République de Côte d'Ivoire

Union - Discipline – Travaille

Ministère De l'Economie Numérique

Ecole Supérieure des technologies de l'information et de la télécommunication

Club DSI Côte d'Ivoire

Année Académique : 2018 – 2019

Examen de Sécurité des Systèmes d'Informations

Analyse de risque d'un centre hospitalier avec le Framework EBIOS

Présenté Par :

Coulibaly Mohamed Tiémogo N
Diomandé Tioulé Jurnior
Kouakou Kan Yves Roland

Encadré Par :

Mamadou NAON
DSI de la poste de Côte d'Ivoire
Président du Club des DSI de Cote d'Ivoire

SOMMAIRE

INTRODUCTION

Un système d'information hospitalier (abrégé SIH) est un système d'information appliqué au secteur de la santé, et plus particulièrement aux établissements de santé tel que les hôpitaux, les cliniques, les centres d'analyses et de radiologie etc.

Il permet d'acquérir des données, de les évaluer, de les traiter par des outils informatiques ou organisationnels, de distribuer des informations contenant une forte valeur ajoutée à tous les partenaires internes ou externes de l'établissement. Vu son importance, plusieurs préoccupations se pose à savoir : Quelles sont les risques que présente un telles systèmes ? Quelles sont les moyens à mettre en œuvres pour faire faces à ses risques.

L'objectif de notre étude sera d'apporter une réponse au problématique citée plus haut. Nous ferons dans un premier temps, une analyse de risque grâce au Framework EBIOS à travers l'identification des différentes valeurs métiers et des biens support associé. Dans un deuxième temps, identifier les mesures de sécurité d'un tel système et leur mise en œuvre grâce à ISO27001/5.

Première partie :

Analyse de risque du système d'information d'un centre hospitalier basé sur EBIOS

(Valeurs Métiers, Biens supports, Evènement redouté)

I. Enumération et description des valeurs métiers d'un système d'information hospitalier

1. Logistique hospitalière

Nature	Information
Description	La logistique hospitalière est un service médical qui s'occupe de la gestion des ressources, de leur ravitaillement et de leur mise à la disposition correspondant à des besoins bien déterminer. Il s'agit entre autre de : • **Équipement de diagnostic** : (ultra-sons, l'IRM, les tomodensitométres et les appareils à rayons X) ; • **Équipement thérapeutique** : (pompes à perfusion, lasers médicaux et appareils chirurgicaux) ; • **Équipement vital ;** • **Stock pharmaceutiques.**

2. Les urgences

Nature	Processus
Description	les urgences sont le service d'un hôpital qui s'occupe de recevoir les malades et les blessés qui se présentent d'eux-mêmes, ou qui sont amenés par les services de secours (SAMU, pompiers, etc.). Elle consiste : • A accueilli le malade a son arrivé ; • A l'apporté un ensemble de soins requis pour la stabilisation de son état (premiers soins) ; • A faire les démarches administratives pour garder les traces de son passages au centre médical.

3. La Télémédecine

Nature	Processus
Description	La télémédecine regroupe les pratiques médicales permises ou facilitées par les télécommunications. C'est un exercice de la médecine par le biais des télécommunications et des technologies qui permettent les prestations de santé à distance et l'échange de l'information médicale s'y rapportant. On a par exemple : - Télé-chirurgie : opération chirurgicale assistée à distance par ordinateur ; - Téléradiologie : interprétation d'examens radiologiques à distance (diagnostic et expertise) ; - Télédiagnostic : diagnostique d'un patiente à distance par spécialiste - Etc.

4. Gestions administratives

Nature	Information
Description	Elle constitue le cœur même du système. Elle s'occupe de tout ce qui est du volet administratif à savoir : - Gestion du patient (Identification, préadmission, sortie, transfert, facturation, …) - Gestion du personnel et corps médical - La gestion financière

5. Laboratoire de recherche et d'analyse

Nature	processus
Description	Activité de recherche et d'analyse : - Recherche de remède contre de nouvelle pathologie - Gestion banque de donnée sanitaire - Effectuer des examens biologiques à la demande du patient

6. Energie et Eau

Nature	Information
Description	L'énergie et eau sont des éléments indispensables dans un système hospitalier. Ils permettent d'assurer des fonctions tels que : - Permettre la continuité des différents services (bloc opératoire, Radiologie, …). - La conservation de certaines ressources (Sang, Vaccin, …) ; - Contribuer à l'hygiène du centre hospitalier

II. Identification des biens supports associés à chaque valeurs métiers

1. Logistique hospitalière

Les biens supports associés sont :

MATÉRIELS	• Ordinateur fixe, imprimante, scanner, clavier, souris, clé USB, Poste d'administration, Borne WIFI.
LOGICIELS	• Serveur d'application, serveur de courrier électronique, serveur de bases de données, progiciels (ERP).
ORGANISATIONS	• Employé, stagiaire, personnel d'entretien, Document manuscrit ou imprimé.
LOCAUX ET INSTALLATIONS PHYSIQUES	• site de stockage.

2. Les urgences

Les biens supports associés sont :

MATÉRIELS	• ordinateur portable, Ambulance, equipement de reanimation, de cardiologie, respiratoire liasons radio.
LOGICIELS	• Serveur scanner.
ORGANISATIONS	• Medecin, infirmier, stagiaire.
LOCAUX ET INSTALLATIONS PHYSIQUES	• Bloc d'urgence.

3. La Télémédecine

Les biens supports associés sont :

MATÉRIELS	•Ordinateur fixe, imprimante, scanner, clavier, souris, clé USB, objet connecté, passerelles d'entrée depuis l'extérieur, Borne WIFI..
LOGICIELS	•Serveur d'application, serveur de courrier électronique, serveur de bases de données.
ORGANISATIONS	•Medecin, infirmier, stagiaire.
LOCAUX ET INSTALLATIONS PHYSIQUES	•Salle d'operation, Bureau.

4. Gestions administratives

Les biens supports associés sont :

MATÉRIELS	• Ordinateur fixe, imprimante, scanner, clavier, souris, clé USB, Poste d'administration, Borne WIFI.
LOGICIELS	• Serveur d'application, serveur de courrier électronique, serveur de bases de données, progiciels (ERP).
ORGANISATIONS	• Employé, stagiaire, personnel d'entretien, Document manuscrit ou imprimé.
LOCAUX ET INSTALLATIONS PHYSIQUES	• Accueil, Bureau des responsables.

5. Laboratoire de recherche et d'analyse

Les biens supports associés sont :

MATÉRIELS	•Ordinateur fixe, Equipement analyse biologique , imprimante, scanner, clavier, souris, clé USB, Poste d'administration, Borne WIFI.
LOGICIELS	•Serveur d'application, serveur de courrier électronique, serveur de bases de données, progiciels (ERP).
ORGANISATIONS	•technicien, medecin, personnel d'entretien, Document manuscrit ou imprimé.
LOCAUX ET INSTALLATIONS PHYSIQUES	•Laboratoire.

6. Energie et eau

Les biens supports associés sont :

MATÉRIELS	• Ordinateur fixe, groupe électrogene , climatisation, Poste d'administration.
LOGICIELS	• Serveur de suppervision
ORGANISATIONS	• technicien.

III. Identification des événements redoutés et évaluation de leur gravité

VALEUR MÉTIER	EVÈNEMENT REDOUTÉ	IMPACTS	GRAVITÉ
Logistique hospitalière	Indisponibilité des équipement , Vol des équipement, Mauvais gestion.	• Impacts financiers • Impacts Sur Les missions et service de l'organisation	2
Les urgences	Manques de personnels d'urgences, Manques de professionnalisme.	• Impacts Sur Les missions et service de l'organisation	3
La télémédecine	Support défectueux, indisponibilité du service, Interruption du service, Panne ,Bogue.	• Impacts Sur Les missions et service de l'organisation • Impact juridique • Impact financiers	4
Gestions administratives	Altération des informations, Fuite des informations, Indisponibilité du service,	• Impacts sur l'image et la confiance • Impacts juridiques	2
Laboratoire de recherche et d'analyse	Indisponibilité du service, équipement défectueux, Panne ,Bogue.	• Impacts sur la sécurité ou la santé des personnes • Impacts sur l'image et la confiance • Impacts juridiques	3
Energie et eau	Indisponibilité du service	• Impacts Sur Les missions et service de l'organisation	3

IV. Identification des sources de risques et scénarios stratégiques

SOURCES DE RISQUE	OBJECTIFS VISÉS	CHEMINS D'ATTAQUE STRATÉGIQUES	GRAVITÉ
Employé malveillant	Vol des équipements de santé pour les vendre sur le marché noir	• Corruption des agents de surveillances pour laisser sortir les équipements ; • Faire sortie les équipement grâce à leur affaire (sacs, porche de vêtement, ..)	3
	Altération des données d'un patient pour se faire de l'argent	• Accéder au ordinateur pour modifier les information de la base de données	4
Pirate	Vol d'informations sur le système d'information du laboratoire.	• Accéder par une faille de sécurité application au information de la base de données • Utiliser les accès d'un employé par ingénierie social pour avoir accès au données de la base données	3
	Altération d'informations sur le système d'information du laboratoire.		4
	Indisponibilité du service	• Effectuer une attaque d'indisponibilité de service comme le Dos et le Ddos • Ou attaque d'équipement d'alimentation	4

Deuxième partie :

Identification des mesures de sécurité et leur mise en œuvre grâce à ISO27002

Risque	Thème ISO 27002	Mesures de sécurité	Description	Nature de la précaution		
				Prévention	Protection	Récupération
Vol des équipements de santé	9.1 Zones sécurisée	Périmètre de sécurité physique	Protéger les zones contenant les stocks logistiques par des périmètres de sécurité. Il doivent être inaccessibles par des personnes non autorisées et donc dans des salles hautement sécurisées.			
		Contrôle physique des accès	Protéger les zones sécurisées pas des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité soit admis			
	6.1 Organisation interne	Attribution des responsabilités en matière de sécurité de l'information	Il convient de définir clairement toutes les responsabilités en matière de sécurité des équipement.			
	10.10 Surveillance	Rapports d'Etats	Il convient ici de faire une surveillance régulière sur les équipement et de faire un point sur les états.			
Altération des données	11.2 Gestion de l'accès utilisateur	Gestion des privilèges	Restreindre et contrôler l'attribution et l'utilisation des privilèges (gestion des habilitations)			
	11.4 Contrôle d'accès au réseau	Authentification des utilisateurs	L'authentification des utilisateurs doit se faire de manière sécurisée par un cryptage des mots de passe et une authentification à deux facteurs.			
	10.5 Sauvegarde	Sauvegarde des informations - backups	Prendre toutes les mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de			

			service exigé. Il doit notamment effectuer un double exemplaire des sauvegardes et doit les conserver dans des locaux physiquement séparés.			
Vol d'informations sur le système d'information du laboratoire.	10.7 Manipulation des supports	Sécurité de la documentation système	La documentation décrivant l'ensemble du système doit être gardée avec un niveau de sécurité suffisant pour ne pas permettre à des personnes malveillantes d'avoir une connaissance poussée de l'architecture (mesures de « diffusion restreinte » systématiques).			
	11.2 Gestion de l'accès utilisateur	Gestion des privilèges	Restreindre et contrôler l'attribution et l'utilisation des privilèges (gestion des habilitations).			
	11.4 Contrôle d'accès au réseau	Authentification des administrateurs et des utilisateurs	Afin d'accéder aux fonctions d'administration, les administrateurs doivent être authentifiés. L'authentification doit se faire de manière sécurisée (chiffrage des mots de passe, authentification à deux facteurs) et L'authentification des utilisateurs doit se faire de manière sécurisée par un cryptage des mots de passe et une authentification à deux facteurs			
	12.6 Gestion des vulnérabilités techniques	Mesures relatives aux vulnérabilités techniques	Etre informé en temps r éel de toute vulnérabilité technique des systèmes d'information en exploitation, évaluer l'exposition de l'organisation auxdites vulnérabilités et entreprendre les actions appropriées pour traiter le risque associé.			

	12.3 Mesures cryptographiqu es	Chiffrement des flux	Les flux contenant des informations sensibles ou à caractère personnel doivent être chiffrées.			
Indisponibilité du service	9.2 Sécurité du matériel	Services généraux	Protéger les câbles électriques ou de télécommunications transportant des données contre toute interception ou dommage			

CONCLUSION

Aux termes de travail, nous retenons que les systèmes information hospitalier présentait des risques. Grâces au Framework EBIOS nous avons pu identifier ces risques grâce à une méthodologie propre au Framework. Nous avons d'abord identifié les différentes valeur métiers de ce système. Ces valeurs métiers nous ont ensuite permis d'identifier les biens support qu'il leurs sont associer et d'en déduire les risques associés et aussi les évènements redoutés. Enfin nous avons utilisé l'ISO 27002 pour identifier les mesures de sécurité et leur mise en œuvre.

Ce travail nous permis de mettre en exergue les connaissances du cours de sécurité des système d'exploitation et aussi d'acquérir des connaissances sur le système d'information hospitalier.