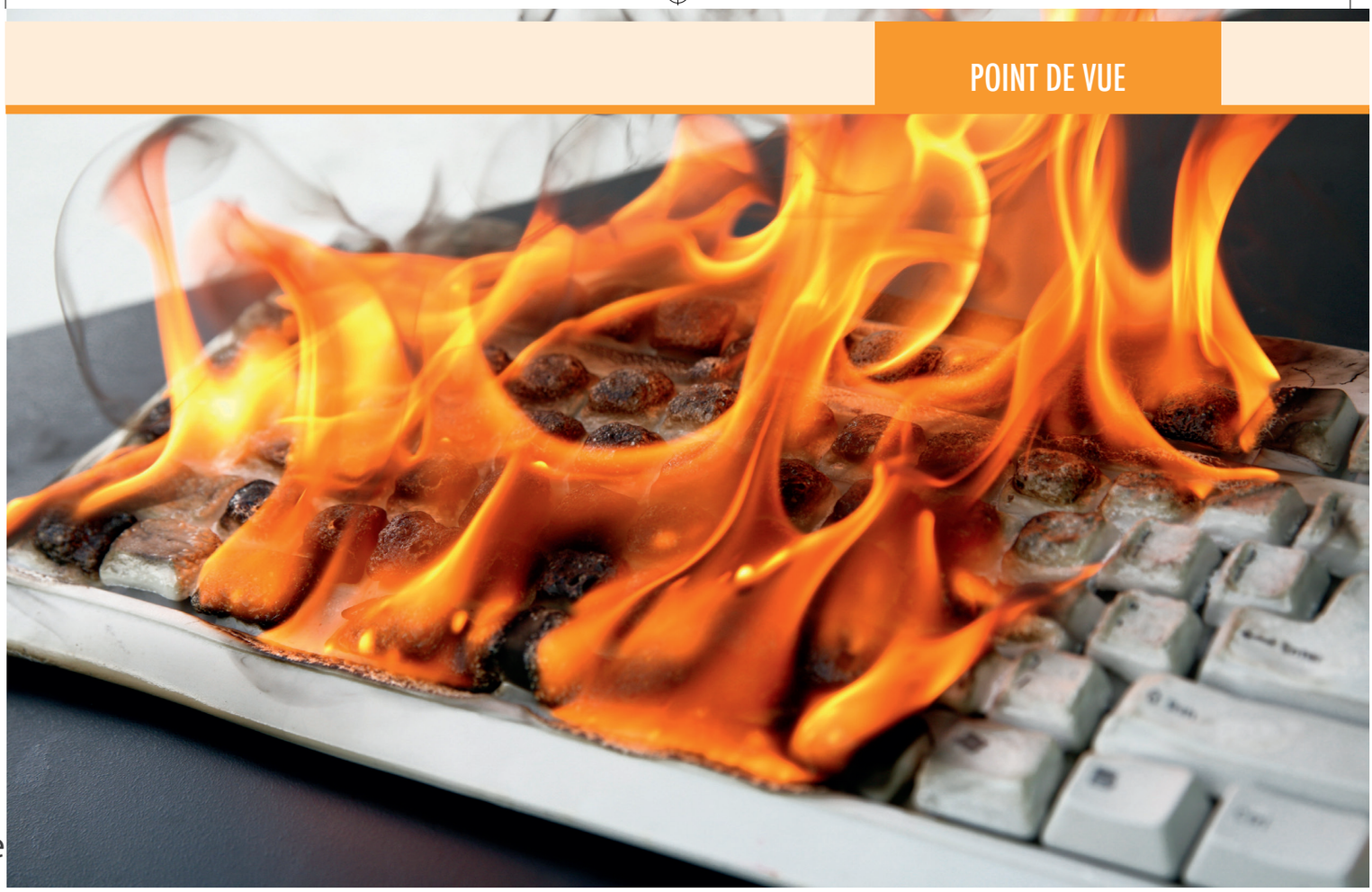

La continuité commence dans le local informatique

Dans la culture 24h/24, 7j/7 actuelle, le maître-mot est la disponibilité. La continuité de l'entreprise dépend à la fois de la disponibilité des installations, de celle des collaborateurs ainsi que des informations. Les responsables informatiques s'efforcent de protéger leurs installations spécifiques contre les risques actuels découlant de la culture du 24h/24, 7j/7. En matière de protection, les responsables informatiques pensent en premier lieu aux mesures techniques au niveau du réseau et du système, mais ils oublient, ce faisant, la protection physique des locaux informatiques.

Ces derniers sont menacés par un dégât des eaux, par l'incendie, l'intrusion, mais aussi par la foudre. Toutefois, les responsables informatiques peuvent faire face à nombre de ces menaces grâce à la prévention et à la détection, et lorsque le mal est fait, à l'aide d'un plan d'urgence approprié. Les pannes peuvent être produites par l'incendie, la fumée, le sabotage, une utilisation incorrecte ou par des personnes non autorisées, par l'effraction, voire par la foudre ou des infiltrations d'eau. Afin de se protéger contre de tels risques, les entreprises se doivent de prendre un certain nombre de mesures. Il est clair que la qualité constante des mesures et exigences appliquées aux locaux informatiques, est d'une importance capitale. Hormis un ou plusieurs locaux informatiques, il y a lieu aussi de protéger les locaux techniques auxiliaires tels que ceux permettant la pénétration de câbles. Ces locaux abritent l'appareillage destiné aux processus auxiliaires. Une panne dans l'un de ces locaux peut avoir des conséquences sérieuses comme la perte d'Internet et de la téléphonie, ou une défaillance des prestations de service.

Le présent article décrit un certain nombre de mesures pouvant endiguer plusieurs risques. Cet article n'est pas exhaustif.

Exigences générales

Les premières exigences que les entreprises doivent appliquer aux locaux informatiques semblent évidentes. Les locaux informatiques ne doivent, de préférence, pas se trouver côté extérieur, au rez-de-chaussée d'un bâtiment. Il est également recommandé que les locaux informatiques ne soient pas implantés au sous-sol ou dans des combles, car ceci augmenterait sensiblement le risque de dégât des eaux. La tuyauterie et les canalisations de chauffage constituent également un risque de dégât par des liquides. En principe, le local ne doit être ni pénétré ni traversé par des liquides, et lorsqu'on ne peut l'éviter, il y a lieu d'installer sous les canalisations un bac de rétention incliné qui, en cas de fuite, évacuerait le liquide hors du local. Les détecteurs de liquide installés au sol peuvent signaler à temps d'éventuelles fuites.

Un local informatique n'est, en principe,

pas équipé de fenêtres. Néanmoins, en cas de présence de fenêtres, celles-ci doivent être équipées de protections supplémentaires antieffraction, d'un film pare-soleil ou éventuellement d'un écran architectonique.
Pour empêcher la panne de certains systèmes, l'accessibilité au local est également importante. Les appareils peuvent, en effet, tomber en panne à tout moment, et les techniciens doivent pouvoir y accéder pour réparation, 24h/24 et 7j/7. Les entreprises doivent empêcher que les techniciens errent à travers le bâtiment pour trouver les locaux informatiques. Pour l'éviter, il faut que ces derniers soient, de préférence, accessibles depuis un local ou une circulation publics et clairement identifiés.
Le but de la protection d'accès est que tous les locaux informatiques et armoires 19 pouces dans lesquels se trouvent des appareils, ne soient accessibles qu'à des personnes devant y effectuer des tâches dans le cadre de leurs fonctions. Cette exigence peut être facilitée par la présence d'un système de contrôle d'accès, ou par des clés matérielles. Le plus important est que la gestion de l'accès soit contrôlable, vérifiable et reproductible. Du point de vue aussi bien technique que sécuritaire, il importe de bien concevoir les locaux informatiques.

Protection architectonique

Par protection architectonique ont entend souvent les ferrures (charnières et serrures). Toutefois, dans le cadre des locaux informatiques, il y a lieu en ce qui concerne la protection architectonique, de vérifier aussi la résistance physique des portes, des fenêtres, des parois, des sols et des plafonds. Un local informatique idéal est, de préférence, un compartiment architectonique offrant suffisamment de résistance à l'effraction et au feu (non pénétration et non propagation). En pratique, on constate que la protection architectonique pose souvent problème, rendant ainsi la protection incendie et la protection anti-intrusion insuffisantes.
Les cloisons sont souvent posées entre le faux plancher et le faux plafond, permettant ainsi à des personnes mal intentionnées, d'enlever une dalle de sol du local informatique et de passer sous la cloison. En cas d'incendie aussi, ce type de construction s'avère funeste et le feu peut, dans ce cas, se propager facilement à un autre local via le plafond ou le sol. Une situation similaire se produit dans le cas d'un faux plafond. Il est donc important que les parois soient bien jointives avec le plancher porteur et avec le plafond porteur.
Les chemins de câbles constituent également un risque pour la sécurité. Le câblage d'un bâtiment doit être de préférence non apparent, faute de quoi il existe un risque de sabotage et de manipulation de câbles. Dans les caves, les greniers et les parkings, le câblage peut cheminer dans des goulottes en acier avec couvercle, qui permettent en outre de prévenir les risques d'incendie. Bien entendu, les traversées de câbles doivent être ignifugées.

En pratique, on constate que la protection architectonique pose souvent problème, rendant ainsi la protection incendie et la protection anti-intrusion insuffisantes.

Infrastructure

Il est d'importance capitale, dans le cadre de la continuité, que les liaisons entre le local informatique et le monde extérieur soient fiables. De ce point de vue, il est préférable de relier le local informatique vers l'extérieur, suivant plusieurs trajets. Ceci peut être fait, par exemple, en tirant des liaisons vers l'infrastructure publique, depuis différents locaux informatiques, ces liaisons quittant de préférence le bâtiment en des endroits différents. On utilisera de préférence l'infrastructure publique de différents pourvoyeurs d'accès.
Lorsqu'une entreprise possède plusieurs établissements, il peut être judicieux de ne prévoir qu'une seule liaison vers une infrastructure publique, et de relier entre eux les établissements. Les exigences en matière d'infrastructure doivent être fixées le plus rapidement possible, d'autant plus que le processus d'obtention de permis d'excavation peut s'avérer, dans de nombreux cas, une œuvre de longue haleine. Le grand avantage est qu'actuellement, on utilise au bureau très souvent le téléphone portable et que de nombreux ordinateurs portables sont équipés d'une réception Internet en Wifi. Du point de vue de la continuité, nous sommes devenus moins dépendants des infrastructures fixes de télécommunications et d'Internet, dans les bâtiments et autour.

Infrastructure électrique

L'informatique ne peut pas fonctionner sans électricité. Dans le cadre des locaux informatiques et de la continuité, il importe d'y réfléchir. Les entreprises sont sujettes en moyenne 10 fois par an à une panne informatique. La durée moyenne nécessaire pour être à nouveau opérationnel est de 4 heures. Le temps nécessaire pour rendre un réseau à nouveau opérationnel peut s'élever à 48 heures.

L'entreprise doit se demander combien de temps l'environnement informatique doit rester actif en cas de panne du réseau électrique. Quelles sont les mesures prises ? Disposez-vous d'une ASI (alimentation sans interruption) ou d'un groupe électrogène de secours ? Ou des deux ? Si oui, faites-vous de temps à autre un essai ? Et si vous avez installé un groupe électrogène, avez-vous passé des accords avec un fournisseur de carburant ? Pouvez-vous le faire venir également le dimanche et les jours fériés ? Bref, quelques questions en rapport avec un groupe électrogène.
Souvent l'ASI et le groupe électrogène sont comparés en termes d'investissement et non en termes de fonctionnement d'entreprise.

En outre, se pose la question, dans le cadre des locaux informatiques, s'il y a lieu de prévoir une protection contre la foudre. En cas de coup de foudre direct, il peut se produire une surtension ou une tension induite dans le local informatique, via les câbles de données, l'alimentation électrique, les canalisations d'eau, les armatures de la construction en béton, etc., pouvant entraîner des dommages aux appareils. Il est recommandé de faire équiper la totalité du local d'une protection contre les surtensions et les tensions induites.

Protection incendie

Pour pouvoir détecter à temps un incendie, les bâtiments et les locaux sont équipés d'installations de détection incendie. La signalisation d'incendie est envoyée à la centrale d'alarme ou aux centraux de surveillance, lesquels avertissent à leur tour les pompiers.

Dans les locaux informatiques, il peut s'avérer problématique de détecter rapidement la fumée d'un début d'incendie (encore appelé feu couvant). Ceci est dû, entre autres, aux flux d'air des climatiseurs. La climatisation provoque une accélération de l'air ; raison pour laquelle les détecteurs de fumée ne fonctionnent pas bien voire pas du tout. Il est néanmoins d'importance cruciale de détecter rapidement un incendie et d'avertir le personnel. L'une des raisons principales est le coût élevé résultant d'un incendie dans les locaux informatiques.

Les systèmes de détection par aspiration sont en mesure de détecter rapidement un feu couvant. Une détection par aspiration est un système d'aspiration de fumée qui prélève des échantillons de l'air afin de déterminer la présence de fumée. Les échantillons d'air sont aspirés à l'aide d'une pompe, via un réseau de canalisations installé dans le local informatique. Cette aspiration a lieu depuis les différents points de prélèvement. Une fois dans le système de détection, les échantillons d'air aspirés sont d'abord filtrés pour éliminer les poussières et autre pollution. Les échantillons sont ensuite amenés dans une chambre de détection où une source lumineuse permet de vérifier la présence de fumée dans l'air. Cette vérification se fait par la mesure de l'obscurcissement de la lumière. Les valeurs de ce dernier peuvent se situer entre 0,005 et 20 %. La mesure étant réglable, ceci entraîne une grande précision du détecteur. Les résultats des mesures s'affichent sur un panneau de contrôle ou sont transmis, via une interface, à un système d'alarme incendie permettant ensuite de déclencher un signal d'évacuation et de piloter une installation d'extinction.

Installations d'extinction au gaz

Les installations d'extinction au gaz sont utilisées pour éteindre des incendies dans des locaux informatiques comportant des appareils coûteux où des installations d'extinction polluantes sont inadmissibles. Ceci veut dire que lorsqu'il naît un incendie, du gaz est insufflé dans le local, ce qui prive le feu d'oxygène et l'empêche de s'étendre, et provoque même son extinction. Du fait de l'utilisation de ce gaz d'extinction, il est indispensable d'évacuer les locaux, juste avant l'insufflation.

Installations de sprinklers

Cela semble bizarre mais depuis un certain nombre d'années, il est possible d'équiper les locaux informatiques d'installations de sprinklers. Dans le cadre de la réglementation environnementale, des accords spéciaux ont été pris entre les autorités d'une part, et les assureurs d'autre part. Les locaux informatiques utilisent alors l'eau comme moyen d'extinction, ce qui, outre le dégât des eaux, entraîne aussi des dommages résiduels. Les entreprises utilisant une installation de sprinklers dans un local informatique, ont besoin d'une assurance spéciale. L'eau servant de moyen d'extinction, ceci entraîne des risques supplémentaires liés aux installations électriques typiques de cette sorte de locaux. Ceci nécessite des procédures spécifiques.

Brouillard d'eau

Ces dernières années, on utilise du brouillard d'eau sous haute pression en lieu et place des installations de sprinklers, dans les locaux informatiques. Le brouillard d'eau étant un très mauvais conducteur et n'étant pas corrosif, on peut l'utiliser en toute sécurité en présence d'appareillages électriques, et il peut donc être utilisé dans les locaux informatiques. En utilisant du brouillard d'eau, il n'y a pas de risque de choc thermique au niveau de l'appareillage électronique. Ceci représente un gros avantage par rapport au CO2. Il y a lieu de mentionner que le brouillard d'eau ne laisse pas de particules ni de résidus huileux, pouvant endommager les appareils électroniques, les ordinateurs, les logiciels, les fichiers de données et autres appareillages de communication.

Conclusion

Comme mentionné dans l'introduction, cet article est loin d'être exhaustif. Il est clair que les locaux informatiques jouent un rôle crucial dans la continuité des prestations de service informatiques. Hélas, les sujets abordés ne le sont pas toujours suffisamment, ce qui fait que la continuité des prestations de service informatiques est soumise à des pressions particulières, alors même que le local informatique constitue le fondement de la prestation de service informatique 7j/7, 24h/24.

(Par Ronald Eygendaal)