# Cahier des charges pour la Sécurisation du Système Informatique d'un Hôpital

## 1. Introduction

L'objectif de ce cahier des charges est de définir les exigences et les tâches pour la sécurisation du système informatique d'un hôpital. Compte tenu des récentes attaques cyber et de la sensibilité des données médicales, il est essentiel de mettre en place une infrastructure informatique robuste et sécurisée. Le projet consistera à créer une architecture réseau cloisonnée, à sécuriser l'accès aux données médicales, à établir une connexion VPN avec un autre hôpital, et à documenter l'ensemble du système.

## 2. Architecture réseau sécurisée

Le réseau de l'hôpital sera structuré en trois espaces séparés : la direction, l'administration et la gestion des données médicales. Chacun de ces espaces devra être isolé des autres. Le standard 802.1X sera utilisé pour sécuriser l'accès au réseau, avec une authentification centralisée via Radius. Les droits d'accès seront définis comme suit :

- Le personnel de la direction pourra accéder aux données de la direction et de l'administration.

- Le personnel de l'administration pourra accéder aux données de l'administration.

- Le personnel médical pourra accéder aux données médicales.

## 3. Sécurisation de l'accès Internet et VPN

L'accès à Internet sera bloqué dans les deux sens, à l'exception de la connexion VPN établie avec un autre hôpital. Cette connexion permettra uniquement la consultation des données médicales, sans accès à Internet. Les tâches comprennent :

- Mise en place d'un VPN avec l'autre hôpital.

- Blocage complet de l'accès à Internet.

- Configuration pour permettre uniquement la consultation des données médicales via le VPN.

## 4. Sécurité physique

L'accès à la salle d'opération sera restreint aux personnels médicaux pendant les opérations, tandis que le personnel d'entretien y aura accès en dehors des opérations médicales.

## 5. Gestion des données

La création de deux bases de données distinctes sera nécessaire pour stocker les informations sur le personnel et les patients. Un serveur sera dédié à la direction, et les données des serveurs seront sauvegardées régulièrement pour permettre une restauration efficace en cas de perte de données. Des procédures de réinstallation automatisée des serveurs seront mises en place pour réactiver un serveur dont le système est effacé ou inutilisable. De plus, une procédure d'échange des rôles entre serveur principal et serveur de secours sera établie pour garantir la continuité des services en cas de défaillance.

## 6. Documentation

Toutes les étapes du projet, y compris la configuration du réseau, l'installation des serveurs, les procédures de secours, les politiques d'accès et de sécurité, devront être minutieusement documentées. Cette documentation sera essentielle pour permettre au personnel du service informatique/réseau d'accomplir les tâches. Il est recommandé d'utiliser GitHub pour stocker la documentation et les configurations du réseau.

## 7. Matériel disponible

Le projet devra être réalisé en utilisant le matériel suivant :

- 2 switches Cisco Catalyst C34/5XX

- 1 borne WiFi Linksys WRT54G

- 1 routeur Cisco 1841/1900 pour gérer les accès et les droits entre les services

- 4 serveurs dédiés : direction, administration, médical, VPN (ou box Cisco)

- Quelques postes clients 802.1X

- 1 ordinateur portable 802.1X

- 1 smartphone Android avec 802.1X

## 8. Autres tâches

En plus des tâches mentionnées ci-dessus, il sera nécessaire de procéder à l'installation des services suivants :

- Active Directory

- Serveur DHCP

- Serveur DNS

- Serveur de Stockage

- Base de données

- Serveur Radius

- Script d'automatisation

- Contrôleur SLB (Server Load Balancer)

- Dispositifs de caméra

- Lecteurs et graveurs de cartes

## 9. Documentation pour les utilisateurs, administrateurs et programmeurs

Une documentation complète devra être créée pour les utilisateurs, les administrateurs et les programmeurs, couvrant tous les aspects du système informatique, de la sécurité et des procédures d'entretien.

Ce cahier des charges servira de référence pour la planification, la mise en œuvre et la documentation du projet visant à sécuriser le système informatique de l'hôpital. Il est essentiel de respecter toutes les réglementations de sécurité et de protéger les données médicales sensibles.