

UNIVERSITÉ DE NAMUR

SÉCURITÉ ET FIABILITÉ DES SYSTÈMES INFORMATIQUES

IHDCM035

---

# Etude des Risques: Informatisation d'un Centre Hospitalier

---

*Auteur*

Kenny WARSZAWSKI

*Professeur*

Jean-Nöel COLIN

December 15, 2019



# Table des matières

<b>1</b>	<b>Introduction</b>	<b>2</b>
1.1	Contexte . . . . .	2
1.2	Objectifs . . . . .	2
<b>2</b>	<b>Analyse de risques</b>	<b>3</b>
2.1	Evènement redoutés . . . . .	3
2.1.1	Accès aux informations médicales . . . . .	3
2.1.2	Encodage des données . . . . .	3
2.1.3	Réputation . . . . .	4
2.2	Scénarios de menace . . . . .	4
2.2.1	Serveurs . . . . .	4
2.2.2	Système d'authentification . . . . .	4
2.2.3	Données . . . . .	4
2.2.4	Réseau interne . . . . .	4
2.2.5	Disques durs . . . . .	4
2.2.6	Ordinateurs . . . . .	4
2.3	Synthèse . . . . .	4
<b>3</b>	<b>Plan d'action</b>	<b>4</b>
3.1	sub-1 . . . . .	4
3.2	sub-2 . . . . .	4
	<b>Table des figures</b>	<b>5</b>
	<b>Bibliographie</b>	<b>5</b>

# 1 Introduction

## 1.1 Contexte

Cette étude des risques concerne le Centre Hospitalier Mercy West(CHMW). Ce centre a mis en place un système informatique qui permet de centraliser les données de leurs patients. Afin de réaliser cela, l'hôpital a mis à disposition un ordinateur connecté à une plateforme en ligne. Ainsi, le corps médical peut encoder les informations nécessaires sur leurs patients à la fin de leur service. Avant de commencer leur journée, le personnel peut également accéder aux dernières informations récoltées par leurs collègues pour rester à jour sur: l'état de santé des patients, les soins reçus, les opérations subies, les médicaments prescrits, etc.

Chaque membre du personnel possède un badge afin de s'authentifier sur la plateforme. Les droits de lecture et modification d'un dossier médical sont associés à des droits qui sont assignés aux utilisateurs. Ces droits sont associés à la fonction professionnelle que l'utilisateur authentifié exerce. Par exemple, si un médecin s'authentifie, il pourra modifier les prescriptions de médicaments d'un patient tandis qu'une aide soignante ne pourra pas. Par contre, cette dernière aura le droit de modifier l'état de santé général du patient: taille, poids, nutrition, etc.

Ce logiciel impacte donc le quotidien des employés de cet hôpital. Il est indispensable que tout le personnel indique rigoureusement les informations concernant le patient. Ainsi, il sera possible de garantir un suivi médical journalier de haute qualité mais également d'en conserver un historique. Si une personne mal intentionnée ou tout simplement non-formée indique des informations erronées, ces peuvent avoir de lourdes conséquences sur le patient. Par conséquent, la réputation de l'hôpital pourrait gravement diminuer. L'accès aux informations médicales, l'encodage des données ainsi que la réputation de l'hôpital sont des **biens essentiels**.

La confidentialité est un des critères de sécurité les plus importants pour l'hôpital. De fait, si les informations médicales d'un patient arrivent entre de mauvaises mains, cela peut également avoir des conséquences dramatiques. Il est essentiel que les données médicales soient sécurisées et exploitables uniquement par les utilisateurs qui en ont le droit.

En ce qui concerne les **biens supports**, le centre hospitalier possède une infrastructure informatique dédiée afin de faire fonctionner l'ensemble de ses logiciels. Cette infrastructure comprend: des ordinateurs, des serveurs, un sous-réseau, un système d'authentification et de multiples disques durs afin de pouvoir stocker les données.

## 1.2 Objectifs

L'objectif de cette étude est de pouvoir établir une analyse de risque concernant ce projet. De plus, un plan d'action sera proposé en réponse aux événements redoutés par le centre hospitalier. Le champ de cette étude sera toutefois limitée uniquement à la plateforme précédemment mentionnée. Tous les autres processus organisationnels ou informatiques nullement liés à la problématique ne seront pas pris en compte.

## 2 Analyse de risques

### 2.1 Evènement redoutés

Cette section est dédiée à une analyse des évènements redoutés. Cette analyse est basée sur les biens essentiels de l'hôpital et des critères de sécurités importants. (Disponibilité, Confidentialité et Intégrité)

#### 2.1.1 Accès aux informations médicales

L'analyse de ce bien essentiel concerne la consultation des informations des patients. Par exemple, en début de service par un membre du corps médical.

Evenements Redoutés	Critère de Sécurité	Source de la Menace	Impact	Severité
Incendie dans la salle des serveurs (+ système de stockage)	Disponibilité	- Dysfonctionnement de matériel - Surtension électrique - Personne mal-intentionnée	- Perte des données - Système inaccessible - Réputation de l'hôpital - Vie des patients	Elevé
Dysfonctionnement du système d'authentification	Disponibilité	- Erreur logiciel - Utilisateur	- Impossibilité de consulter les informations	Elevé
Intrusion d'une personne non autorisée	Confidentialité	- Personnel qui a oublié son badge et utilise celui d'un collègue - Mauvaise gestion des roles assignés aux utilisateurs - Personne mal-intentionnée	- Divulgateion de données personnelles à une personne non-autorisée. (secret médical)	Elevé
Panne de courant	Disponibilité	- Problème sur le réseau électrique - Personne mal-intentionnée	- Impossible de récupérer les informations des patients	TODO
TODO	TODO	TODO	TODO	TODO

Table 1: Table d'analyse de l'accès aux information médicales

#### 2.1.2 Encodage des données

L'analyse de ce bien essentiel concerne l'encodage des données sur un patient. Par exemple, en fin de service par un membre du corps médical.

Evenements redoutés	Critère de Sécurité	Source de la Menace	Impact	Severité
Intrusion d'une personne non-autorisée	Intégrité	- Personnel qui a oublié son badge et utilise celui d'un collègue - Mauvaise gestion des roles assignés aux utilisateurs - Personne mal-intentionnée	- Altération des données des patients - La vie du patient est mise en danger	Elevé
Dysfonctionnement du système d'authentification	Disponibilité	- Erreur logiciel - Utilisateur	- Système inutilisable	Elevé
Panne de courant	Disponibilité	- Problème sur le réseau électrique - Personne mal-intentionnée	- Système inutilisable	Elevé
Incendie dans la salle des serveurs (+ système de stockage)	Disponibilité	- Dysfonctionnement du matériel - Surtension électrique - Personne mal-intentionnée	- Système inutilisable	Elevé

Table 2: Table d'analyse de l'encodage des données

### **2.1.3 Réputation**

## **2.2 Scénarios de menace**

Cette section est dédiée à une analyse des scénarios de menaces. Cette analyse est basée sur les biens support de l'hôpital.

### **2.2.1 Serveurs**

Scénario de menace	Source de la menace	Probabilité
Panne du serveur	Obsolescence du matériel	Moyenne
Incendie		

### **2.2.2 Système d'authentification**

### **2.2.3 Données**

### **2.2.4 Réseau interne**

### **2.2.5 Disques durs**

### **2.2.6 Ordinateurs**

## **2.3 Synthèse**

# **3 Plan d'action**

## **3.1 sub-1**

## **3.2 sub-2**

## Table des figures

## Bibliographie

- [1] F. A. Kraemer et al. “Fog Computing in Healthcare–A Review and Discussion”. In: *IEEE Access* 5 (2017), pp. 9206–9222. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2017.2704100.