IRON MOUNTAIN®

LE MONDE POST-COVID OU LA NÉCESSAIRE ÉVOLUTION DES PLANS DE CONTINUITÉ DE L'ACTIVITÉ

Peu d'entreprises disposaient de plans de continuité de l'activité (PCA) leur donnant véritablement les moyens d'affronter les perturbations colossales d'une pandémie mondiale. Si beaucoup s'efforcent toujours de s'adapter à la nouvelle réalité, certaines leçons du COVID-19 peuvent d'ores et déjà être intégrées à la réflexion sur les PCA de demain.

De l'avis des experts en gestion de crise, il est crucial, dans le cadre d'une réaction à une situation de catastrophe, de relever sur le vif les défaillances ou les lacunes à combler. Ces éléments étant souvent oubliés une fois la crise passée, il est judicieux de tenir un journal pour inspirer par la suite des améliorations du PCA.

Voici quelques points à envisager.

Préparez-vous à une révolution pour encadrer de gros effectifs à distance. Le passage au télétravail de presque toutes les équipes travaillant dans les bureaux et les centres d'appel a été un tour de force pour les entreprises qui ne fournissaient jusqu'alors des ordinateurs portables qu'à leur seuls collaborateurs itinérants.

Beaucoup ont été contraints de se connecter aux réseaux de leur entreprise depuis des ordinateurs dépourvus de logiciels validés par l'entreprise, d'une protection à jour contre les malware, de contrôles par du chiffrement et de clients de messagerie sécurisés. De plus, le fait de devoir partager ces ordinateurs avec parfois le reste de la famille, enfants compris, n'a fait qu'amplifier les risques pour la sécurité.

Les services informatiques doivent réfléchir à constituer un parc d'ordinateurs portables partagés utilisables en cas d'urgence selon Brendan Carr, Chef des produits Solutions Cloud chez Iron Mountain. Il suggère de relever au moins certains renseignements sur les ordinateurs personnels mis à contribution, notamment leurs adresses MAC et IP uniques. Et pour éviter que les collaborateurs ne saturent le service d'assistance, il faut leur donner des consignes détaillées sur le téléchargement et l'installation des logiciels utiles.

Renforcez la résilience de la messagerie. « Sans messagerie, les activités sont stoppées net », précise Stan Lowe, directeur de la sécurité des systèmes d'information chez Zscaler, un éditeur de solutions de sécurité dans le Cloud, dans un article publié sur CIO.com. Et nous savons tous qu'il a raison. Aujourd'hui, quasiment tous les services de messagerie sont dans le Cloud ou ont une option « webmail » accessible via un navigateur. Il est impératif que les collaborateurs qui n'auraient pas accès à la messagerie approuvée de l'entreprise puissent disposer d'autres moyens d'accès. Par ailleurs, il faut les avertir de ne pas transférer d'emails professionnels à un service consommateurs qui n'aura peut-être pas les ressources de sécurité et d'audit exigées par l'entreprise

Inventoriez les opérations critiques pour l'activité. La pandémie a contraint les entreprises à faire un tri dans leurs opérations pour définir dans la précipitation les fonctions essentielles lorsque l'activité passe en mode ralenti. Il peut s'agir aussi bien d'opérations internes, telles que la maintenance des équipements, les détails de sécurité, les services de conciergerie, le support informatique et les centres de contact, que de fonctions externes comme l'intervention sur site. Faites la liste des fonctions essentielles et des plans pour les exécuter, en n'oubliant pas que certaines situations obligeront peut-être à mettre des collaborateurs en quarantaine sur place, auquel cas il faudra leur fournir des services essentiels de type restauration, suivi sanitaire et hébergement.

Préparez un plan de secours des compétences. Parce qu'elles ont été inondées d'appels à leur centre de contact dans les premières semaines de la crise, nombre d'organisations sanitaires ont été amenées à solliciter du renfort auprès d'autres services. Réfléchissez à la manière dont votre entreprise traiterait une situation qui génère une brusque augmentation de la demande ou qui met des personnes clés hors service. Les services de RH doivent s'intéresser à la création d'une sorte de « guichet d'emplois » interne dressant la liste des compétences de l'ensemble du personnel, ce qui permettra en cas d'urgence d'affecter les bons profils en remplacement des collaborateurs défaillants.

Passez les chaînes logistiques en revue. La pandémie a révélé un cruel travers de la gestion des stocks en mode « juste à temps ». En effet, certains revendeurs et fabricants ont été pris au dépourvu par la fermeture de leurs fournisseurs pour cause de maladie ou sur décision administrative. De l'avis de nombreux experts, les entreprises vont être contraintes de revoir leurs futurs plans de chaîne logistique en privilégiant des mesures de résilience, notamment en ayant des fournisseurs de secours et des stocks plus fournis.

Prévoyez une sauvegarde des données distribuée. Les collaborateurs qui travaillent tous les jours dans un bureau ne s'embarrassent pas de sauvegarder les données puisque le service informatique s'en occupe. Mais lorsqu'ils sont brusquement contraints de travailler depuis chez eux, l'idée qu'il faille protéger les données peut ne même pas les effleurer. Sur les 200 millions d'utilisateurs mensuels d'Office 365, la plupart ne sait probablement pas que la suite bureautique de Microsoft ne propose pas de service de sauvegarde. L'éditeur estime en effet qu'il appartient aux clients de prendre eux-mêmes leurs dispositions.

Depuis deux ans, la sauvegarde est devenue une fonction de plus en plus critique pour l'activité en partie du fait de la flambée des attaques par ransomware qui chiffrent les principaux équipements de stockage et rendent les PC inutilisables. Les services tels que la solution de sauvegarde dans le Cloud de l'offre Carbonite fonctionnent de manière transparente en arrière-plan avec le chiffrement de bout en bout des données via une connexion sécurisée. Grâce au partenariat stratégique entre Iron Mountain et Carbonite, les clients de la plateforme Iron Cloud peuvent facilement intégrer à leur stratégie de protection des données la sauvegarde des équipements d'extrémité de leurs collaborateurs travaillant sur site et à distance.

Organisez un cours intensif de formation à la sécurité. Les attaques par hameçonnage, qui visent à manipuler les utilisateurs pour qu'ils cliquent sur des liens malveillants contenus dans des emails inoffensifs en apparence, ont explosé au cours de l'épidémie de COVID-19 à mesure que les personnes en quête d'informations ont baissé la garde. Ce n'est là que l'un des risques que le virus a créés en matière de cybersécurité. Il y a eu par ailleurs une forte augmentation de l'utilisation de services de partage de fichiers dans le Cloud et d'applications collaboratives qui sont autant de sources de vulnérabilités potentielles s'ils ne sont pas supervisés par le service informatique. Les entreprises doivent mettre en place une liste de contrôle de sécurité pour le télétravail et également fournir aux collaborateurs à distance un accès aux logiciels et services autorisés qui offrent une sécurité suffisante tout en garantissant au service informatique une visibilité sur la disponibilité et l'utilisation.

Repensez l'infrastructure et la bande passante du data center. Nombre d'entreprises ont du mal à faire face aux contraintes inédites qui pèsent sur leurs réseaux et ressources de data center. L'afflux soudain de collaborateurs se connectant via un réseau VPN peut saturer la bande passante et freiner les performances du réseau pour les opérations critiques. Et à l'heure où toujours plus d'entreprises en viennent à vendre davantage de produits en ligne, le ralentissement des performances se répercute directement sur le chiffre d'affaires.

Les entreprises dont l'infrastructure de data center est concentrée dans leurs propres locaux ont par ailleurs eu du mal à maintenir leurs niveaux de service avec des équipes aux rangs éclaircis par la maladie, le confinement ou la distanciation physique. En revanche, celles qui ont déjà délégué de vastes pans de leur infrastructure à des centres de colocation, des fournisseurs de services d'infogérance et à des infrastructures dans le Cloud ont géré la transition avec une relative facilité.

Lorsqu'elles préparent leur stratégie de continuité de l'activité pour demain, les entreprises doivent s'intéresser davantage à la mutualisation de leur propre infrastructure, selon Sander Deutekom, Directeur mondial de l'activité Iron Mountain Data Centers. Les fournisseurs de services « garantissent le bon fonctionnement, la résilience et une capacité d'évolutivité ascendante ou descendante selon les besoins. « Vous pouvez compter sur une disponibilité de 99,9999 %. »

Quant aux fournisseurs de services de mutualisation, ils donnent aussi accès à un large éventail de fournisseurs réseaux pour que leurs clients puissent choisir la meilleure association d'opérateurs en fonction de leurs besoins. Sander Deutekom en profite pour préciser que le data center d'Iron Mountain implanté à Amsterdam fonctionne avec plus de 50 opérateurs. « Parce que nous sommes indépendants d'un quelconque opérateur, nous pouvons vous aider à trouver la solution qui répond le mieux à vos contraintes. »

Chaque crise porte en elle des opportunités. Les entreprises qui retiennent les leçons du COVID-19 en sortiront à la fois plus fortes pour affronter les chocs ultérieurs et plus réfléchies par rapport à leurs propres opérations.