|  |
| --- |
|  |
| Analyse de risque |
| CHU de Ynov |

|  |
| --- |
| VIOLLET Yoan, ETESSE Tristan |

# 1. Actifs Critiques

Le système d'information du CHU repose sur un ensemble d'actifs essentiels, dont la compromission aurait un impact direct sur la continuité des soins, la sécurité des patients et la conformité réglementaire.

- Infrastructures techniques : serveurs de fichiers, équipements médicaux connectés, réseau interne, commutateurs, routeurs, pare-feu.

- Applications métiers : logiciels hospitaliers, portails patients, système de gestion des rendez-vous, bases de données médicales.

- Données sensibles : dossiers médicaux, identifiants personnels, données administratives, financières et RH.

# 2. Vulnérabilités identifiées

### a) Vulnérabilités techniques

- Une segmentation du réseau insuffisante favorise les mouvements latéraux en cas de compromission.

- Certains systèmes ne sont pas à jour, exposant des failles connues.

- L’absence d’authentification forte sur des applications critiques augmente les risques d’accès non autorisé.

- Logiciels obsolètes utilisés sur des équipements médicaux, difficilement maintenables.

### b) Vulnérabilités organisationnelles et humaines

- Le personnel hospitalier n'est pas suffisamment formé aux bonnes pratiques de cybersécurité.

- Aucune politique de sécurité (PSSI) clairement formalisée.

- Conformité insuffisante avec les exigences du RGPD et des normes ISO 27001.

### c) Vulnérabilités liées aux outils et au déploiement

- Outils de détection de vulnérabilités mal configurés ou rarement utilisés.

- Absence de supervision continue (SIEM) ou de réponse rapide en cas d’anomalie.

# 3. Principales menaces

### a) Menaces externes

- Campagnes de phishing ciblant le personnel hospitalier.

- Attaques par rançongiciel (ransomware) visant les bases de données médicales.

- Tentatives de déni de service (DDoS) sur les portails web publics.

### b) Menaces internes

- Abus de privilèges d'accès par des utilisateurs légitimes.

- Fuites de données sensibles à la suite d’un partage non autorisé ou à un défaut de chiffrement.

- Erreurs de configuration dues à un manque de supervision ou de procédures claires.

# Plan d'action proposé

### Gouvernance & conformité

- Mise en place d’une PSSI formalisée, intégrant les responsabilités, les procédures et les contrôles de sécurité.

- Alignement progressif avec les standards ISO 27001 et le RGPD.

### Sécurisation technique

- Segmentation du réseau via VLANs.

- Déploiement d’un pare-feu pfSense et d’un IDS/IPS Snort.

- Application régulière des mises à jour de sécurité sur tous les systèmes.

- Whit List/Black List

### Gestion des accès

- Activation de l’authentification multi-facteurs (MFA) sur tous les comptes à privilèges.

- Centralisation de la gestion des identités via Active Directory et restrictions par rôle.

- Déploiement d’un bastion d’administration pour les accès sensibles.

### Surveillance et détection

- Mise en place d’un SIEM (ex. : ELK, Splunk) pour la corrélation des logs et la détection d’activités anormales.

- Déclenchement d’alertes en temps réel et journalisation centralisée.

### Sensibilisation & formation

- Organisation de campagnes de simulation de phishing.

- Formations continues en cybersécurité pour le personnel administratif et médical.

### Continuité d’activité (PCA/PRA)

- Sauvegardes chiffrées quotidiennes et hebdomadaires.

- Tests réguliers de restauration sur un environnement de secours.

### Audits & tests d’intrusion

- Réalisation trimestrielle de scans de vulnérabilités (Nessus, OpenVAS).

- Mise en œuvre de tests d’intrusion internes (via Metasploit) pour évaluer les systèmes.