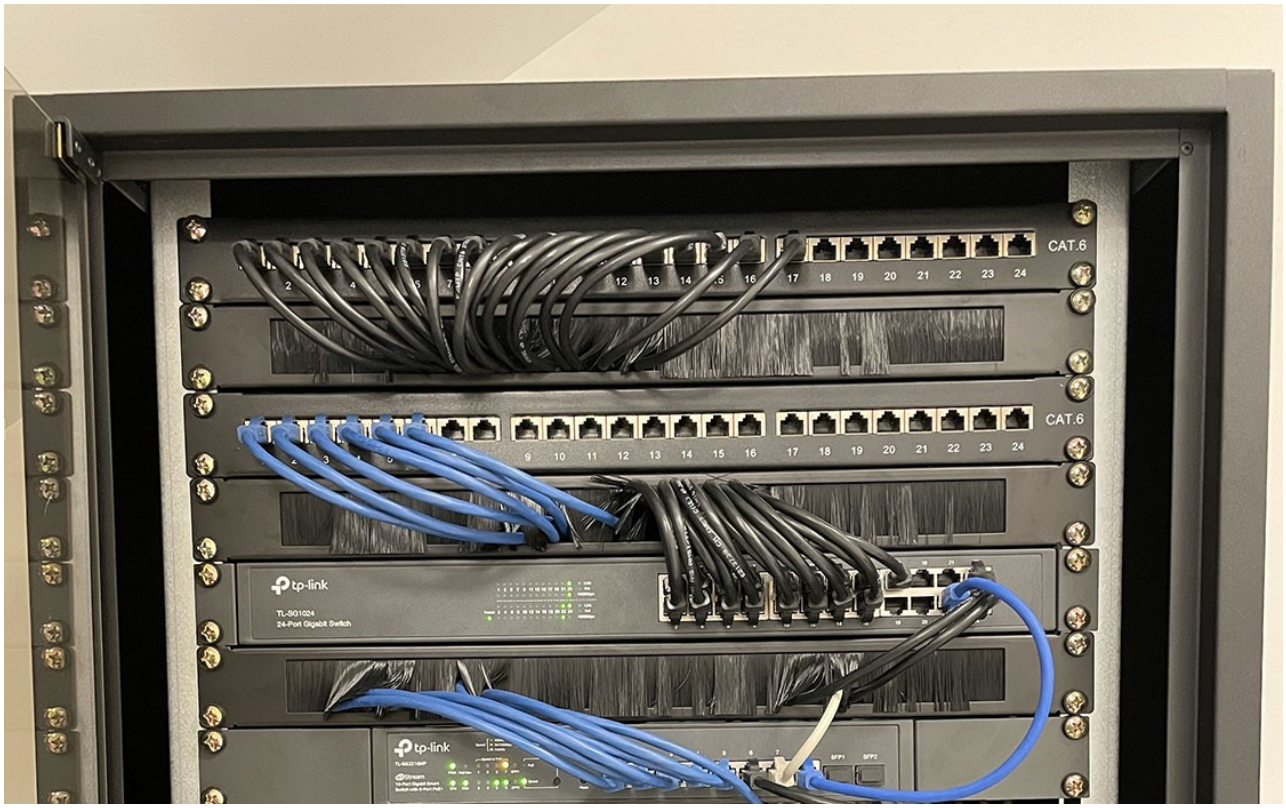
Entreprise : ROBUSTSÉCURITÉ
Version : 1.3

Plan de sécurité réseau pour la Mairie Maison Alfort



Auteur : Houari Chafi, Mohammed Chafi, Ayyoub Belhassen

1.Introduction

La Mairie de Maisons-Alfort souhaite offrir à ses administrés une salle d'exposition ouverte au public tout en garantissant que son réseau interne reste **sécurisé, stable et fiable**. La protection du réseau ne se limite pas aux menaces venant de l'extérieur : les risques peuvent également provenir de l'intérieur, par exemple lorsqu'un équipement non autorisé est branché ou lorsqu'une erreur est commise par un membre du personnel.

Dans ce contexte, la mairie a fait appel à la société **ROBUSTSECURITÉ**, notre entreprise, pour analyser les vulnérabilités du réseau et proposer des solutions permettant de **prévenir les incidents, protéger les informations sensibles et assurer la continuité des services**.

Ce rapport a pour objectif de :

- Identifier les **faiblesses et risques** existants, tant au niveau physique (local, câbles, alimentation) qu'organisationnel (procédures, formation du personnel).
- Proposer des **mesures correctives claires et efficaces** pour sécuriser le réseau.
- Garantir que les services proposés aux administrés puissent fonctionner **sans interruption ni compromis sur la sécurité**.

En suivant ces recommandations, la mairie pourra bénéficier d'un réseau sécurisé et stable, tout en réduisant les risques liés aux intrusions, aux erreurs humaines et aux pannes.

2. Faiblesses physiques

1. Local technique mal sécurisé

Le local où sont stockés les switches et autres équipements réseau n’est pas suffisamment protégé. Un accès trop facile ou mal contrôlé peut permettre à des personnes non autorisées de brancher du matériel, voler des équipements ou même saboter le réseau.

2. Absence de vidéosurveillance

Sans caméra de surveillance, toute intrusion ou manipulation malveillante dans la salle reste invisible. En cas d’incident, il n’y a pas de preuve permettant de retracer les actions de la personne responsable.

3. Pas de contrôle d’alimentation électrique

L’absence d’onduleurs (UPS) ou de protections électriques expose le réseau à des pannes en cas de coupure de courant ou de surtension. Cela pourrait provoquer un arrêt brutal des services disponibles pour le public.

4. Accès insuffisamment restreint pour les visiteurs

La salle d’exposition ouverte au public est proche du local technique. Sans séparation physique ou contrôle strict, les visiteurs pourraient interagir avec le matériel réseau ou les câbles et provoquer des incidents involontaires.

3. Faiblesses organisationnelles

1. **Manque de procédures claires pour l'accès au réseau**

Il n'existe pas de règles formelles sur qui peut se connecter au réseau ou manipuler les équipements. Cela ouvre la porte à des branchements non autorisés et à une absence de traçabilité des actions.

2. **Formation insuffisante du personnel**

Le personnel peut ignorer certaines bonnes pratiques de sécurité, ce qui augmente le risque d'erreurs humaines : mots de passe visibles, câbles mal branchés, manipulations inappropriées, etc.

Cette analyse met en évidence que **la sécurité physique et organisationnelle du réseau actuel présente plusieurs vulnérabilités critiques**, susceptibles d'affecter le fonctionnement du réseau interne et des services offerts au public.

La prochaine étape consiste à proposer des **mesures correctives** concrètes pour réduire ces risques et assurer un fonctionnement sûr et stable du réseau.

4. Mesures correctives – Sécurité physique

Pour réduire les risques identifiés dans la partie précédente, plusieurs mesures correctives peuvent être mises en place afin de sécuriser physiquement le réseau de la Mairie de Maisons-Alfort. Ces mesures visent à protéger le matériel, à limiter l'accès aux personnes autorisées et à garantir la continuité des services.

1. Installation d’un local sécurisé

Le local technique contenant les switches et autres équipements réseau doit être **physiquement protégé** :

- Accès contrôlé par **badge ou clé sécurisée**, réservé uniquement aux administrateurs et techniciens autorisés.
- Les portes et les serrures doivent être robustes et régulièrement vérifiées.
- L’accès des visiteurs et du public doit être strictement interdit, même pour des manipulations mineures.

Bénéfice : réduit fortement le risque de branchements non autorisés, de sabotage ou de vol de matériel.

---

2. Sécurisation des câbles

Les câbles réseau et d’alimentation sont souvent vulnérables aux manipulations accidentelles ou malveillantes. Pour les protéger :

- Utiliser des **câbles blindés** et de qualité industrielle.
- Organiser les câbles dans des chemins et goulottes sécurisées.
- Éviter les câbles exposés ou accessibles aux visiteurs.

Bénéfice : prévient les déconnexions accidentelles, les interférences et les tentatives d’accès physique au réseau.

---

3. Mise en place de vidéosurveillance

La surveillance visuelle du local technique et des zones sensibles permet de détecter toute intrusion ou manipulation suspecte :

- Installer des **caméras dans le local technique et aux entrées principales**.
- Les enregistrements doivent être consultables par le personnel autorisé.

- Les caméras servent également de **preuve en cas d'incident**.

Bénéfice : dissuade les intrusions et facilite l'identification des personnes en cas d'anomalie ou de problème.

---

4. Alimentation sécurisée

Pour éviter les interruptions du réseau ou des services critiques :

- Installer des **onduleurs** pour assurer une alimentation continue en cas de coupure de courant et ainsi assuré un maximum de disponibilité.
- Verrouiller les **multiprises et prises électriques** afin que seules les personnes autorisées puissent manipuler le matériel.
- Vérifier régulièrement les câbles d'alimentation et les protections contre les surtensions.

Bénéfice : assure la continuité du service et protège le matériel contre les dommages électriques.

5. Mesures correctives – Sécurité du réseau (version client)

Après avoir sécurisé le **local et le matériel**, il est essentiel de protéger le réseau **de l'intérieur** pour que tout fonctionne correctement et que seules les personnes autorisées puissent intervenir.

---

1. Protection par mot de passe

Chaque équipement du réseau est protégé par **un mot de passe fort** :

- Seuls les administrateurs autorisés peuvent modifier le réseau.
- Les mots de passe sont invisibles pour les autres utilisateurs.

Bénéfice : personne ne peut modifier ou perturber le réseau sans autorisation.

---

2. Connexion sécurisée pour la configuration

Quand un administrateur doit intervenir sur le réseau depuis son bureau :

- La connexion se fait de manière **complètement sécurisée**, comme si le réseau était un coffre-fort numérique.
- Personne ne peut voir ou intercepter ce qui est envoyé.

Bénéfice : protège les réglages du réseau contre tout accès ou espionnage.

---

3. Sauvegardes régulières

Toutes les configurations du réseau sont **sauvées régulièrement** :

- Si un problème survient, le réseau peut être **remis à l'état normal rapidement**.
- Ces sauvegardes sont vérifiées pour être sûres et à jour.

Bénéfice : réduit le risque d'interruption ou de perte des réglages importants.

---

4. Redondance du réseau et de l'alimentation

Pour éviter toute panne :

- Chaque switch important a un **second switch de secours** prêt à prendre le relais automatiquement.
- L'alimentation électrique est également **double** : si une source tombe en panne, l'autre prend le relais.

Bénéfice : le réseau reste opérationnel en permanence, même en cas de problème.

Avec ces mesures, le réseau de la mairie sera **protégé contre les erreurs et les interventions non autorisées**, tout en garantissant que **les services pour le public et le personnel fonctionnent toujours correctement**.