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 30, 2019

Table des matières

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'hopital 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 prescris, etc.

Chaque membre du personnel possède un badge afin de s'authentifier sur la plateforme. Les droits de lecture et de modification d'un dossier médical sont associés à des rôles qui sont assignés aux utilisateurs. Ces rôles sont associés à la fonction professionelle 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 hopital. Il est indispensable que tout le personnel indique rigoureusement les information 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 important pour l'hôpital. De fait, si les informations médicales d'un patient arrivent entre de mauvaises mains, cela peut avoir des conséquences dramatiques. Il est essentiel que les données médicales soient sécurisées et exploitable 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 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 risques redoutés par le centre hospitalier. Le champs de cette étude sera toutefois limitée 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. Cette étude est inspirée par la méthodologie *Expression des Besoins et Identification des Objectifs de Sécurité* (EBIOS).[2]

2 Analyse de risques

2.1 Liens entre biens essentiels et biens supports

Biens essentiels **Biens supports**	Accès aux informations médicales	Encodage de données	Gestion des stocks pharmaceutiques
SYS - Reseau interne			
MAT - Serveurs	X	X	X
MAT - Serveur Active Directory	X	X	X
MAT - Ordinateurs	X	X	X
MAT - Disques durs	X	X	X
ORG - Organisation de l'hôpital			
PER - Aide soignant	X	X	
PER - Infirmier	X	X	
PER - Medecin	X	X	
PER - Chirurgien	X	X	
PER - Administrateur système	X	X	X
PER - Gestionnaire de stock			X
LOC - Locaux			
LOC - Salle des serveurs	X	X	X
LOC - Salle d'ordinateurs	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
Panne de courant	Disponibilité	- Condition météorologique - Problème sur le réseau électrique - Personne mal-intentionnée	- Impossibilité de consulter les données	Moyenne
Dysfonctionnement du système d'authentification	Disponibilité	- Erreur logiciel - Problème matériel - Cable débranché par erreur - Personne mal-intentionnée	- Impossible de se connecter - Impossibilité de consulter les données	Moyenne
Incendie dans la salle des serveurs	Disponibilité	- Dysfonctionnement de matériel - Surtention électrique - Personne mal-intentionnée	- Impossibilité de consulter les données - Indisponibilité de longue durée	Elevé
Panne de disque dur	Intégrité	- Dysfonctionnement de matériel - Surtension électrique - Personne mal-intentionnée	- Aucune données visibles dans l'interface graphique - Le personnel ne sait plus suivre le dossier des patients - Perte des données	Elevé
Intrusion d'une personne non-autorisée	Confidentialité	- Personnel qui a oublié son badge et utilise celui d' un collègue - Vol de badge - Mauvaise gestion des rôles assignés aux utilisateurs - Personne mal-intentionnée	- Divulgation de données personnelles à une personne non-autorisée (Violation du secret médical)	Elevé

Table 2: Table d'analyse de l'accès aux information 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
Panne de courant	Disponibilité	- Condition météorologique - Problème sur le réseau électrique - Personne mal-intentionnée	- Impossibilité d'encoder les données (désynchronisation avec l' état actuel des patients)	Moyenne
Dysfonctionnement du système d'authentification	Disponibilité	- Erreur logiciel - Problème matériel - Cable débranché par erreur - Personne mal-intentionnée	- Impossible de se connecter - Impossibilité d'encoder les données	Moyenne
Personnel qui utilise le badge d'un collègue	Confidentialité	- Personnel qui a oublié son badge	- Historique de modification faussé - Si erreur d'encodage, risque judiciaire	Moyenne
Incendie dans la salle des serveurs	Disponibilité	- Dysfonctionnement de matériel - Surtention électrique - Personne mal-intentionnée	- Le personnel ne sait plus alimenter le dossier des patients - Indisponibilité de longue durée	Elevé
Panne de disque dur	Intégrité	- Dysfonctionnement de matériel - Surtension électrique - Personne mal-intentionnée	- Le personnel ne sait plus alimenter le dossier des patients - Perte des données	Elevé

Intrusion d'une personne non-autorisée	Confidentialité	- Vol de badge - Mauvaise gestion des rôles assignés aux utilisateurs - Personne mal-intentionnée	- Altération des données des patients - La vie des patients est mise en danger	Elevé
Dosage de médicament encodé de manière erronée	Intégrité	- Médecin qui ne maîtrise pas le logiciel - Personne mal-intentionnée	- L'administration d'un dosage trop élevé peut mettre la vie des patients en danger	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 prescris 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. Grace 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**
Panne de courant	Disponibilité	- Condition météorologique - Problème sur le réseau électrique - Personne mal-intentionnée	- Impossible de consulter le stock restant - Impossible de réapprovisionner les stocks	Moyenne
Dysfonctionnement du système d'authentification	Disponibilité	- Erreur logiciel - Problème matériel - Cable débranché par erreur - Personne mal-intentionnée	- Impossible de se connecter - Impossible de consulter le stock restant - Impossible de réapprovisionner les stocks	Moyenne

Incendie dans la salle des serveurs	Disponibilité	- Dysfonctionnement de matériel - Surtention électrique - Personne mal-intentionnée	- Impossible de consulter le stock restant - Impossible de réapprovisionner les stocks - Indisponibilité de longue durée	Elevé
Panne de disque dur	Intégrité	- Dysfonctionnement de matériel - Surtension électrique - Personne mal-intentionnée	- Impossible de consulter le stock restant - Impossible de réapprovisionner les stocks - Perte des données	Elevé
Intrusion d'une personne non-autorisée	Confidentialité et Intégrité	- Vol de badge - Mauvaise gestion des rôles assignés aux utilisateurs - Personne mal-intentionnée	- Divulgation d' informations de stocks - Altération des informations liées aux stocks (annulation des réservations ou surplus de stocks non-nécessaire)	Elevé
Dosage de médicament encodé de manière erronée	Intégrité	- Médecin qui ne maîtrise pas le logiciel d' encodage - Personne mal-intentionnée	- Trop de commandes => Mise à mal du budget de l'hôpital - Trop peu de commandes => Pas assez de médicaments pour les patients	Elevé
Mauvaise programmation du système automatisé de gestion du stock	Intégrié	- Gestionnaire de stock - Personne mal-intentionnée	- Trop peu de stock - Trop de stock	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 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
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
Panne d'ordinateur	Personne mal-intentionnée	Faible
	Dégradation naturelle des composant du serveur	Moyenne
	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 phase d'analyse de risques 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 pour une autre, inutilisable, 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 politique 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 décidés de traiter les évènement redoutés dont la sévérité est élevée et dont la menace a une probabilité moyenne et haute.

3 Plan d'action

3.1 Solutions

Cette section répertorie l'ensemble des risques dont l'hôpital voudrait se prémunir. Pour chaque risque, la source peut évidemment être différente. C'est pourquoi, le même risque peut être sub-divisé en plusieurs sous-solution en fonction de l'origine de la menace.

3.1.1 Panne de courant

Exigences: Il est nécessaire que le personnel puisse assurer les services medicaux durant 8 heures au minimum. Ainsi, il existe une marge de manoeuvre afin de trouver l'origine de la panne et d'y apporter une solution.

- Prévoir un ou plusieurs groupe élèctrogène afin de pouvoir maintenir l'alimentation des appareils qui sont nécessaires au fonctionnement de la plateforme. (ordinateurs, serveurs, etc)
- Prévoir des batteries lithium-ion ou des batteries à l'hydrogène.

Surtension électrique:

- Prévoir un disjoncteur afin d'éviter que les composants ne soient affectés lors d'une surtension électrique.
- Installer des parafoudres aux points d'entrée des câbles.

Technicien qui débranche un cable par erreur:

- Ajouter des étiquettes sur les cables.
- Prévoir deux alimentations pour les composants critiques.

3.1.2 Dysfonctionnement de matériel:

- Prévoir des pièces de rechanges afin de pouvoir remplacer au plus vite le matériel qui est défecteux.
- Un service de dépannage 24h/24 qui peut intervenir en cas de problème.

3.1.3 Dysfonctionnement du système d'authentification:

- Prévoir un système d'authentification de secours. Par exemple, un système nom d'utilisateur/mot de passe géré par le serveur.
- Si problème matériel, voir section 3.1.2

Erreur logiciel:

- Ajouter des logs.
- Ajouter des exceptions qui peuvent être remontées jusqu'à l'affichage (avec code d'erreur).

Cable débranché par erreur:

- Prévoir un message signifiant ce problème dans l'interface graphique du logiciel. Ainsi, le personnel peut facilement résoudre le problème par eux-mêmes.
- Si le matériel n'est toujours pas reconnu, prévoir un bouton d'aide et/ou appel vers un technicien (section 3.1.2).

3.1.4 Personnel qui utilise le badge d'un collègue:

- Présenter des affiches de prévention sur les ordinateurs afin d'éviter cette pratique. Etant donné que chaque badge est nominatif, chaque action réalisée dans le système peut être tracée. Par conséquent, si une erreur a été commise, celle-ci peut être traquée. L'erreur sera donc juridiquement de la faute du porteur de badge et non de l'emprunteur.

- Prévoir une authentification à plusieurs facteurs. (ex: badge + empreinte digitale)

3.1.5 Intrusion d'une personne non-autorisée:

Vol de badge:

- Ajouter la possibilité de déclarer le vol ou la perte d'un badge. De cette manière, il sera possible de désactiver l'authentification pour le badge qui n'est plus valable. Par extension, cette fonctionnalité pourrait, si l'hôpital le désire, désactiver les badges d'employés qui ne font plus partie de l'hôpital.

- Authentification à plusieurs facteurs. (ex: badge + empreinte digitale)

Mauvaise gestion des rôles assignés aux utilisateurs:

- Système d'approbation: Lors de l'administration des rôles à un utilisateur, celui-ci se voit occtroyer le(s) rôle(s) correspondant(s) à son poste. Cependant, il est parfois nécessaire d'occtroyer à des personnes, des droits supplémentaires car ils possèdent de multiples responsabilités. Cependant, ceux-ci ne correspondent parfois qu'à une partie d'un autre rôle. Pour ce cas spécifique, un système d'approbation par plusieurs entités peut être mis en place afin de garantir les droits minimums pour l'utilisateur. L'occtroi des droits utilisateurs dans ce cas spécifique devra être approuvé par plusieurs personnes. Ces personnes auront le devoir d'analyser rigoureusement les demandes.

3.1.6 Panne de disque dur:

Exigences: Les données des patients sont cruciales pour l'hôpital. Aucune perte ne peut être tolérée. Il est donc nécessaire de prévoir des mécanismes de redondance.

- Prévoir une technique de virtualisation de stockage en RAID 50. Cette technique se base sur le principe du RAID 5 avec de la redondance du RAID 0[1]. C'est-à-dire que cette méthode permet la perte d'un disque par grappe de raid 5. Par exemple, si l'hôpital possède 6 disques et met en place 2 grappes de 3 disques dur, il est sans danger de perdre 2 disques si ceux-ci sont répartis sur les deux grappes.

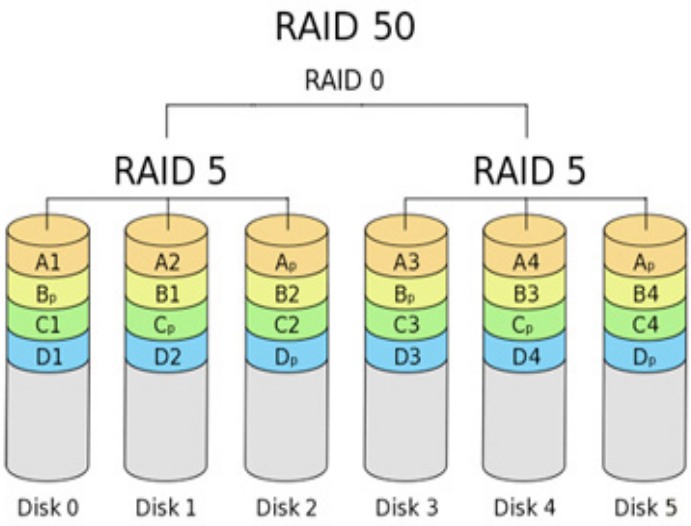

Figure 1: Raid 50. (Source: [1])

- La solution précédente est efficace mais ne peut couvrir la perte des données en cas d'incendie. Si tous les disques durs sont touchés, il sera impossible de restaurer les données. Afin de prévenir ce cas défaillant, un système de backup journalier vers un autre centre hospitalier localisé dans une autre ville peut être mis en place. Ainsi, il sera toujours possible de récupérer les données en cas de gros désastre. Un compromis avec un autre hôpital peut être convenu afin de limiter les coûts. (Chaque hôpital peut conserver un backup de l'autre)

3.1.7 Dosage de médicament encodé de manière erronée

- Prévoir des séances de formation à l'encodage des données
- Permettre plusieurs unités de mesures dans le logiciel. Ainsi, le logiciel peut convertir le dosage dans d'autres unités si nécessaire.
- Prévoir des message d'information si le dosage semble trop élevé ou trop faible. (avec pop-up de confirmation)

3.1.8 Mauvaise programmation du système automatisé de gestion du stock

- Prévoir des séances de formation pour les gestionnaires de stock
- Prévoir des aides dans le logiciel afin d'avertir si la programmation est cohérente par rapport à l'existant. (= détecteur d'anomalie)

3.1.9 Incendie dans la salle des serveurs

- Voir section 3.1.1
- Prévoir des détecteurs de fumée.
- Prévoir des portes coupe-feu.

- Prévoir des extincteurs automatique à gaz neutre. Contrairement aux extincteurs automatiques à eau, le matériel informatique n'est pas abîmé par l'eau. Les gaz extincteurs vont permettre d'étouffer le feu sans abîmer les composants.

3.1.10 Panne de serveur

- Prévoir un mécanisme de Fail-Over. Les illustrations ci-dessous représentent le scénario d'un mécanisme de failover.

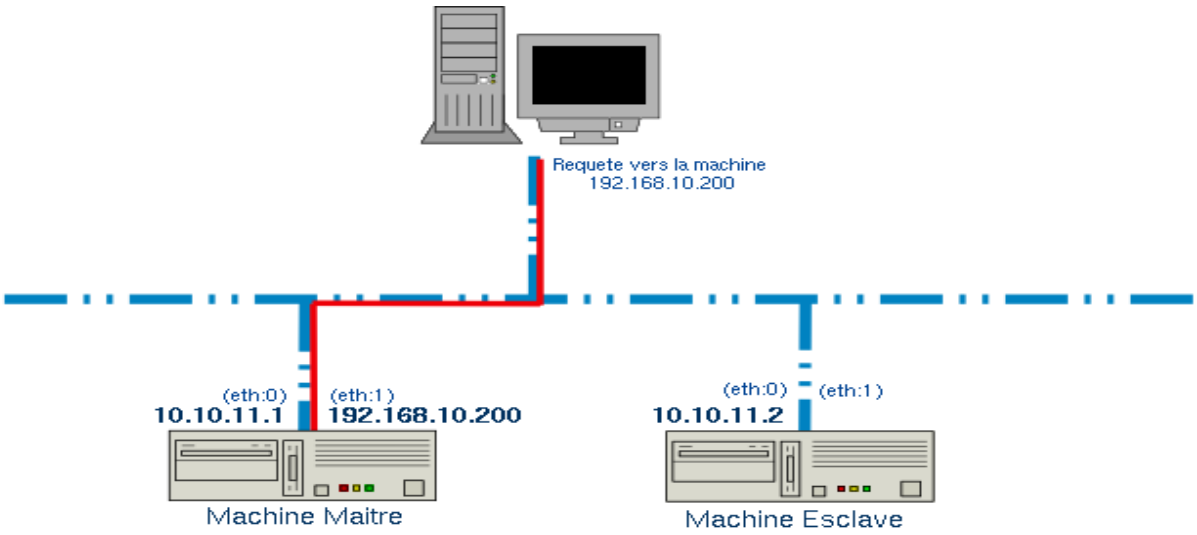

Figure 2: Système fonctionnel. (Source: [3])

Si la machine maitre tombe en panne. La machine esclave est capable de reprendre la main. Ainsi, le système peut toujours fonctionner en attendant que la première machine soit remplacée.

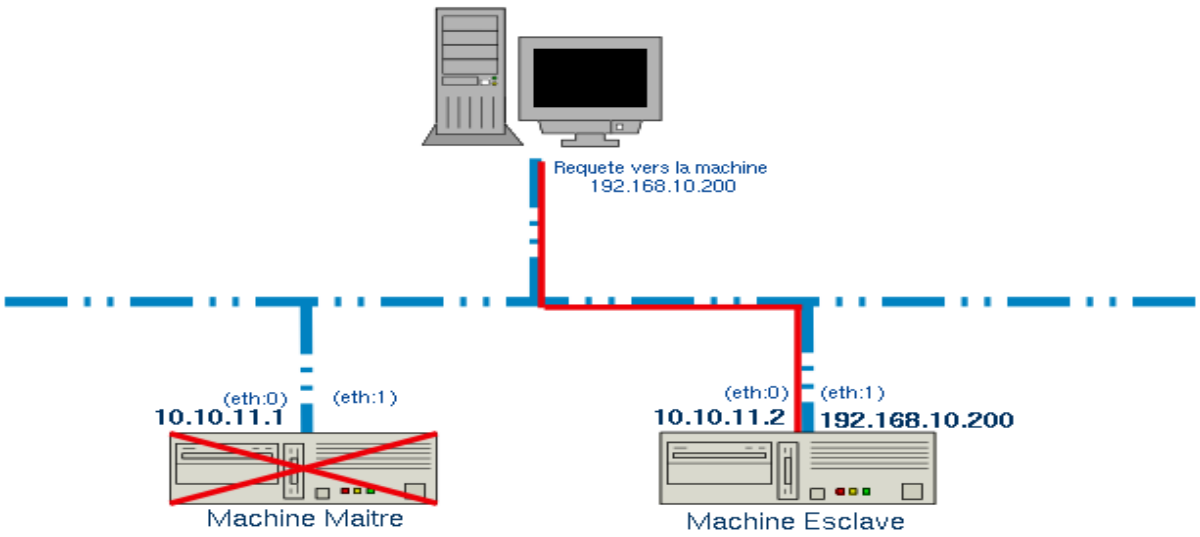

Figure 3: Réatribution des responsabilités à la machine esclave. (Source: [3])

- Voir section 3.1.2

3.1.11 Infection par un virus informatique

- Pour les ordinateurs, l'accès à internet n'est pas obligatoire. Le simple accès à la plateforme est nécessaire. Il suffit de ne pas donner un accès à internet à ces machines.
- Pour les serveurs, il est nécessaire d'installer au minimum un antivirus.
- Pour les serveurs, il est important de désactiver tous les ports inutiles.
- Le routeur qui mène à internet possède déjà un firewall. Par contre, la configuration de celui-ci n'est pas à jour. Il faudrait configurer ce routeur afin de bloquer tout le traffic qui n'est pas nécessaire pour l'hôpital.

3.1.12 Récupération de données confidentielles

- Mettre en place un mécanisme de cryptographie asymétrique afin de sécuriser le transport des données critiques entre l'ordinateur et le serveur applicatif. L'ordinateur va chiffrer les données à envoyer avec clé publique du serveur. De l'autre côté, le serveur va pouvoir déchiffrer le message envoyé par l'ordinateur avec sa clé privée. Il sera le seul à pouvoir lire ce message.

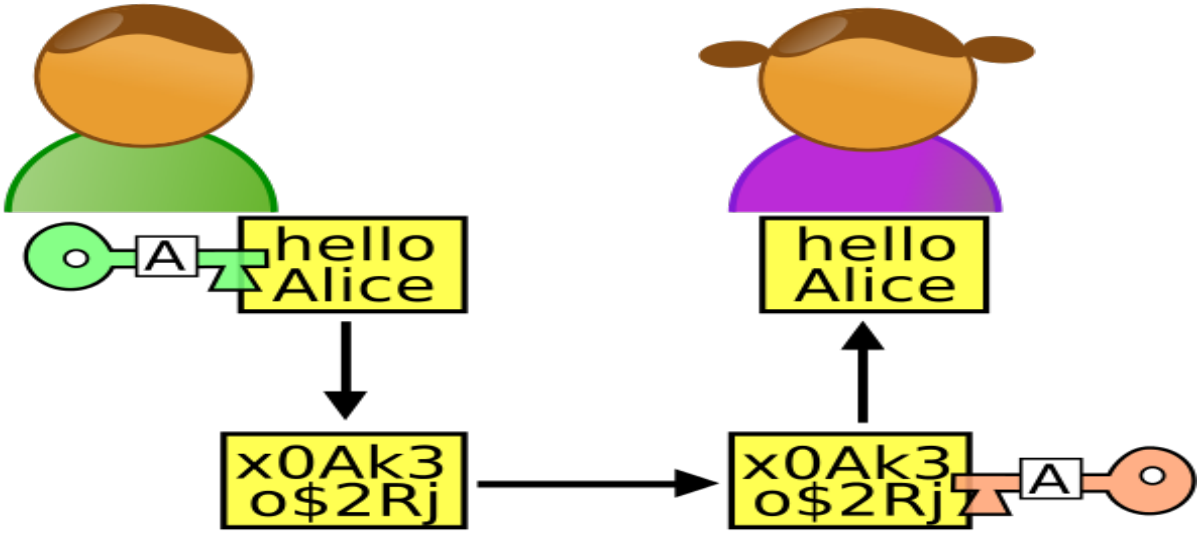

Figure 4: Mécanisme de cryptographie asymétrique. (Source: [4])

- Sécuriser l'accès aux bases de données avec par nom d'utiliseur/mot de passe. Il faut penser à utiliser des utilisateurs spécifiques pour les applications. Ainsi, les droits d'accès peuvent être géré plus facilement. (pas accès à la modification/suppression de schéma, colonnes, etc)

3.1.13 Altération des données de connexion

Administrateur système externe:

- Réduire les droits d'accès. Donner uniquement les accès suffisants.

3.1.14 Suppression des données

Administrateur système externe:

- Réduire les droits d'accès. Donner uniquement les accès suffisants.

3.1.15 Corruption des données

Erreur matériel:

- Si une corruption de données est causée par le disque dur, il est nécessaire d'avoir un mécanisme de récupération de données. Voir section 3.1.6

3.2 Mesures de sécurité

Mesure de sécurité	R 1	R 2	R 3	R 4	R 5	R 6	R 7	R 8	R 9	R 10	R 11	R 12	R 13	R 14	R 15	Bien support sur lequel elle repose	Thème ISO 27002	Prévention	Protection	Récupération
Prévoir plusieurs groupes élèctrogènes	X								X							SYS Reseau interne	11. Sécurité physique et environnementale			X
Prévoir des batteries au lithium-ion	X								X							SYS Reseau interne	11. Sécurité physique et environnementale			X
Prévoir des bateries à l'hydrogène	X								X							SYS Reseau interne	11. Sécurité physique et environnementale			X
Prévoir des disjoncteurs	X	X							X							SYS Reseau interne	11. Sécurité physique et environnementale		X	
Installer des parafoudres aux points d'entrée des câbles	X															SYS Reseau interne	11. Sécurité physique et environnementale		X	
Ajouter des étiquettes sur les cables	X															SYS Réseau interne	11. Sécurité physique et environnementale	X		
Prévoir deux alimentations	X									X						SYS Réseau interne	11. Sécurité physique et environnementale		X	X
Prévoir des pièces de rechanges		X	X			X				X						SYS Réseau interne	11. Sécurité physique et environnementale			X
Service de dépannage 24h/24		X	X			X				X						SYS Réseau interne	14. Acquisition, développement et maintenance des systèmes d'information			X
Système d' authentification de secours	X		X													MAT Serveur	9. Contrôle d'accès			X

Mesure de sécurité	R 1	R 2	R 3	R 4	R 5	R 6	R 7	R 8	R 9	R 10	R 11	R 12	R 13	R 14	R 15	Bien support sur lequel elle repose	Thème ISO 27002	Prévention	Protection	Récupération
Ajouter des logs			X							X						MAT Serveur	12. Sécurité liée à l' exploitation	X		
Ajouter des exceptions			X							X						MAT Serveur	12. Sécurité liée à l' exploitation	X		
Prévoir des avertissement dans l'interface graphique		X	X			X	X	X		X						MAT Serveur	12. Sécurité liée à l' exploitation	X		
Bouton d'aide vers des techniciens en cas de problème		X	X			X	X			X						MAT Serveur	14. Acquisition, développement et maintenance des systèmes d'information	X		
Fiche de prévention				X												MAT Ordinateur	7. La sécurité des ressources humaines	X		
Authentification à plusieurs facteurs					X											MAT Ordinateur	9. Contrôle d' accès		X	X
Désactivation de badge					X											MAT Serveur	8. Gestion des actifs		X	
Système d' approbation								X								MAT Serveur	12. Système d'approbation	X	X	
RAID 50						X										MAT Disques durs	12. Sécurité liée à l' exploitation		X	X
Backup multi-site						X								X	X	MAT Disques durs	12. Sécurité liée à l' exploitation		X	X
Séance de formation							X	X								ORG Organisation de l' hôpital	7. La sécurité des ressources humaines	X		
Pop-up d'aide dans l'interface			X				X	X								MAT Serveur	12. Sécurité liée à l' exploitation	X		
Detecteur de fumée									X							LOC Locaux	11. Sécurité physique et environnementale	X		
Porte coupe-feu									X							LOC Locaux	11. Sécurité physique et environnementale		X	X
Extincteur automatique à gaz									X							LOC Locaux	11. Sécurité physique et environnementale		X	X
Mécanisme de Fail-Over	X	X								X						MAT Serveur	12. Sécurité liée à l' exploitation		X	X
Retirer la connexion à internet											X					MAT Ordinateur	12. Sécurité liée à l' exploitation	X		
Installer un anti-virus											X					MAT Ordinateur Serveur	12. Sécurité liée à l' exploitation	X	X	
Désactiver les ports inutiles											X					SYS Réseau interne	12. Sécurité liée à l' exploitation	X	X	

Mesure de sécurité	R 1	R 2	R 3	R 4	R 5	R 6	R 7	R 8	R 9	R 10	R 11	R 12	R 13	R 14	R 15	Bien support sur lequel elle repose	Thème ISO 27002	Pré-vention	Pro-tection	Récu-pération
Configurer le firewall afin de bloquer les sites non-nécessaires											X					SYS Réseau interne	12. Sécurité liée à l' exploitation	X	X	
Mécanisme de crypto-graphie asymétrique												X				SYS Réseau interne	10. Cryptographie		X	
Authentifi-cation user/password													X	X		SYS Réseau interne	9. Contrôle d' accès		X	
Réduire les droits d'accès													X	X	X	MAT Serveur AD	9. Contrôle d' accès	X	X	

Table 9: Tableau des mesures de sécurité

Table des figures

Liste des tableaux

Bibliographie

[1] Sylvain ADAMI. *Raid - Ses différents types*. 2015. URL: https://www.supinfo.com/articles/single/1176-raid-ses-differents-types (visited on 12/27/2019).

[2] *EBIOS*. URL: https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite (visited on 10/23/2019).

[3] Léalinux. *La haute disponibilité*. 2002. URL: https://lea-linux.org/documentations/La_haute_disponibilit%C3%A9 (visited on 12/28/2019).

[4] Wikipedia. *Cryptographie asymétrique*. URL: https://fr.wikipedia.org/wiki/Cryptographie_asym%C3%A9trique (visited on 12/28/2019).