Sécuriser les données numériques dans un local technique

Tamara Crétard - 07.05.2025

Sommaire:

1. Introduction

Aujourd'hui, les systèmes informatiques ont une place fondamentale tant dans notre quotidien que dans les entreprises. Ne pas se questionner sur la protection des données numériques est donc impensable. Au sein d'une société, le local technique occupe une place centrale. En effet, on y retrouve tous les équipements nécessaires au fonctionnement de l'entreprise, tels que les serveurs, les dispositifs de stockage, le matériel réseau ou encore les systèmes de sécurité.

Afin d'assurer la fiabilité et la sécurité de ces données et donc garantir leur confidentialité, intégrité et disponibilité, il est essentiel de mettre en place une sécurisation adaptée de ce local.

Dans ce document, nous verrons donc les différentes infrastructures matérielles et informatiques à prévoir pour bien sécuriser un local technique, sans oublier les aspects organisationnels importants, tels que l'externalisation de certains services ou la mise en place de solutions pour assurer la haute disponibilité.

2. Local technique

Un local technique est une salle dédiée regroupant les équipements tels que les serveurs, baies de stockage, commutateurs réseau, pare-feux… Son rôle est d'héberger et de protéger ces équipements afin de garantir la confidentialité, l'intégrité et la disponibilité des données.

3. Serveurs

Au sein d'un local technique, on peut trouver des serveurs. Les serveurs sont des ordinateurs nettement plus puissants que nos ordinateurs habituels. Ils sont capables de traiter des charges de travail plus importantes, car les composants sont souvent doublés (redondance). Les serveurs peuvent exécuter des services ou rôles tels que DNS, DHCP ou Active Directory. Lorsque plusieurs serveurs fonctionnent ensemble et qu'ils se substituent on appelle cela un cluster ou une grappe**.**

Les serveurs dégagent énormément de chaleur. Paradoxalement, en plus d'être sensibles à la poussière, ils le sont également à la chaleur.

Il existe plusieurs types de serveurs en fonction des besoins.

3.1. Serveur Tour

Les serveurs tour sont adaptés aux petites entreprises car ils ne nécessitent pas d'infrastructure particulière (climatisation…) et leur installation est facile.

3.2. Serveur en rack

Les serveurs en rack, eux, sont à plat et contiennent les mêmes éléments qu'un serveur tour. Ils sont faits pour être rangés dans des armoires, si possible dans des salles dédiées telles que les locaux techniques.

Afin d'assurer un fonctionnement stable des équipements en cas de panne de courant, on ajoute un onduleur en plus de l'alimentation du serveur.

La largeur des serveurs en rack est standard mais la hauteur varie avec un format minimal de 1U soit 4.4 cm.

3.3. Serveur lame ou Blade server

Pour les serveurs lames, nous avons un châssis et les serveurs y sont encastrés. Il est possible d'y placer une vingtaine dans un espace réduit, ce qui les rend plus économe en place que les serveurs en rack. Également, les lames, à puissance équivalente coûtent moins cher car elles ne nécessitent pas d'alimentation, de connexions… car cela est géré par le châssis. Enfin, les lames peuvent être ajoutées à chaud, et il est donc possible d'augmenter la puissance du serveur sans rien arrêter.

3.4. NAS

Le NAS est un serveur dédié à la sauvegarde qui se branche directement sur un switch, sur le réseau. Synology est la marque la plus aboutie. Pour l'utiliser, il suffit d'insérer des disques à l'intérieur et de le brancher sur le secteur, en plus du réseau. Les disques sont connectés en RAID, c'est-à-dire que la copie d'un disque se fait sur un autre pour plus de sécurité.

4. Baies et disques

Les serveurs fournissant uniquement de la puissance de calcul (une centaine de Go en RAM), il est nécessaire d'utiliser des systèmes de stockage pour les données. Dans les locaux techniques, les données sont stockées dans des baies disques.

Ces baies de stockage peuvent être de différents types selon les besoins et la taille de l'entreprise :

- Baies SAN (Storage Area Network) : Ces baies haut de gamme sont connectées directement aux serveurs via un réseau dédié à haute vitesse. Elles offrent de très bonnes performances et une grande capacité, mais représentent un investissement conséquent.
- Baies DAS (Direct Attached Storage) : Ces baies sont directement connectées aux serveurs. Elles sont plus simples à mettre en œuvre que les SAN, mais offrent moins de flexibilité.

Dans les baies disques, on peut ajouter notamment des :

- Disques durs 3,5" : Ces disques possèdent un bon rapport capacité/prix et peuvent être achetés pour de l'externalisation avec différents prestataires.

- SSD NVMe: Ces disques sont de haute performance. Contrairement aux disques 3.5”, les SSD NVMe utilisent l’interface PCIe, ce qui leur permet d’avoir des vitesses de lecture et d’écriture nettement supérieures. Dans un local technique, ils sont utiles en cas de besoin d’accès très rapide aux données. Tout comme les disques durs 3.5”, ils peuvent être achetés pour de l’externalisation avec différents prestataires. Cependant, leur coût par gigaoctet est plus élevé que celui des disques durs 3,5".

Afin d’assurer une redondance des données pour plus de sécurité, il est nécessaire, comme vu précédemment, de connecter les disques en RAID.

Le choix du système de stockage dépend des besoins spécifiques de l'entreprise en termes de capacité, de performance, de budget et du niveau de sensibilité des données.

5. Sécurisation physique

La sécurisation physique d’un local technique est incontournable pour garantir la protection des équipements et des données. Elle ne se limite pas au contrôle des accès et à la surveillance, il est également important de prendre en compte l’environnement immédiat du local ainsi que sa situation géographique.

5.1. Contrôle d’accès et surveillance

La première étape pour sécuriser un local technique consiste à limiter au maximum les accès physiques. En effet, l’accès au local doit être strictement réservé aux personnes qui en ont réellement l’utilité. Pour cela, plusieurs solutions existent.

Premièrement, il est possible d’installer un lecteur biométrique, qui reconnaît une empreinte digitale ou un visage, afin de s’assurer que seuls les employés autorisés pénètrent à l’intérieur.

Également, pour renforcer la sécurité, la vidéosurveillance est utilisée. Les caméras utilisées sont parfois équipées de vision nocturne et de détection de mouvement, ce qui peut servir à décourager les personnes malveillantes et à garder une trace des incidents.

En outre, certaines entreprises demandent aux salariés de se peser avant l’entrée dans le local, puis à la sortie, afin de vérifier qu’aucun matériel n’a été volé. Cela est mis en place en plus de la fouille des sacs, de l'utilisation de détecteurs de métaux et de la tenue d’inventaires et d’enregistrements précis du matériel entrant/sortant.

De plus, l’utilisation de badges RFID est envisageable : chaque badge est ainsi attribué à un employé et permet de savoir lequel d’entre eux est entré ou sorti, et à quelle heure.

De même, des capteurs de mouvement, de bris de vitre ou d’ouverture de porte peuvent déclencher des alertes instantanément en cas de tentative d’effraction.

Également, certaines entreprises choisissent d’installer des serrures électroniques qui peuvent être contrôlées à distance. Cela permet, par exemple, de bloquer l’accès à tout moment ou de vérifier facilement l’historique des ouvertures.

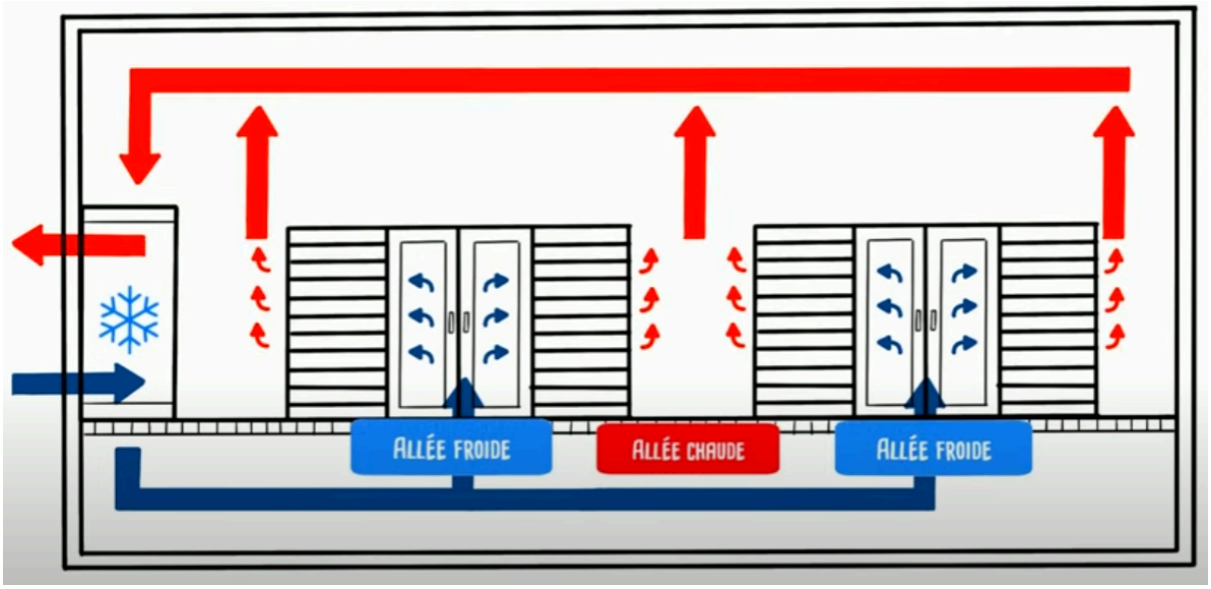
Enfin, dans les locaux où la sécurité doit être maximale, il est même possible d’installer des cages “anti-intrusion” autour des racks pour protéger physiquement les équipements les plus sensibles.

5.2. Sécurité environnementale

Tout d'abord, afin d'assurer la sécurité des équipements informatiques dans un local technique, il ne faut pas seulement empêcher les accès non autorisés. En effet, il faut aussi surveiller l'environnement dans lequel ils fonctionnent. Tout d'abord, il est fondamental de surveiller l'humidité de la pièce : un taux trop élevé risque d'endommager les circuits imprimés par corrosion, tandis qu'un air trop sec peut provoquer de l'électricité statique, dangereuse pour les composants électroniques. Dans l'idéal, l'humidité doit être maintenue aux alentours de 50%.

Ensuite, la température est un autre point clé. Les équipements informatiques, comme vu précédemment, dégagent beaucoup de chaleur, et une surchauffe peut entraîner des pannes importantes. Pour éviter cela, on peut utiliser un refroidissement par eau avec la climatisation. Ces dispositifs permettent de garder la température du local entre 23 et 26 °C, ce qui limite les risques de surchauffe.

Aussi, le refroidissement des équipements peut se faire par air froid. En effet, ce dernier arrive à travers les dalles du faux plancher et passe par les allées froides dans lesquelles se situent les racks qui absorbent l'air froid, puis rejettent l'air chaud à l'arrière dans les allées chaudes. Cet air chaud est ensuite évacué:



Afin de faire des économies, il est aussi possible d'utiliser le "free cooling", c'est-à-dire utiliser le froid extérieur pour aider et optimiser le système de refroidissement et donc réduire les besoins d'énergie.

Également, pour améliorer la circulation de l'air, il n'est pas rare d'installer des ventilateurs industriels et, si possible, un plancher technique surélevé. Ce type de plancher facilite non seulement le passage des câbles, mais permet aussi une ventilation homogène dans tout le local.

De même, il ne faut pas oublier la protection contre les incendies. Des détecteurs de fumée et de gaz sont indispensables : ils doivent être reliés à un système d'extinction

automatique utilisant des gaz inertes (1,1,1,2,3,3,3-Heptafluoropropane ou FK-5-1-12), afin de ne pas abîmer les équipements en cas d'incident. Des extincteurs manuels doivent être présents dans le local, en plus du reste du bâtiment.

De plus, il faut anticiper les coupures de courant. Pour cela, il est nécessaire d'utiliser des onduleurs (UPS) dont le rôle est de prendre immédiatement le relais en cas de panne, ainsi que des groupes électrogènes qui permettent de maintenir une alimentation continue si la coupure se prolonge.

Également, le local technique doit être alimenté par un circuit électrique indépendant du reste du bâtiment, afin d'éviter toute interférence ou surcharge provoquée par d'autres équipements. Il est recommandé d'utiliser des tableaux électriques secondaires dédiés exclusivement à ce local.

Enfin, les serveurs doivent être protégés par des prises sécurisées et des parafoudres. Ces blocs multiprises sont faits pour protéger contre les surtensions, la foudre, les hausses de tension sur le réseau électrique et les décharges électrostatiques.

5.3. Sécurité géographique

Avant même d'installer un local technique, il est important de prendre en compte les risques liés à l'environnement et à la géographie. Le choix de l'emplacement ne doit pas se faire au hasard : il vaut mieux éviter les zones sujettes aux inondations, aux séismes, ou encore aux épisodes de canicule ou de tempête. Si l'entreprise n'a pas d'autre choix que de s'installer dans une région exposée à ce type de dangers, il faudra alors renforcer la structure du bâtiment, prévoir des barrières anti-inondation (batardeaux) et adapter les installations pour mieux résister aux problématiques climatiques.

Dans ces situations, il est aussi essentiel de prévoir un Plan de Continuité d'Activité (PCA) qui tienne compte des risques spécifiques à la zone, afin de pouvoir réagir rapidement et limiter l'impact sur le fonctionnement de l'entreprise en cas d'incident.

6. Infrastructure informatique de sécurité

Pour garantir la sécurité informatique d'un local technique, il est indispensable de s'appuyer à la fois sur une infrastructure réseau solide et protégée, ainsi que sur des solutions de sauvegarde fiables.

6.1. Matériel de réseau sécurisé

Protéger un local technique ne consiste pas seulement à sécuriser physiquement les équipements : il faut également mettre en place une architecture réseau et logicielle adaptée, afin de limiter les risques d'intrusion et de propagation d'attaques.

L'un des éléments centraux de cette protection est le pare-feu, qui joue le rôle de filtre entre le réseau interne de l'entreprise et l'extérieur. Il existe des pare-feux matériels, proposés par des constructeurs comme Cisco, Fortinet ou Palo Alto Networks, mais aussi des solutions logicielles telles que pfSense ou OPNsense. Leur fonction principale est de

contrôler les flux entrants et sortants, en bloquant les connexions non autorisées ou suspectes.

De plus, pour renforcer la sécurité, il est courant de mettre en place une DMZ (zone démilitarisée). Cette dernière est une zone intermédiaire du réseau permettant d'isoler les serveurs accessibles depuis Internet (comme un site web ou une messagerie) du reste du système d'information de l'entreprise. Cela permet de faire en sorte que, même si un serveur de la DMZ est compromis, l'attaquant ne peut pas accéder directement aux données sensibles du réseau interne.

La segmentation du réseau est un autre principe essentiel. Grâce à des commutateurs (switchs) configurés en VLAN, il est possible de séparer les différents services et départements de l'entreprise. Cette séparation permet de limiter la propagation d'une attaque. En effet, si un poste de l'entreprise est infecté, le reste du réseau, dont les données, reste protégé.

Pour ce qui est des serveurs, comme vu dans la partie 3, la sécurité passe aussi par la redondance et la fiabilité du stockage. L'utilisation de disques en RAID permet de continuer à fonctionner même en cas de défaillance d'un disque dur. Les fichiers et données critiques sont généralement centralisés sur des serveurs NAS ou SAN, qui offrent des solutions de sauvegarde automatisée et chiffrée. Le chiffrement des sauvegardes, par exemple avec l'algorithme AES-256, garantit la confidentialité des informations, même en cas de vol ou de perte de support.

Il est également recommandé de surveiller en permanence l'activité réseau, à l'aide de systèmes de détection d'intrusion (IDS/IPS), qui analysent les flux pour repérer tout comportement anormal.

Enfin, la mise à jour régulière des logiciels, des firmwares et des systèmes d'exploitation est indispensable pour corriger les failles de sécurité et limiter les risques d'exploitation de vulnérabilités connues.

6.2. Sauvegardes

En plus de tous les aspects de la sécurité informatique d'une entreprise vus précédemment, la sauvegarde des données occupe une place capitale. Il ne suffit pas seulement de protéger les équipements, il faut aussi anticiper les incidents, que ce soit une panne matérielle, une erreur humaine ou une attaque informatique.

Également, la sécurité des sauvegardes ne doit pas être négligée. En effet, toutes les données stockées, qu'elles soient locales ou externalisées, doivent être chiffrées à l'aide d'algorithmes robustes (comme l'AES-256). Cela permet de préserver la confidentialité des informations, même si un support venait à être perdu ou volé.

De plus, il faut aussi s'assurer régulièrement que les sauvegardes peuvent réellement être restaurées.Pour cela, il faut organiser des tests de restauration, afin de s'assurer que les données peuvent être récupérées rapidement et sans erreur en cas de problème. Cette étape est indispensable pour garantir la fiabilité du dispositif de sauvegarde.

Enfin, pour limiter les risques de perte définitive de données, il est recommandé de suivre la règle du « 3-2-1 ». Cela signifie qu'il faut disposer de trois copies de chaque donnée, sur au moins deux types de supports différents, et qu'au moins une de ces copies doit être conservée hors site (externalisation).

6.2.1. Sauvegarde locale

Les sauvegardes locales peuvent se faire sur différents supports : disque dur externe, bande magnétique ou NAS. Ces solutions permettent une restauration rapide en cas de besoin et peuvent être automatisées grâce à des logiciels spécialisés comme Veeam ou Rsync.

6.2.2. Sauvegarde externalisée

En plus de la sauvegarde locale et pour se protéger contre les incidents majeurs (incendie, vol, inondation…), il est indispensable de prévoir une sauvegarde externalisée.

Aujourd'hui, cela passe souvent par l'utilisation de services cloud sécurisés. Ces plateformes offrent une grande fiabilité et une accessibilité constante, tout en garantissant la conservation des données dans des centres spécialisés (Data Center).

Il existe plusieurs types de services cloud.

6.2.2.1.1. SAAS

Tout d'abord, le SaaS (Software as a Service) propose des logiciels accessibles directement en ligne, sans installation locale. Par exemple, avec Microsoft 365, il suffit d'une connexion Internet pour accéder à ses documents, ses emails ou ses outils de collaboration, ce qui facilite le travail à distance.

6.2.2.1.2. PAAS

Ensuite, le PaaS (Platform as a Service), lui, fournit un environnement de développement déjà configuré. Cela simplifie la mise en place d'applications, car tout ce qui concerne l'infrastructure, la gestion des bases de données ou la sécurité de la plateforme est pris en charge par le fournisseur. Par exemple, Azure App Services permet de déployer rapidement un site web ou une application métier sans avoir à gérer les aspects techniques.

6.2.2.1.3. IAAS

Puis, le modèle IaaS (Infrastructure as a Service) consiste à louer des ressources matérielles à distance, telles que des machines virtuelles. Ce système permet à l'entreprise de gérer le système d'exploitation et les applications installées, tout en se libérant des contraintes d'achat et de maintenance des serveurs physiques. Des plateformes comme AWS S3, Blackbaze B2, OVH VPS ou Microsoft Azure proposent ce type de service, ce qui permet de modifier facilement la puissance de calcul en fonction des besoins réels.

6.2.2.1.4. Hébergement dédié

Il y a également l'hébergement dédié qui consiste à louer un ou plusieurs serveurs physiques spécifiquement réservés à une entreprise, ce qui garantit un contrôle total sur l'environnement et les performances.

6.2.2.1.5. Hébergement mutualisé

A l'inverse de l'hébergement dédié, l'hébergement mutualisé permet à plusieurs clients de partager les ressources d'un même serveur, ce qui réduit les coûts mais limite la personnalisation et peut avoir un impact sur les performances en cas de forte utilisation.

6.2.2.1.6. Infogérance

Enfin, l'infogérance correspond à la prise en charge totale ou partielle, de la gestion de l'infrastructure informatique par un prestataire externe. Cela inclut la maintenance, la supervision, la sécurité, les mises à jour et l'assistance technique 24/7. Un contrat de type SLA (Service Level Agreement) précise les engagements du prestataire, notamment en termes de disponibilité et de temps d'intervention.

6.3. Coûts

Au niveau d'une entreprise, le budget, en plus de la sécurité, est très important. Le questionnement sur le choix de la sauvegarde locale ou externalisée est donc inévitable.

Pour le stockage des données en local, par exemple, un NAS Synology à 4 baies avec disques compris représente un investissement compris entre 600 et 800 euros. Ce type d'équipement est particulièrement adapté pour la centralisation des fichiers.

L'externalisation du stockage dans le cloud est une possibilité intéressante, notamment pour la sauvegarde hors site. Par exemple, la solution Wasabi propose un tarif d'environ 7 euros par téraoctet et par mois, ce qui permet de modifier facilement la capacité en fonction de l'évolution des besoins. Pour l'hébergement de services ou de machines virtuelles, un VPS OVH équipé de 4 vCPU Intel, 16 Go de RAM et 320 Go de stockage en SSD NVMe coûte aux alentours de 45 euros par mois.

Il ne faut pas oublier non plus le coût des logiciels, notamment pour la gestion des sauvegardes. Des solutions professionnelles comme Veeam ou Acronis demandent un budget annuel entre 70 et 500 euros selon les fonctionnalités choisies et le volume de données à protéger.

Voici ci-dessous un tableau récapitulatif des prix (estimations) de différents services cités précédemment:

Solution	Coût indicatif (HT)
NAS Synology 4 baies	600–800 € (matériel)
NAS QNAP 4 baies	700–900 € (matériel)

Cloud Wasabi	7 €/To/mois
Backblaze B2	6 €/To/mois
AWS S3	20–25 €/To/mois
VPS OVH 4 vCPU/16Go RAM/320 Go SSD NVMe	45 €/mois
Veeam (licence annuelle)	300–500 €
Acronis (licence annuelle)	70 €

6.3.1. Avantages et inconvénients

Ces deux types de sauvegardes possèdent des avantages comme des inconvénients, c'est aux entreprises de faire un choix en fonction des besoins.

6.3.1.1. Sauvegarde locale

La sauvegarde locale a l'avantage de garantir un contrôle total sur les données et l'infrastructure. Elle permet de restaurer les données rapidement en cas de problème, sans dépendre d'une connexion Internet ou d'un prestataire externe. De plus, les données restent physiquement sur site, ce qui facilite leur gestion et leur confidentialité.

Cependant, cette solution demande d'investir dans du matériel de stockage fiable et de prévoir un budget pour la maintenance régulière. Il est aussi essentiel de mettre en place des mesures de sécurité physique et logique pour protéger les sauvegardes contre le vol, les sinistres ou les attaques informatiques.

Enfin, il ne faut pas négliger l'importance de stocker au moins une copie de sauvegarde hors site, afin de se prémunir contre les risques majeurs tels qu'un incendie ou une inondation.

6.3.1.2. Sauvegarde externalisée

L'externalisation permet de réduire les coûts liés à l'achat et à la maintenance de matériel. Elle offre également une accessibilité mondiale et une évolutivité rapide.

Cependant, elle suppose une dépendance vis-à-vis du prestataire. Il faut également veiller à la localisation des données pour respecter le RGPD. En effet, les données des citoyens européens doivent rester hébergées dans l'Union européenne ou dans des pays reconnus. Il est donc nécessaire d'exiger des prestataires des certifications reconnues, telles que l'ISO 27001 pour la sécurité de l'information ou HDS pour les données de santé, et de vérifier que l'hébergement des données s'effectue dans l'Union européenne ou dans des pays reconnus.

7. Haute disponibilité, Plan de Reprise et de Continuité d'Activité (PRA/PCA)

Il est essentiel d'aborder la haute disponibilité, ainsi que les Plans de Reprise et de Continuité d'Activité, car ces dispositifs permettent de garantir la continuité des services

informatiques et de limiter l’impact des incidents majeurs sur le fonctionnement de l’entreprise.

7.1. Définitions

La haute disponibilité (HA) permet de garantir un accès continu aux services informatiques, 24 heures/24, 7 jours/7, même en cas de panne. Pour cela, il y a une redondance des équipements et des transferts automatiques sont mis en place en cas d’incident.

Le Plan de Reprise d’Activité (PRA) anticipe une interruption de l'activité et prévoit les conditions de sa reprise.

Le Plan de Continuité d’Activité (PCA), lui, organise la poursuite des activités de l'entreprise en cas d'incident.

Le PRA et le PCA sont complémentaires.

7.2. Mise en œuvre

Afin de garantir la continuité, la haute disponibilité des services informatiques, il est indispensable d’utiliser des solutions qui permettent de limiter au maximum les interruptions, même en cas d’incident. Grâce à la virtualisation, il est possible d’exécuter plusieurs environnements virtuels sur un même serveur physique à l’aide d’outils tels que VMware, Proxmox ou Hyper-V. Ces machines virtuelles peuvent être déplacées d’un serveur à un autre sans perturber les utilisateurs, ce qui offre une grande flexibilité et permet de maintenir les services opérationnels, même en cas de travaux de maintenance ou de panne.

Un autre avantage de la virtualisation est la possibilité de réaliser des instantanés réguliers des machines virtuelles. Ces instantanés permettent de revenir rapidement à un état antérieur si un problème survient, ce qui limite les pertes de données et réduit le temps d’indisponibilité. En plus de cela, la copie en temps réel des données vers un site distant ou un datacenter dans le cloud garantit une restauration rapide de l’activité, même si le site principal devient inutilisable à la suite d’un incident.

La haute disponibilité est également assurée par la mise en place de serveurs redondants, organisés en cluster. Ce système permet un basculement automatique (failover) , c’est-à-dire que si un serveur tombe en panne, un autre prend immédiatement le relais, sans impact pour les utilisateurs. Cette organisation garantit que les services restent accessibles en permanence, ce qui est essentiel pour les entreprises qui ne peuvent pas se permettre la moindre interruption, que ce soit au niveau financier ou au niveau de leur image.

De plus, pour anticiper les situations de crise, il est fondamental de mettre en place un Plan de Reprise d’Activité (PRA) et un Plan de Continuité d’Activité (PCA).

Comme vu précédemment, le PRA définit les étapes à suivre pour relancer les systèmes informatiques après un incident majeur, tandis que le PCA vise à maintenir les services essentiels en fonctionnement durant toute la durée de la crise.

Pour que ces deux plans restent efficaces, il est indispensable de les accompagner d'une maintenance préventive régulière. Cela inclut la vérification des alarmes incendie, le contrôle des onduleurs et des accès, mais aussi la réalisation de tests périodiques des PRA et PCA, idéalement chaque année. Enfin, la formation du personnel aux procédures d'urgence et à la gestion des incidents est importante : tout salarié doit savoir comment réagir rapidement et efficacement en cas de problème.

8. Surveillance et audit de la sécurité

Dans un local technique, la surveillance et la journalisation jouent un rôle essentiel pour garantir la sécurité et la fiabilité des systèmes. Elles permettent non seulement de détecter rapidement les incidents et comportements anormaux, mais aussi d'assurer une traçabilité complète des actions réalisées, ce qui facilite l'analyse et la réaction en cas de problème. Il est donc important de présenter les principaux outils qui rendent possibles ces fonctions.

8.1. Outils de surveillance

La surveillance continue de l'activité du réseau et des serveurs est nécessaire pour garantir la sécurité d'un local technique. Il ne faut pas seulement mettre en place des protections, il faut aussi pouvoir détecter rapidement toute anomalie ou tentative d'intrusion, afin de réagir avant qu'un incident ne prenne de l'ampleur.

Pour cela, il existe plusieurs outils spécialisés. Les solutions de type SIEM (Security Information and Event Management), comme Wazuh ou Splunk, permettent de collecter et d'analyser en temps réel les journaux système et les logs des différents équipements. Grâce à ces plateformes, il est alors possible de repérer des comportements suspects, des connexions inhabituelles ou la répétition d'erreurs, qui peuvent être le signe d'une attaque ou d'un dysfonctionnement.

En plus de cela, il est recommandé d'utiliser des systèmes de détection d'intrusion (IDS) et de prévention d'intrusion (IPS), comme vu précédemment tels que Snort ou Suricata. Ces outils peuvent analyser en profondeur le trafic réseau et sont capables de repérer des tentatives d'accès non autorisées, des scans de ports ou des attaques connues. Ils peuvent également bloquer automatiquement certains types de menaces avant qu'elles n'atteignent les serveurs.

Également, pour renforcer la sécurité des accès, des solutions comme Fail2ban sont très utiles. Ce logiciel permet de surveiller les tentatives de connexion aux serveurs. En effet, en cas d'essais répétés avec des mauvais mots de passe (attaque par force brute), il bloque automatiquement l'adresse IP de l'attaquant, ce qui limite ainsi les risques d'intrusion.

Enfin, l'analyse des logs, associée à des alertes en temps réel, permet de garder une trace de toutes les actions réalisées sur le réseau et les serveurs.Cela facilite non seulement la détection des incidents, mais aussi leur analyse pour comprendre l'origine d'un problème et améliorer les dispositifs de sécurité.

8.2. Journalisation

Afin d'assurer une surveillance efficace et garder une trace de tout ce qu'il se passe sur le réseau et les serveurs, il est important de centraliser les journaux d'activité. Cette centralisation se fait généralement sur un serveur Syslog, qui collecte automatiquement les logs provenant de tous les équipements du local technique. Pour faciliter l'analyse de ces données souvent très volumineuses, des outils comme la suite ELK (Elasticsearch, Logstash, Kibana) sont utilisés. Cette solution permet de visualiser les événements sous forme de graphiques, de rechercher rapidement des incidents précis et d'identifier d'éventuels comportements anormaux.

Également, il est conseillé d'effectuer des audits de sécurité de manière régulière.Ces contrôles peuvent être menés en interne par l'équipe informatique, ou confiés à des prestataires spécialisés pour avoir recours à un regard extérieur. L'idéal est de programmer au moins un audit complet chaque année, afin de vérifier que les dispositifs en place restent efficaces face à l'évolution des menaces.

De même, l'utilisation de scanners de vulnérabilités comme Nessus ou OpenVAS est fortement conseillée. Ces outils parcourent les systèmes et logiciels utilisés dans le local technique, afin de rechercher des failles connues ou des mauvaises configurations. Ils génèrent ensuite des rapports détaillés, qui permettent de corriger rapidement les points faibles identifiés avant qu'ils ne soient exploités par un attaquant.

En regroupant la centralisation des journaux, l'analyse visuelle à l'aide d'outils spécialisés, la conduite régulière d'audits et la détection anticipée des vulnérabilités, on peut significativement renforcer la sécurité du local technique et intervenir rapidement en cas d'incident.

9. Conclusion

Pour conclure, il n'existe donc pas de solution unique pour sécuriser de manière efficace les données dans un local technique. En effet, il est nécessaire de combiner plusieurs méthodes, matérielles et organisationnelles: contrôle strict des accès, surveillance permanente, gestion de l'environnement, duplication du matériel, sauvegardes régulières et externalisation. Il faut également ajouter la formation des utilisateurs et l'audit continu des dispositifs utilisés. Malgré le fait que l'investissement de départ puisse paraître important, il est nécessaire afin d'assurer la durabilité, la stabilité et la réputation de l'entreprise. En conclusion, un local technique bien protégé permet de garantir la confidentialité, l'intégrité et la disponibilité des données, quelles que soient les circonstances. Ainsi, nous avons l'assurance d'une haute disponibilité.

10. Ressources

- https://clusif.fr/wp-content/uploads/2015/10/secphysreseaulocal.pdf
- https://www.cnil.fr/fr/securite-proteger-les-locaux#:~:text=L'acc%C3%A8s%20aux%20locaux%20doit,.%20%3A%20incendie%2C%20inondation).
- https://www.carinel.com/post/securite-locaux-techniques-guide-entreprises
- https://www.naitways.com/nos-guides/guide-cloud/comment-traiter-la-securite-de-linfrastructure-informatique-le-guide-complet/
- https://www.outillageprofessionnel.net/securisation-d-un-local-technique-avec-porte-adaptee/
- https://blockproof.fr/blog/dpo-externe-tarif
- https://www.fibre-pro.fr/infrastructure-numerique-securisee/
- https://www.united-solutions.fr/infrastructure-on-premise/
- https://www.georisques.gouv.fr/
- https://www.maaf.fr/fr/evenements-climatiques/inondation-proteger-locaux-pros
- https://knauf.com/fr-FR/knauf/expertises/protection-incendie/locaux-techniques
- https://www.linkedin.com/pulse/la-s%C3%A9curit%C3%A9-s%C3%BBret%C3%A9-des-locaux-techniques-k5rle/
- https://cloud.google.com/sensitive-data-protection/docs/locations?hl=fr
- https://www.on-x.com/intrusion-physique-comprendre-et-prevenir-les-menaces-contre-la-securite-des-infrastructures/
- https://learn.microsoft.com/fr-fr/azure/security/fundamentals/physical-security
- https://nowteam.net/lexternalisation-de-mes-donnees-pourquoi-et-comment/
- https://neoshore.eu/externalisation/avantages-et-inconvenient/contrats-externalisation/
- https://www.everping.eu/blog/externalisation-informatique
- https://www.tascloudservices.fr/guide/externalisation-de-sauvegarde-pourquoi-confier-la-securite-de-vos-donnees-a-des-experts
- https://www.vizee.io/infrastructure-informatique/
- https://www.cnpp.com/etre-accompagne/datacenters
- https://www.vaadata.com/blog/fr/comment-renforcer-la-securite-de-votre-infrastructure-reseau-pour-contrer-les-attaques-les-plus-courantes/
- https://www.studysmarter.fr/resumes/ingenierie/ingenierie-aerospatiale/infrastructure-de-securite/
- https://fr.wikiversity.org/wiki/R%C3%A9seau_Local/S%C3%A9curit%C3%A9_mat%C3%A9riel
- https://www.dastra.eu/fr/guide/mesure-technique-et-organisationnelle-de-securite--rgpd/367
- https://www.plus-que-pro-solution.fr/en-savoir-plus/securite-informatique/bonnes-pratiques-securiser-acces-physiques-locaux-entreprise/
- https://ads-securite.fr/comment-proteger-vos-locaux-contre-les-intrusions-et-les-incidents/
- https://learn.microsoft.com/fr-fr/microsoft-copilot-studio/geo-data-residency-security
- https://www.adaptaville.fr/batardeaux-barrieres-anti-inondation
- https://www.fortinet.com/fr/products/next-generation-firewall
- https://www.ldlc.pro/reseaux/firewall-hardware/c5633/+fb-C000036938.html
- https://www.acronis.com/fr-fr/products/cyber-protect/purchasing/
- https://www.newr.fr/optimiser-la-temperature-et-l-humidite-d-une-salle-de-serveur/

- https://www.youtube.com/watch?v=LAhhhpuKp_c&list=PLaGzW8ncx-2LyQI6dUl0V7NBKKZJDkJ7T&index=3&ab_channel=Divalto
- https://www.youtube.com/watch?v=HvZWXDdPykE&list=PLaGzW8ncx-2LyQI6dUl0V7NBKKZJDkJ7T&index=4&ab_channel=DataXcentric
- https://www.youtube.com/watch?v=rO6bXt7d2L8&list=PLaGzW8ncx-2LyQI6dUl0V7NBKKZJDkJ7T&index=5&ab_channel=Cookieconnect%C3%A9