bien les hommes, les biens que l'environnement. L'INRS estime que 70 % des entreprises ayant subi un sinistre majeur ne s'en relèvent pas. Avec la disparition brutale du système d'information lors d'un incendie, c'est toute la donnée d'exploitation qui disparaît, l'ensemble de la comptabilité, des registres clients, l'information produits, le suivi des innovations...

Un virus agressif affectant l'ensemble du système peut quant à lui conduire les machines, les serveurs, le réseau et les outils de communication à l'arrêt total. Il peut être déroutant de constater à quelle vitesse une entreprise réduite au silence peut disparaître des radars de ses partenaires et de sa clientèle.

Une boutique en ligne, notamment lors de quelques moments forts de l'année, peut perdre des centaines de milliers d'euros en quelques heures d'interruption de service. D'une façon générale, plus les cycles de vente sont courts, plus les pertes commerciales sont immédiates.

Une erreur humaine peut aussi coûter très cher, ne serait-ce que si l'on s'en tient à la réputation de l'entreprise et à la confiance qu'elle doit impérativement préserver vis-à-vis de sa clientèle. Marketplace, système de paiement en ligne, solution de réservation touristique ne peuvent se permettre ni ralentissement de l'activité ni coupures intempestives.

Le plan de reprise d'activité, quoiqu'il arrive

C'est justement parce qu'il n'existe pas de sécurité parfaite, parce que tout arrive et particulièrement l'inattendu qu'il existe des assurances. Pour l'infrastructure informatique, il s'agit des plans de reprise d'activité, dont l'objectif, on l'aura compris, est de permettre la récupération des données et la réactivation des services perdus au plus vite.

Certes le processus d'établissement d'un PRA, éprouvé et testé, comporte de multiples volets selon les types de sinistres, leur envergure ou la structure de l'organisation impactée.

Mais il répond aussi à de nombreux critères communs à toute entreprise. Il en va des différentes étapes de construction, qu'il s'agisse de l'implication initiale de la Direction générale, de l'identification des besoins et des attentes ou des activités les plus critiques.

Un plan de reprise d'activité informatique s'appuie sur un site de secours, un datacenter et de plus en plus, sur le cloud. Il exige une démarche logique, très documentée pour en assurer la performance le jour où l'entreprise en aura besoin, et ce dans les plus brefs délais. L'établissement d'un PRA est un travail complexe.

Définir les priorités, choisir les équipements de sauvegarde, attribuer les rôles et les tâches, savoir faire évoluer et tester régulièrement son PRA, prendre en compte les contraintes réglementaires, tout cela peut être attribué à un prestataire spécialisé. Dans ce cas, l'entreprise prendra garde de s'assurer de l'existence de garanties, tant du point de vue des niveaux de services que de sa capacité à détecter d'éventuels nouveaux risques et à remettre en cause régulièrement, la fiabilité de l'infrastructure mise en place.