

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 26, 2019



Table des matières

1	Introduction	2
1.1	Contexte	2
1.2	Objectifs	2
2	Analyse de risques	3
2.1	Liens entre biens essentiels et biens supports	3
2.2	Evènement redoutés	3
2.2.1	Accès aux informations médicales	3
2.2.2	Encodage des données	4
2.2.3	Gestion des stocks pharmaceutiques	5
2.3	Scénarios de menace	7
2.3.1	Serveurs	7
2.3.2	Serveur Active Directory	8
2.3.3	Ordinateurs	8
2.3.4	Disques durs	9
2.4	Conclusion	9
3	Plan d'action	10
3.1	sub-1	10
3.2	sub-2	10
	Table des figures	11
	Bibliographie	11

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. Via cette plateforme, il est également possible de gérer les stocks de médicaments. L'accès aux informations médicales, l'encodage des données ainsi que la gestion des stocks pharmaceutiques sont donc les **biens essentiels** liés à ce projet.

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 serveur Active Directory 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 scénarios de menace et aux événements redoutés par le centre hospitalier. Le champ de cette étude sera toutefois limité uniquement à la plateforme en ligne précédemment mentionnée. Tous les autres processus organisationnels ou informatiques nullement liés à ce projet ne seront pas pris en compte.

2 Analyse de risques

2.1 Liens entre biens essentiels et biens supports

Biens essentiels Bien supports	Accès aux informations médicales	Encodage des données	Gestion des stocks pharmaceutiques
<u>SYS - Réseau interne</u>			
<i>MAT - Serveurs</i>	X	X	X
<i>MAT - Serveur Active Directory</i>	X	X	X
<i>MAT - Ordinateurs</i>	X	X	X
<i>MAT - Disques durs</i>	X	X	X
<u>ORG - Organisation de l'hôpital</u>			
<i>PER - Aide soignant</i>	X	X	
<i>PER - Infirmier</i>	X	X	
<i>PER - Medecin</i>	X	X	
<i>PER - Chirurgien</i>	X	X	
<i>PER - Administrateur système</i>	X	X	X
<i>PER - Gestionnaire de stock</i>			X
<u>LOC - Locaux</u>			
<i>LOC - Salle des serveurs</i>	X	X	X
<i>LOC - Salle d'ordinateurs</i>	X	X	X

Table 1: Tableau des liens entre biens essentiels et bien supports

2.2 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)

2.2.1 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.

Evènements Redoutés	Critère de Sécurité	Source de la Menace	Impact	Sévérité
Incendie dans la salle des serveurs (+ système de stockage)	Disponibilité	<ul style="list-style-type: none"> - Dysfonctionnement de matériel - Surtension électrique - Personne mal-intentionnée 	<ul style="list-style-type: none"> - Perte des données - Système inaccessible - Réputation de l'hôpital - Vie des patients 	Elevé
Dysfonctionnement du système d'authentification	Disponibilité	<ul style="list-style-type: none"> - Erreur logiciel - Personne mal-intentionnée 	<ul style="list-style-type: none"> - Impossibilité de consulter les informations 	Elevé
Intrusion d'une personne non-autorisée	Confidentialité	<ul style="list-style-type: none"> - Personnel qui a oublié son badge et utilise celui d'un collègue - Mauvaise gestion des rôles assignés aux utilisateurs - Personne mal-intentionnée 	<ul style="list-style-type: none"> - Divulcation de données personnelles à une personne non-autorisée. (secret médical) 	Elevé
Panne de courant	Disponibilité	<ul style="list-style-type: none"> - Problème sur le réseau électrique - Personne mal-intentionnée 	<ul style="list-style-type: none"> - Impossible de récupérer les informations des patients 	Elevé

Table 2: Table d'analyse de l'accès aux informations médicales

2.2.2 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. Cependant, l'encodage requiert un formalisme précis. Les nouveaux médecins ou tout médecin non-initié à ce formalisme peut engendrer un encodage erroné.

Evènements Redoutés	Critère de Sécurité	Source de la Menace	Impact	Sévérité
Intrusion d'une personne non -autorisée	Intégrité	<ul style="list-style-type: none"> - Personnel qui a oublié son badge et utilise celui d'un collègue - Mauvaise gestion des rôles assignés aux utilisateurs - Personne mal-intentionnée 	<ul style="list-style-type: none"> - Altération des données des patients - La vie du patient est mise en danger 	Elevé
Dysfonctionnement du système d'authentification	Disponibilité	<ul style="list-style-type: none"> - Erreur logiciel - Utilisateur 	- Système inutilisable	Elevé
Panne de courant	Disponibilité	<ul style="list-style-type: none"> - Problème sur le réseau électrique - Personne mal-intentionnée 	- Système inutilisable	Elevé
Incendie dans la salle des serveurs (+ système de stockage)	Disponibilité	<ul style="list-style-type: none"> Dysfonctionnement du matériel - Surtension électrique - Personne mal-intentionnée 	- Système inutilisable	Elevé

Table 3: Table d'analyse de l'encodage des données

2.2.3 Gestion des stocks pharmaceutiques

Ce bien essentiel correspond à la partie du système informatique qui est capable de gérer les stocks pharmaceutique. Etant donné que les médicaments sont prescrits aux patients de manière informatisée, il est possible pour le gestionnaire de stocks d'accéder à une estimation des médicaments qui restent en stocks et également les médicaments qu'il faudrait commander dans les prochains jours. Grâce à ce système, il peut optimiser au mieux les stocks afin de ne pas tomber en rupture de médicaments. A cette fin, le système prévoit également la possibilité de programmer des commandes aux fournisseurs de manière automatisée.

Evènements Redoutés	Critère de Sécurité	Source de la Menace	Impact	Sévérité
Incendie dans la salle des serveurs	Disponibilité	<ul style="list-style-type: none"> - Dysfonctionnement du matériel - Surtension électrique - Personne mal-intentionnée 	<ul style="list-style-type: none"> - Impossible de consulter le stock restant - Impossible de réapprovisionner les stocks 	Elevé
Dosage de médicaments erronés	Intégrité	<ul style="list-style-type: none"> - Nouveaux médecins ne maîtrisant pas le logiciel - Personne mal-intentionnée 	<ul style="list-style-type: none"> - Trop de commandes => Mise à mal de la finance de l'hôpital - Trop peu de commande => Pas assez de médicaments pour les patients 	Elevé
Mauvaise programmation du système automatisé de gestion des stocks	Intégrité	<ul style="list-style-type: none"> - Nouveaux médecins ne maîtrisant pas le logiciel - Personne mal-intentionnée 	<ul style="list-style-type: none"> - Dosage de médicaments erronés 	Elevé
Intrusion d'une personne non-autorisée	Intégrité	<ul style="list-style-type: none"> - Personnel qui a oublié son badge et utilise celui d'un collègue - Mauvaise gestion des rôles assignés aux utilisateurs - Personne mal-intentionnée 	<ul style="list-style-type: none"> - Sabotage des stocks informatisés 	Elevé
Panne de courant	Disponibilité	<ul style="list-style-type: none"> - Problème sur le réseau électrique - Personne mal-intentionnée 	<ul style="list-style-type: none"> - Impossible de consulter le stock restant - Impossible de réapprovisionner les stocks 	Elevé

Dysfonctionnement du système d'authentification	Disponibilité	- Erreur Logiciel - Personne mal-intentionnée	- Impossible de consulter le stock restant - Impossible de réapprovisionner les stocks	Elevé
---	---------------	--	---	-------

Table 4: Table d'analyse de gestion des stocks pharmaceutiques

2.3 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.

2.3.1 Serveurs

Les serveurs de l'hôpital sont situés dans une salle qui est prévue à cet effet. Historiquement, l'hôpital ne possédait que très peu de logiciels informatiques. Ils n'ont donc pas investi dans des équipements afin de protéger leur infrastructure. Cette catégorie reprend donc les serveurs où sont installés les logiciels de l'hôpital.

Scénario de Menace	Source de la Menace	Probabilité
Incendie dans la salle des serveurs	Personne mal-intentionnée	Faible
	Dysfonctionnement du matériel	Moyenne
	Surtension électrique	Haute
Infection par un virus informatique	Personne mal-intentionnée	Faible
	Téléchargement de données non-vérifiées sur internet par un utilisateur	Moyenne
Panne de serveur	Personne mal-intentionnée	Faible
	Dégradation naturelle des composants du serveur	Moyenne
	Mauvaise manipulation d'un technicien	Moyenne
Récupération de données confidentielles	Personnes mal-intentionnée	Faible
	Administrateur système	Faible
	Administrateur système externe	Moyenne
Panne de courant électrique	Personne mal-intentionnée	Faible
	Condition météorologique	Moyenne
	Problème sur le réseau électrique	Moyenne
	Technicien qui débranche un câble par erreur	Haute

Table 5: Tableau des scénarios de menace pour les serveurs

2.3.2 Serveur Active Directory

Le serveur Active Directory de l'hôpital est situé dans la même salle où se trouvent les serveurs. Ce serveur se trouve sur une machine dédiée et est appelé par les différentes applications de l'hôpital afin de pouvoir authentifier les utilisateurs de manière centralisée.

Scénario de Menace	Source de la Menace	Probabilité
Incendie dans la salle des serveurs	Personne mal-intentionnée	Faible
	Dysfonctionnement du matériel	Moyenne
	Surtension électrique	Haute
Infection par un virus informatique	Personne mal-intentionnée	Faible
	Téléchargement de données non-vérifiées sur internet	Moyenne
Panne de serveur	Personne mal-intentionnée	Faible
	Dégradation naturelle des composant du serveur	Moyenne
	Mauvaise manipulation d'un technicien	Moyenne
Récupération de données confidentielles	Personnes mal-intentionnée	Faible
	Administrateur système	Faible
	Administrateur système externe	Moyenne
Altération des données de connexion	Personne mal-intentionnée	Faible
	Administrateur système	Faible
	Administrateur système externe	Moyenne
Panne de courant électrique	Personne mal-intentionnée	Faible
	Condition météorologique	Moyenne
	Problème sur le réseau électrique	Moyenne
	Technicien qui débranche un câble par erreur	Haute

Table 6: Tableau des scénarios de menace pour le serveur Active Directory

2.3.3 Ordinateurs

Ce bien support reprend les ordinateurs qui sont mis à disposition du personnel pour accéder à la plateforme de gestion.

Scénario de Menace	Source de la Menace	Probabilité
Infection par un virus informatique	Personne mal-intentionnée	Faible
	Téléchargement de données non-vérifiées sur internet par un utilisateur	Moyenne
	Personne mal-intentionnée	Faible
	Dégradation naturelle des composant du serveur	Moyenne

Panne d'ordinateur	Mauvaise manipulation d'un technicien	Moyenne
Panne de courant électrique	Personnes mal-intentionnée	Faible
	Condition météorologique	Moyenne
	Problème sur le réseau électrique	Moyenne
	Technicien qui débranche un câble par erreur	Haute

Table 7: Tableau des scénarios de menace pour les ordinateurs

2.3.4 Disques durs

Les disques durs de l'hôpital sont stockés dans un endroit spécifique de la salle serveur. Ces disques durs n'ont aucune configuration particulière afin de garantir des backups. (pas de RAID)

Scénario de Menace	Source de la Menace	Probabilité
Incendie	Personne mal-intentionnée	Faible
	Dysfonctionnement du matériel	Moyenne
	Surtension électrique	Haute
Suppression des données	Personnes mal-intentionnée	Faible
	Administrateur système	Faible
	Administrateur système externe	Moyenne
Corruption des données	Personne mal-intentionnée	Faible
	Erreur du matériel	Moyenne

Table 8: Tableau des scénarios de menace pour les disques durs

2.4 Conclusion

Cette première phase d'analyse permet de mettre l'accent sur certains points importants:

- La salle des serveurs est un espace critique pour le système informatique de cet hôpital. Si les serveurs sont, pour une raison ou une autre, inutilisables, l'ensemble du système informatique s'écroule. Dès lors, il sera impossible de consulter, d'encoder des informations sur les patients ainsi que de gérer les stocks pharmaceutiques.
- Le système de stockage ne possède pas de système de backup. Si un disque est hors-service, il sera impossible de récupérer les données perdues.

Suite à une discussion avec le centre hospitalier, l'établissement a décidé d'entreprendre des mesures pour certains faits évoqués. Ils ont décidé de traiter les événements redoutés dont la sévérité est élevée et dont la menace a une probabilité moyenne et haute.

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.