

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 9, 2019



Table des matières

1	Introduction	2
1.1	Contexte	2
1.2	Objectifs	2
2	Analyse de risques	3
2.1	Evènement redoutés	3
2.2	sub-2	3
3	Plan d'action	3
3.1	sub-1	3
3.2	sub-2	3
	Table des figures	4
	Bibliographie	4

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 nom d'utilisateur ainsi qu'un mot de passe pour 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: poids, TODO, TODO, TODO. (demander à mam)

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. La qualité des soins, le suivi médical et réputation sont des assets essentiels pour cet hôpital.

La confidentialité est également un élément très important. 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 exploitable uniquement par les utilisateurs qui en ont le droit.

Le centre hospitalier possède une infrastructure informatique afin de faire fonctionner l'ensemble de ses logiciels. Les données sont stockées sur de multiples disques durs configurés en RAID 50. Cette méthode permet de récupérer les données en cas de panne d'un disque.

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 organisationnel ou informatiques nullement liés à la problématique ne seront pas mentionnés.

Dreaded event	Security criteria	Threat source	Impact	Severity
Incendie de l'infrastructure informatique				High

2 Analyse de risques

2.1 Evènement redoutés

toutes les informations des patients sont perdues. Il s'agit ici d'un énorme risque.

2.2 sub-2

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.