"La disponibilité des données est un prérequis à la réussite économique des entreprises"

Un incendie s'est déclaré dans la nuit du 9 au 10 mars 2021 dans un centre de données d'OVHcloud, provoquant la mise hors ligne de 3,6 millions de sites web depuis cette date. Maddyness revient avec Karl Rigal, directeur marketing du cabinet de conseil en industrie et ingénierie Stedy, sur les mesures que peuvent prendre les entreprises dans le but d'éviter la paralysie suite à un tel incident.

Temps de lecture : minute

---

26 juin 2021

Republication d'un article du 11 mars 2021

Dans la nuit du mardi 9 au mercredi 10 mars 2021, 3,6 millions de sites web – parmi lesquels celui de *Maddyness* – ont été hors ligne selon l'expert de la surveillance des noms de domaines Netcraft, après un incendie survenu dans le centre de données d'OVHcloud à Strasbourg. L'incident, qui serait d'origine accidentelle d'après l'AFP, a de fait paralysé des centaines d'entreprises dont l'activité dépend de la distribution de services en ligne.

Les risques de coupures, qui restent rares, peuvent être réduits en amont par les acteurs économiques. Il s'agit d'anticiper pour se saisir de ces enjeux avant même que la catastrophe ne survienne. *Maddyness* a demandé à Karl Rigal, directeur du marketing du cabinet de conseil en industrie et ingénierie Stedy, les bonnes pratiques en la matière.

Quel risque la perte de données, temporaire ou définitive, représente-t-elle pour une entreprise ?

Karl Rigal : "On ne le dira jamais assez : les données sont l’or noir du 21e siècle. La perte de données constitue dès lors un danger majeur pour les entreprises, qui doivent s’assurer que ce trésor de guerre restera exploitable en toute circonstance. La disponibilité permanente et immédiate de ces informations est même devenue un prérequis : la réussite économique des entreprises y est désormais largement conditionnée. Les divers acteurs doivent considérer ce sujet avec grand intérêt, puisque les événements d’origine accidentelle ou intentionnelle peuvent survenir. L’incident chez OVHcloud est exceptionnel par nature. Les cyberattaques le sont beaucoup moins, en témoignent les récentes mésaventures d’hôpitaux français."

À lire aussi
OVHcloud s'allie avec Google en promettant aux Européens le contrôle des données

Comment une entreprise peut-elle prévenir ce type d’incident ?

K. R. : "Deux options. Le cloud public est une technologie de haute disponibilité. Il permet aux entreprises qui le souhaitent de distribuer leurs données en temps réel sur plusieurs datacenters. Ce partage entre différentes infrastructures limite le risque de perte d’informations, mais il y a un inconvénient : il coûte cher. C’est pourquoi la plupart des entreprises choisissent une manœuvre plus accessible, qui consiste à répliquer les données. Cette procédure, plus abordable, s’inscrit dans un plan de reprise d’activité (PRA). Ce dernier pose, de manière anticipée, un cadre permettant d’agir dans l’urgence pour sécuriser l’ensemble des portes d’entrées aux données exposées. À cette date, seule une minorité d’acteurs en ont établi un. Les petites et moyennes entreprises (PME), notamment, continuent de penser que ce chantier n’est pas prioritaire. Il nous faut encore sensibiliser.

Deux indicateurs sont pris en compte quand il s’agit de mettre un PRA sur pied. Il faut déterminer la quantité maximale de données que l’on risque de perdre. Si une sauvegarde a lieu à intervalles réguliers, il faut savoir que les informations produites dans les 12 heures précédant un incident sont généralement perdues. Dans un second temps, il convient de s’assurer que l’on puisse rendre la copie des données opérationnelle dans un délai réduit. C’est la clé pour permettre une reprise d’activité rapide. En établissant le rapport entre coûts d’investissement et coût d’exposition au risque, mettre un PRA sur mesure en place est possible. Ce dernier sera, d’ailleurs, meilleur s’il est régulièrement mis à l’épreuve avant toute situation d’urgence. Le triptyque gagnant : préparation, déploiement et entretien. Selon les besoins en sous-traitants ainsi qu’en accès aux données, le coût de ce dispositif s’étale entre quelques dizaines de milliers d’euros et plusieurs millions."

Après l’incendie chez OVHcloud, quelles solutions se présentent aux entreprises touchées ?

K. R. : "Il ne faut pas oublier qu’il revient, avant quiconque, au directeur des systèmes d’information de protéger les données de l’entreprise. Il doit orchestrer la copie sur deux serveurs distants physiquement. OVHcloud se contente d’héberger les données dans les conditions demandées par ce professionnel. Ce type d’incident est très rare : l’hébergeur est, pour sa part, tenu de sécuriser les données qu’on lui confie. Si ces dernières devaient être entièrement parties en fumée suite à l’incendie, on peut supposer que les clients se retourneraient contre OVHcloud pour défaut de protection des données. Même chose si les données étaient corrompues, dans le cas où un acteur tiers y aurait eu accès suite à l’incident. La prochaine étape consisterait alors à quantifier la perte de données pour réclamer une réparation appropriée. Au niveau technique, d’anciennes versions seraient éventuellement récupérables... mais l’impact sur le client d’ores et déjà puissant."

À lire aussi

"Le développement de Blade sera axé sur les infrastructures"

Des alternatives, telles que les hébergeurs de proximité, sont-elles viables ?

K. R. : "L’écosystème datacenters est riche. Des solutions dites de proximité existent, en effet. Elles constituent parfois une bonne alternative aux gros acteurs, comme OVHcloud ou Scaleway. Il faut toujours s’assurer que les opérateurs qui les gèrent ont bien les moyens d’assurer l’entretien des infrastructures et la protection des données. Ce n’est pas à la portée de tout le monde. C’est pourquoi il convient de se faire accompagner par des experts, qui évaluent le risque encouru.

Les datacenters vont se multiplier, portés par l’explosion des usages numériques. On estime, par exemple, que le confinement a provoqué une accélération d’une dizaine d’années en la matière en France. Des technologies, telles que l’Internet des objets ou la 5G, participent également de cette tendance. Ces fermes de serveurs sont gourmandes en électricité, ce qui conduit une part des ingénieurs qui arrivent sur le marché de l’emploi à s’en désintéresser. C’est regrettable, tant l’enjeu est majeur : l’usage des données est voué à durer dans le temps. Alors plutôt que de mettre le sujet de côté, il faut s’en saisir pour accompagner son développement… tout en réduisant au maximum l’empreinte environnementale. À mesure que le numérique s’impose comme une priorité, la sécurité va de pair."

Article écrit par Arthur Le Denn