Documentation Méthodes de sécurisation des données dans un local

Sécurité des données ?

Aujourd'hui nous sommes dans un monde où énormément de données sont stockées et cette quantité augmente de façon exponentielle. On appelle le principe de stocker énormément de données le Big Data. Il y a un enjeu majeur sur ces données, la sécurité. Il est primordial de répondre aux problèmes de sécurité concernant 3 critères, la disponibilité, l'intégrité et la confidentialité.

Sécurité physique

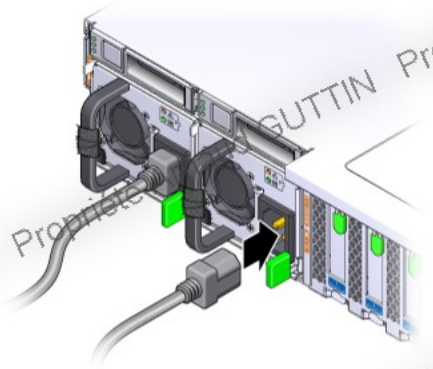
Lors de la sécurisation des données, il est nécessaire de protéger les données de façon physique, de protéger l'environnement dans lequel elles sont stockées. Lorsque nous mettons en place une sécurité physique, nous répondons principalement aux critères de sécurité sur la disponibilité.

Sécurité électrique

Les principaux problèmes physiques portant atteinte aux données sont électriques, il est donc important de mettre plusieurs systèmes de sécurisation en place.

Redondance alimentation

Dans un local technique il est important de mettre en place une redondance électrique sur les serveurs hébergeant les données, cela permet de répondre au critère de disponibilité et permet à tous les utilisateurs de pouvoir exploiter leur données en permanence.



Le principe est de placer une deuxième (ou plus) alimentation électrique, en cas de panne de l'une d'elle, l'autre peut prendre le relais. De plus, Il est également recommandé de brancher les deux alimentations sur des panneaux de brassage électrique différents afin de réduire les risques de panne simultanée.

Système anti-coupure de courant

Les problèmes de coupure de courant sont assez fréquents, il est primordial d'apporter une solution, pour conserver une disponibilité totale mais aussi de ne pas porter atteinte aux appareils électriques.
Pour ce faire, il est nécessaire de mettre en place un onduleur ou un groupe électrogène.

Un onduleur est une batterie permettant d'alimenter les serveurs durant la coupure de courant, si la coupure est trop longue il peut aussi donner l'ordre au serveur de s'éteindre proprement pour éviter les dégâts logiciels. Il permet également de réguler et stabiliser le courant électrique, (Sécurité surtension, sous-tension, court circuit).

Un groupe électrogène est un moteur thermique permettant d'alimenter les machines d'un local technique sur une longue durée de coupure.

Lorsqu'on utilise plusieurs alimentations sur un serveur, switch..., il faut brancher une alimentation sur l'onduleur et l'autre directement sur secteur, cela permet en cas de panne de l'onduleur de quand même pouvoir fonctionner.

Système anti-surtension, sous-tension, court circuit

Lorsque les appareils sont alimentés dans un local, il est possible que le courant est des irrégularité et donc des surtension ou sous-tension, ces irrégularités ont un impact sur la durée de vie des alimentations et des machines hébergeant les données.
Il est donc possible d'utiliser un onduleur, il permet aussi de réguler le courants pour éviter les surtensions et sous-tensions.
En cas de mauvais branchement ou de fusion de câbles, le phénomène de court-circuit peut se produire dans un local technique. Il est donc nécessaire d'installer des disjoncteurs sur chaque panneau d'alimentation dans les armoires. Ces disjoncteurs vont couper le courants lorsqu'un incident aura lieu et donc éviter les risques d'incendie ou dégât plus important sur le matériel hébergeant les données.

Système de redondance de ligne internet

Mettre en place une redondance de ligne internet va permettre que les données soit disponible de l'extérieur mais aussi, pouvoir continuer les sauvegardes externes en cas de défaillance d'une ligne internet.

Il est conseillé de placer les deux (ou plusieurs) arrivées de ligne à des endroits différents du site pour enfin rejoindre le local, cela permet en cas d'accident de rupture de ligne, d'avoir une redondance.

Catastrophe naturel

Les phénomènes de catastrophe naturelle peuvent survenir à tout moment dans un local technique, il faut donc mettre en place différents systèmes pour conserver la sécurité des données.

Sécurité anti-incendie

Le risque d'incendie est élevé dans un local où des dizaines d'appareils fonctionnent en même temps et consomment beaucoup d'énergie. Il faut donc mettre en place des systèmes anti incendie afin de garantir la conservation et la disponibilité de nos données.

Il est possible de mettre en place un système d'extinction par aspiration d'air. C'est-à-dire, lorsqu'un incendie est détecté dans le local, la salle va se mettre sous vide grâce à des pompes, l'incendie va donc s'éteindre étant donné qu'il n'a plus de comburant.

Il est possible de mettre en place un système de gazéification de la salle en CO_2. Lorsque l'incendie est détecté, les bouteilles de gaz de CO_2 vont remplir la pièce, étant donné que le feu ne peut survivre qu'en présence de CO_2, il s'éteindra automatiquement.

Sécurité anti-inondation

Le risque d'inondation causé par une catastrophe naturelle ou par un problème est possible. Il est donc important de mettre en place des systèmes anti-inondation.

Il est conseillé de placer les locaux techniques aux étages supérieurs et non au rez-de chaussée ou au sous-sols.

Il est aussi possible de mettre en place un système d'irrigation de l'eau dans les locaux techniques pour que l'eau puisse s'évacuer le plus rapidement possible.

Sécurité thermique et hygrométrique

Les machines hébergeant les données ont besoin d'être dans de bonnes conditions, thermique et hygrométrique pour pouvoir fonctionner correctement et améliorer la durée de vie. La température idéale dans un local hébergeant des serveurs est entre 18° et 25° et pour l'hygrométrie entre 40% et 60% d'humidité.

Afin de respecter ces conditions, il faut mettre en place un système de VMC permettant de réguler l'hygrométrie du local. Il est aussi important de pouvoir refroidir le local car les machines et serveurs produisent beaucoup d'énergie thermique, l'utilisation d'une climatisation et d'une redondance de celle-ci est indispensable.
De plus, il est fortement recommandé de mettre en place un système de contrôle et d'alerte en cas de mauvaises conditions thermiques ou hygrométriques.

Cluster de locaux techniques

Si les différentes mesures de sécurité sont prises pour éviter les problèmes énoncés précédemment, il est tout de même possible d'en rencontrer.
Il est donc important de réaliser un cluster de locaux techniques, c'est-à-dire de doubler une salle informatique, cela permettra une redondance de cette salle en cas de problème de l'une d'elle. La disponibilité et l'intégrité des données pourront être maintenues grâce à ce système de redondance.

Sécurité anti-intrusions

Des personnes mal intentionnées peuvent vouloir s'introduire dans les locaux techniques pour porter atteinte aux machines (destruction, vol…) mais aussi aux données, il pourra alors altérer la disponibilité, l'intégrité et aussi voler celle-ci.

Il est donc important de mettre en place plusieurs systèmes de sécurité intrusion.
Les systèmes les plus conseillés sont la mise en place de caméras de vidéo-surveillance, d'alarme de présence et de verrouillage des armoires.
Il est important de sécuriser l'entrée dans les locaux grâce à une serrure à empreinte digitale, (un badge est volable et falsifiable).

Une solution pour contrer les vols de matériels, qui pourraient porter atteintes aux données est d'utiliser l'encoche de sécurité Kensington.
Ces encoches sont présentes sur pas mal de matériels informatiques dont certains serveurs, switchs, onduleurs…

Sécurité logiciel

Il est important de sécuriser les données de façon logiciel, en contrôlant des accès aux données et donc pouvoir les rendre confidentielles.

Sécurité de sauvegarde

Afin de sécuriser les données de façon durable, il est nécessaire de mettre en place un système de sauvegarde journalière. La quantité et la récurrence des sauvegardes doivent être réalisées en fonction de l'importance des données, et de la quantité de données qu'on peut se permettre de perdre.

RAID

Le principe de RAID consiste à séparer les données sur différents disques dur matériel. Ce système permet une meilleure performance, et aussi une meilleure sécurité des données.

Il existe différents RAID, définissant les caractéristiques de sécurité et de redondance pour les disques hébergeant les données.

Le RAID 0 ne permet de répondre à aucune redondance, il relie juste plusieurs disques en un seul. En cas de panne de l'un, la totalité des données sur les disques sont inutilisables.

Le RAID 1 est du mirroring, il est utilisé pour les petites infrastructures, il dédouble les données bits à bits sur chacun des disques.

Il existe d'autres structures de RAID comme le RAID 5, RAID 6, RAID 50…, il faudra choisir le RAID correspondant à l'importance des données et combien peut- on perdre de disques matériel avant de perdre la totalité des données.

Sauvegarde cloud

La sauvegarde cloud peut être un atout pour la conservation des données, il est possible de stocker vos données directement dans des datas centers hors site, ou réaliser des sauvegardes externes et conserver l'hébergement de vos données sur site.

Sauvegarde autre site

Si l'entreprise dispose de plusieurs sites, il est possible de sauvegarder les données hébergées dans les locaux dans d'autres. Il est aussi possible de solliciter des entreprises externes pouvant héberger les données chez eux.

Mise en place d'envoie de mail en cas d'alerte

En cas de défaillance d'une sauvegarde ou d'un disque dur ou autre, il est important de mettre en place un système d'alerte par mail ou notification en utilisant par exemple le protocole SNMP ou Syslog. Ce sont deux protocoles permettant de transmettre l'état d'une machine sur un réseau.

Système d'archivage

La mise en place d'un système d'archivage est nécessaire afin de trier les données qui doivent être conservées plus longtemps que d'autres. Ce système apporte une sécurité en plus et prévient des suppressions accidentelles des fichiers où on s'en est rendu compte quand il n'y avait plus de sauvegarde.

Sécurité confidentialité

Chiffrement des données

Afin de conserver la confidentialité de vos données il est important de chiffrer les données à la fois au repos et en transit. Il existe plusieurs algorithmes de chiffrement, les principaux sont AES et RSA.

Si les données sont stockées dans une base de données, le système de gestion de bases de données propose le chiffrement des données. Si elles sont stockées sur des serveurs NTFS ou FTP il est aussi possible de les chiffrer.

Lors du transit des fichiers, il est important d'utiliser un protocole de communication chiffré, comme le protocole HTTPS utilisant TLS/SSL, il existe aussi le protocole SSH, utilisé par le protocole FTPS.

Sécurisation par pare-feu et proxy

Il n'existe pas uniquement de l'intrusion physique mais aussi de façon logiciel, sans se déplacer directement dans les locaux. Il faut donc mettre en place un système de pare-feu et de proxy.

Le pare-feu permet de filtrer toutes les communications entrant et sortant en autorisant ou non les adresses IP à entrer sur le réseau.

Le proxy permet de filtrer ces paquets mais a la couche logiciel, ce qui permet d'avoir un filtrage plus précis.

L'utilisation de ces deux systèmes est fortement conseillée pour sécuriser les données et conserver la confidentialité, l'intégrité et la disponibilité des données.