CYBERSÉCURITÉ

PROTECTION DE LA SALLE INFORMATIQUE

Comment sécurisé un local technique ?

Définition Local technique : Un local technique désigne toute partie d'un bâtiment destiné à abriter des éléments techniques (serveur, chaudière, climatiseur, commutateur téléphonique, VMC, etc.), mais aussi tout ce qui peut être relativement dangereux (tableau, fils et câbles électriques (fil de terre, électrique) ou qu'il faut modifier avec précaution (téléphonique, de télévision, internet, etc.) ainsi que les vannes et tuyaux (gaz, eau, etc.), les circuits et compteurs de gaz ou des fluides (gaz de ville, air comprimé, eau potable, eau chaude sanitaire, chauffage collectif, etc.) permettant le bon fonctionnement d'une maison ou d'un bâtiment.

Dans ce dossier nous allons nous concentrez sur les locaux technique contenant des données numériques

Quelles que soient les protections que vous mettez en place , ne pas oublier que l’indisponibilité d’un local technique peux provoquer une indisponibilité d’une fonction vitale de l’organisation(ex:site internet , réseau interne,). En conséquence pensez à prévoir une architecture sécurisée du réseau avec des redondances aux points stratégiques et à réserver exclusivement l'usage des locaux techniques aux équipements informatiques ou de télécommunications. L’ensemble des locaux et des éléments du réseau local doivent être sous surveillance avec un contrat de maintenance adaptés aux enjeux (obligation de moyens ou de résultats). Le plan de maintenance peut être impacté par un plan de continuité des opérations.
Il faut bien comprendre l’enjeu : en effet, la salle serveur, ou salle informatique, représente véritablement le cœur d’une entreprise. Aussi, toutes les précautions doivent être prises afin d’éviter tous dommages (numériques mais aussi physiques) qui pourraient mettre en péril l’activité de l’entreprise.

Il faut bien comprendre l’enjeu : en effet, la salle serveur, ou salle informatique, représente véritablement le **cœur** d’une entreprise. Aussi, toutes les précautions doivent être prises afin d’éviter tous dommages (numériques mais aussi physiques) qui pourraient mettre

en péril l’activité de l’entreprise.
Ainsi, la sécurité d’un data center doit être une préoccupation prioritaire et permanente afin de garantir une qualité de service et une sécurisation des données maximale. La sécurité est présente à différents niveaux tels que le contrôle d’accès , la prévention d’incendie, la surveillance etc.

Analyse des risques du réseau local

Les locaux techniques sont des points essentiels du réseau local, sans ça il ne peut pas fonctionner correctement. Ils présentent plusieurs point de vulnérabilité important simplement car il abritent nombre d’appareils sensibles (hubs, routeurs,serveur etc.) et sur lesquels pèsent des menaces importantes (écoute, piratage, vol etc.).
Bien que ces équipements soient souvent regroupés dans une même salle, nous vous conseillons de séparer les différents types de matériel.
Ils sont intégrés dans un ensemble de bâtiments délimités géographiquement répondant à des règles d’organisation particulières et à des contraintes spécifiques en matière de sécurité (accessibilité, usage unique ou compatible, moyens de surveillance, etc.). Dans ce document ne sont traitées que les menaces pesant sur les équipements de réseaux et serveur dans les locaux techniques, bien que ces locaux puissent abriter d’autres équipements. Ces locaux devront être alimentés en énergie électrique sécurisée, et éventuellement équipés d’une climatisation. Les câblages, courants forts et courants faibles, devront respecter les normes NF C 15-100 en vigueur. Au même titre que l’ensemble des éléments d’une entité, certaines menaces pèsent sur ces locaux.

Nous allons vous synthétiser tout les risques qu’un local technique peut présenté ainsi que les solutions pour palier a ces problèmes sous formes de tableau

Risques	**Conséquences**	**Solutions**
Incendies	Indisponibilité des équipements du local. Destruction des équipements. Indisponibilité totale du réseau.	Prévision d'un système de détection de fumé et protection contre l’incendie avec un retour d’alarme vers un poste permanent. Un système d’arroseur automatique en cas de fumée détecter Vérification périodique de l’efficacité des équipements. Affichage des consignes de sécurité en cas d'incendie. Affichage de consignes de sécurité spécifiques. Information et formation aux moyens de secours du personnel amené à travailler dans les locaux

		techniques. Exercices périodiques. Exigence d’"un permis de feu" pour tous les travaux par points chauds dans les sites classés ou les installations soumises à déclaration. Mise en place d’extincteur a dans le local technique.
Inondations	Indisponibilité des équipements du local. Destruction des équipements. Indisponibilité partielle ou totale du réseau.	Installation de système de prévention (sonde hygrométrique) avec remontée d’alarme vers un poste permanent. Installation de système d’évacuation d’eau.
Coupure d’électricité	Indisponibilité et/ou destruction totale ou partielle des équipements. Dysfonctionnement des équipements du local. Perte complète ou partiel des données stockées.	Système permettant la coupure automatique de l’électricité. Analyse du schéma des canalisations. Localisation formalisée des robinets d’arrêts d’urgence. Prévision d'une alimentation de secoure (groupe électrogène) et stabilisée(onduleur). Prévoir schéma de câblage au cas ou.
Erreurs de manipulation.	Indisponibilité des équipements.	Prévision d'un système de repérage des câbles ainsi qu’un schéma du câblage. Prévision de matériel en « roue de secours ». Information et formation du personnel. Mise en place d’un cahier d’intervention. (pour y notez toutes les modifications apporté) Prévision de matériel de secours et

		des éléments nécessaires à la configuration. Backup régulière pour pouvoir rétablir le service en cas d'erreur
Intrusion.	Détérioration physique des équipements et/ou du local. Débranchement ou inversion de câble. Pose de sonde d'écoute. Dysfonctionnement des équipements et/ou du réseau. Vol de matériel	Prévision d'un accès sécurisé (clé,badge, etc.) avec historique des accès et une alarme automatique vers un poste permanent. Prévision d'un système de repérage des câbles ainsi qu'un schéma du câblage. Détection d'ouverture (portes, fenêtres,etc.). Éviter, l'utilisation des locaux techniques partagés

Description des solutions par problème :

Incendie :

- Le minimum obligatoire pour la protections contre les incendie du local technique et le Systèmes de détection et d'alarme incendie ce système est imposé par la norme NBN S 21-100 de plus vous pouvez reliée l'alarme a un poste en permanence

- Extincteurs: La norme NF S 61 900 vous impose de mettre un extincteur lui même normé CE (« Le marquage CE a été créé dans le cadre de l'harmonisation des législations techniques européennes » donc parfaitement fonctionnel) dans une pièce a grand potentiels d’incendie (comme une salle serveur)

- Supervision : La supervisons sert à prévenir l’incendie en super visant la **température*** des machines avec un seuil maximum a ne pas dépassé

***(En utilisant le plugin "check_snmp_temperature)**

- Soufflage automatique : Une mesure coûteuse: l’installation d’un extincteur automatique de gaz qui si une alarme se déclenche rempliela salle entierement de **gaz inerte**(C02, Azote) qui étouffera la flamme. Cela ne peut se faire que si personne d’autre ne travaille dans la pièce, car ce gaz est très dangereux pour la santé.

Inondation :

- protection de l’enveloppe extérieure : Toutes les entrées d’eau sont à sécuriser Toutes les voies de pénétration de l’eau doivent être examinées. L'idéal etant aucune arrivé d'eau a proximité du local technique.
- Installation de sonde hygrométrique(sonde permettant de mesurer l'humidité relative ou absolue se qui permet de prévoir les inondations a moindre mesure) avec remontée d’alarme vers un poste permanent.
- Système d’évacuation d’eau : un système empêche l’eau de stagné a l’intérieur de la salle serveur
- Installation de prise coupe-veille intelligente : configurer ces prises coupe les arrivés de courant liée

a une sonde hygrométrique qui demanderas a la prise de couper le courant si une forte variation d’humidité est ressenti

Intrusion :

- Accessibilité : La salle doit uniquement être accessible par 1 entrée(si petite) maximum 3 (si très grande) et ne doit présenté aucune fenêtre de plus
  L’ouverture de la porte de la salle doit s’effectuer uniquement avec carte magnétique ou d’un équivalent permettant de gérer les autorisations d’accès : seules les personnes habilitées à entrer dans la salle y sont autorisé , ajouter un historique des accès avec l’identité de la personne, la date et l’heure exacte pour que en cas de problème retrouver la personne qui a accédé a la salle serveurs

- Camera : Installer des cameras qui pointe la porte et l’intérieur du local relié a un poste en permanence pour avoir une vu omnisciente sur la salle.

- Verrou : Le bâtiment qui abritent la salle serveur doit évidemment lui aussi être munit d’un système anti intrusion , Chaque baie de serveurs sera elle-même verrouillée physiquement avec une serrure.

- Structure : Renforcement des murs,toit,sol extérieur pour empêché tout accès forcé , Détecteur d’ouverture de la porte
- Prévision d’un système de repérage des câbles ainsi qu’un schéma du câblage au cas ou une personne mal intentionné réussi accédé a la salle serveur et débranche/modifie l’emplacement des câbles pour pouvoir tout remettre en place facilement

Maintenant que vous avez en têtes les principaux problème et leurs solution nous allons vous présentez notre sélections des choses à mettre en place pour que votre local technique soit parfaitement protégé

Commençons par la base l’emplacement géographique du local
Le local ne doit pas être installée a proximité d’arrivée d’eau , le lieu doit contenir aucune ouverture vers l’extérieur pour évité l’ensoleillement et la poussière, La température ambiante doit être plutôt froide pour pouvoir économisé sur le refroidissement , le taux d’humidité doit se situé entre 60 % et 40 % le cas parfait est 50 % (impossible a maintenir sans

installation spécifique) pour maintenir un bon taux d’humidité il vous faudra : un hygromètre qui permet de mesuré le taux d’humidité dans la pièce et une ventilation mécanique contrôlée(VMC) pour pouvoir influer artificiellement le taux d’humidité (si votre taux d’humidité est trop élevée vous pouvez utilisez un déshumidificateur ,

Une fois que nous avons notre emplacement parfait il va falloir contrer les potentiels incendie pour cela il vous faut installer des détecteurs de fumée reliée a un poste en permanence ainsi qu’un extincteur a proximité pour qu’il puissent agir rapidement vous pouvez aussi couplez les détecteur avec des pulvérisateurs d’eau pour qu’il éteigne l’incendie malheureusement ces méthode sont peu coûteuse mais endommage a coup sûr les infrastructures pour minimiser les dommages vous pouvez installer un système coûteux qui se nomme le soufflage automatique un système qui permet de priver le local de co2 en le remplissant d’un gaz quand un incendie est détecté pour empêche le feu de se propager actuellement le plus efficace sur le marché

une fois les risques d’incendie palier passons au risque d’inondation

Pour les risques d’inondation même si votre local est située loin des arrivée d’eau il vous faudra un hygromètre pour pouvoir vous projeter si le taux d’humidité augmente trop vite

Une des erreurs les plus fréquentes est coûteuse l’erreur de manipulation en effet imaginons que nous voulions mettre a jour un logiciel dans le réseau nous effectuons la mise a jour nous redémarrons le réseau et nous nous rendons compte que le logiciel ne fonctionne pas pour diverse raison se logiciel est un outils indispensable pour le travail sans cette outils l’entreprise ne tourne pas sans précaution nous avons privez l’entreprise des ces recettes quotidienne en une mise a jour pour paliers a ça il faut mettre en place un protocole qui oblige

avant d’agir d’établir un plan de retour en en arrière au cas ou sa se passerais mal pour cela ils nous faudra inévitablement faire une back-up en plus des back-up automatique avant de toucher au réseau, pour les modifications plus hardware il faudra maintenir un système de repérage des câbles et un schéma pour que le technicien puissent si retrouver en cas de panne évidemment il vous faudra prévoir du matériel en doublons etc:serveur , Switch,câble etc,

L’intrusion est un risque un peu moins présent physiquement mais bien plus a distance mais ce n’est pas une raison pour la négligé un incontournable a mettre en place une porte verrouillé uniquement ouvrable si vous avez un badge avec historique d’accès pour pouvoir connaître les entrés/sorties du local couplé au carnet des changements vous aurez toutes les informations nécessaire en cas d’intrusion de plus vous pourrez placé des caméras relié a un poste en permanence pour être en total sécurité, Pour les Cyber attaques ils faut impérativement mettre en place un par feux qui bloque tout entrer de données non connu par l’entreprise via des Access Control List (une listes qui permet de filtrer les flux entrant et sortant) précisent, grâce a ce document vous avez tout les éléments pour sécurisé votre local technique.