

Celeste : La sécurité d'un datacenter, la sécurité de vos données ou de vos clients

Internet

Posté par : JerryG

Publié le : 15/3/2012 15:00:00

La sécurité d'un datacenter, c'est la sécurité de vos données ou de celles vos clients. Ne vous laissez pas abuser par des praxtextes sécuritaires, souvent marketing d'ailleurs, pour éviter les questions sur les conditions réelles d'exploitation et de maintenance des sites de votre hébergeur, commente **Nicolas Aubert**, président de CELESTE.

Les centres de données sont les usines des temps modernes. Ils hébergent Internet : les sites web, les emails, les données et les photos des particuliers ; mais également les données des entreprises. A l'heure de la centralisation de l'informatique et du Cloud Computing, ils deviennent la clé de voûte de l'économie numérique. Une panne d'un datacenter, et des milliers de personnes peuvent être privées de réseau, de téléphone, d'emails ou de données.

Pour autant, on ne connaît pas bien leur sécurité. Souvent sous praxtexte de confidentialité, certains exploitants de datacenters communiquent peu d'information sur leur architecture thermique, électrique, et sur les pannes rencontrées. Cette communication est plutôt faite par les utilisateurs qui ont souffert d'une interruption de service. Il n'existe pas de norme définissant la sécurité d'un datacenter.



Des critères basés sur l'architecture des datacenters permettent à un organisme privé, l'Uptime institute, de classer les datacenters. Ils sont catégorisés de « Tier I » à « Tier IV ». Toutefois, ces catégories sont souvent utilisées à tort et sans contrôle par les concepteurs de datacenters. De surcroît, elles ne tiennent pas compte des nouvelles configurations des datacenters et des processus d'exploitation.

Afin de connaître la sécurisation de son datacenter, voici quelques questions de base qu'il nous paraît utile de poser à son hébergeur :

La sécurité thermique est souvent l'élément le plus négligé, et il est l'origine de nombreuses pannes. Pour un datacenter de 1 MW de puissance informatique, si le système de refroidissement ne fonctionne plus, c'est 1 MW de chaleur qui s'accumule et

fait monter la salle en température. Comment sont refroidies les machines ? Est-ce par un système de circulation d'eau glacée dans un faux-plancher ? Est-ce de l'eau glacée directement dans les machines ? Est-ce de l'air recyclé et climatisé ? Du refroidissement par l'air ambiant ? Quelles sont les plages de température extérieure pour lesquelles le système est conçu ? Que se passe-t-il en cas de fuite d'eau si l'eau est utilisée ?

Il est nécessaire de contrôler la tolérance aux pannes de ce système de refroidissement. Le réseau est-il doublé ? Les unités de production de froid sont-elles redondées ?

La sécurité électrique doit être examinée depuis la haute tension jusqu'aux serveurs informatiques. De combien de sources électriques haute-tension votre datacenter dispose-t-il ? Les câbles haute-tension sont-ils doublés, sur deux parcours différents ? Un risque d'incendie existe sur les transformateurs haute-tension : sont-ils protégés contre l'incendie ? Sont-ils doublés ? De nombreux datacenters n'ont qu'un seul tableau général basse tension : est-ce le cas du vôtre ? Les salles informatiques sont-elles protégées des micro-coupures électriques ; c'est-à-dire est-ce que les onduleurs sont utilisés en permanence ? Quelles sont les procédures de maintenance et d'entretien des systèmes de stockage d'énergie, comme par exemple les batteries ? Comment les groupes électrogènes sont-ils dimensionnés ? Peuvent-ils secourir tout le datacenter ou uniquement la puissance de l'informatique ? Quelle est la réserve de carburant disponible ?

Au niveau des baies électriques, combien de sources électriques sont distribuées ? S'agit-il de phases différentes de la même voie, ce qui ne représente pas une sécurisation ; ou bien de voies produites par des onduleurs distincts ? Les serveurs informatiques sont-ils branchés sur deux sources distinctes ?

Les réseaux de fibre optique des datacenters doivent également être sécurisés. Combien d'adductions en fibre optique sont présents ? Les chemins de fibre optique sont-ils disjoints de bout en bout : dans la rue et dans le bâtiment ? des points de présence opérateur jusqu'au baies des clients ?

D'autres éléments de sécurité peuvent être examinés : contrôle des accès, vidéosurveillance, détection d'incendie, extinction automatique d'incendie. Un élément capital est aussi la présence de personnel sur le site : agents de sécurité, mais aussi personnel de maintenance, soudeurs de fibre optique, techniciens réseaux et systèmes. Les procédures de mise en production, maintenance, SAV, astreinte doivent être clairement définies et appliquées. Pour avoir des indications sur la qualité de l'exploitation, une visite est utile : le site doit être propre et des cartons vides ne doivent pas se trouver dans les salles. Les portes d'accès aux salles et aux baies doivent être fermées, le câblage bien ordonné et étiqueté. Les salles, baies et locaux techniques doivent être clairement repérés.

On ne peut jamais être certain qu'un incident ne se produira pas dans un datacenter. Cependant il est tout fait indispensable d'être très exigeant vis-à-vis de son hébergeur en termes de sécurité, disponibilité et conditions d'exploitation. La sécurité ne consiste pas à se murer dans des sous-terrains et protéger le secret professionnel. La sécurité est avant tout une question de moyens et de processus mais aussi d'information claire et transparente vis-à-vis de ses clients.

CELESTE est fournisseur d'accès Internet Haut Débit et Haute Disponibilité pour les entreprises partout en France.

Doté d'un datacenter écologique et haute densité et d'un réseau en fibre optique, CELESTE propose une offre 5-play : Internet, réseaux, téléphonie fixe, mobile, et hébergement. Grâce à son positionnement haut de gamme et innovant, les solutions haut débit CELESTE sont

uniques sur le march , comme la fibre optique 1G