Houari Chafi, Mohammed Chafi, Ayyoub BELHASSEN | Date : 07/10/2025

Compte rendu de la journée du 07/10/2025

Mairie de Maisons-Alfort

Objet : Clôture du projet – Validation finale du plan de sécurité réseau
Entreprise : ROBUSTSÉCURITÉ

Version 1.2

Sommaire du Plan de Sécurité Réseau pour la Mairie Maison Alfort

Introduction

Madame, Monsieur,

Toute l'équipe de

ROBUSTSÉCURITÉ vous remercie de la confiance que vous nous accordez pour sécuriser votre infrastructure réseau. Notre mission est de garantir que votre réseau interne reste sécurisé, stable et fiable, tout en assurant l'ouverture de votre nouvelle salle d'exposition au public.

L'analyse menée a permis de mettre en évidence des points de vigilance essentiels pour prévenir les incidents, protéger vos informations sensibles et assurer la continuité de vos services.

2. Faiblesses et Risques Actuels

Le diagnostic initial a révélé des **vulnérabilités physiques et organisationnelles** pouvant compromettre le bon fonctionnement du réseau et la sécurité des données. Ces risques provenaient autant de l’extérieur que d’une utilisation interne non maîtrisée.

Faiblesses Physiques

- **Local technique mal sécurisé** : accès trop facile, risque de vol ou de sabotage des équipements.
- **Absence de vidéosurveillance** : aucune possibilité de contrôle ni de preuve en cas d’incident.
- **Alimentation électrique non contrôlée** : absence d’onduleurs (UPS), risque d’arrêt brutal du réseau.
- **Accès visiteurs insuffisamment restreint** : proximité avec la salle d’exposition, exposition du matériel aux manipulations involontaires.

Faiblesses Organisationnelles

- **Manque de procédures d’accès claires** : pas de règles définies pour l’accès au matériel réseau.
- **Formation insuffisante du personnel** : risques d’erreurs humaines (mots de passe faibles, mauvaise manipulation du matériel).

---

3. Plan de Mesures Correctives

Sécurité Physique et Matérielle

Ces mesures visent à protéger le matériel et à garantir la continuité du service :

1. **Installation d’un local sécurisé**
    - Accès restreint par badge ou clé sécurisée.
    - Interdiction d’accès au public.
    - Contrôle régulier des serrures et des portes.
      → **Bénéfice :** réduction des risques de sabotage et d’accès non autorisé.
2. **Sécurisation des câbles**
    - Utilisation de câbles blindés et passage dans des goulottes sécurisées.
    - Élimination des câbles exposés au public.
      → **Bénéfice :** prévention des déconnexions accidentelles et interférences.
3. **Mise en place de vidéosurveillance**
    - Caméras installées dans le local technique et aux accès principaux.
    - Enregistrements disponibles uniquement pour le personnel autorisé.
      → **Bénéfice :** dissuasion des intrusions et traçabilité accrue.
4. **Alimentation sécurisée**
    - Installation d’onduleurs (UPS) pour assurer la continuité électrique.
    - Verrouillage des prises et contrôle des protections contre les surtensions.
      → **Bénéfice :** continuité de service et protection du matériel.

Sécurité du Réseau et Organisationnelle

Ces mesures garantissent un réseau protégé, segmenté et résilient :

1. **Protection par mot de passe**

- Tous les équipements réseau disposent de mots de passe forts et distincts.
- Seuls les administrateurs y ont accès.
  → **Bénéfice :** prévention des modifications non autorisées.

2. **Connexion sécurisée pour la configuration**
   - Accès distant via protocoles sécurisés (SSH, HTTPS).
   - Aucune configuration non chiffrée autorisée.
     → **Bénéfice :** protection contre l'interception des données.
3. **Sauvegardes régulières**
   - Sauvegarde complète des configurations réseau.
   - Vérification périodique de l'intégrité des fichiers de sauvegarde.
     → **Bénéfice :** restauration rapide en cas de panne ou d'erreur.
4. **Redondance du réseau et de l'alimentation**
   - Installation d'un switch secondaire de secours.
   - Double alimentation électrique sur les équipements critiques.
     → **Bénéfice :** continuité du service même en cas de défaillance.

---

4. Actions Réalisées – Phase de Finalisation

Les opérations suivantes ont été menées pour clôturer le projet :

- ✅ **Finalisation du schéma réseau** : tous les équipements ont été représentés et documentés dans le plan final.
- ✅ **Attribution des adresses IP** : adressage complet selon le plan d'adressage établi (VLAN 20 et VLAN 30 intégrés).
- ✅ **Création des VLAN 20 et VLAN 30** : segmentation du réseau pour séparer les flux internes et publics.
- ✅ **Désactivation des ports inutiles** : pour limiter les connexions non autorisées et renforcer la sécurité.
- ✅ **Mise à jour du diagramme de Gantt** : toutes les étapes du projet sont complétées et archivées.

- ✅ **Validation finale avec la Mairie** : présentation du plan de sécurité, validation client et clôture officielle du projet.

---

5. Conclusion

L’application de l’ensemble de ces mesures garantit désormais un **réseau stable, segmenté et protégé** contre les risques d’intrusion, de panne ou de mauvaise manipulation.
La **Mairie de Maisons-Alfort** dispose d’une infrastructure **sécurisée, documentée et prête à l’exploitation** pour l’ouverture de sa salle d’exposition.

L’équipe **ROBUSTSÉCURITÉ** remercie la mairie pour sa confiance et reste disponible pour l’accompagner lors des phases de **maintenance et de suivi post-projet**.