Thomas GRZESINSKI

Description du contexte :

Le Centre Hospitalier X est un établissement public de santé implanté depuis le XIXe siècle. À l'origine, il servait de refuge pour les enfants abandonnés, dans un contexte social marqué par la pauvreté et la précarité des familles.

Au fil des décennies, l'établissement s'est considérablement développé pour devenir un hôpital moderne et polyvalent.

Aujourd'hui, le Centre Hospitalier X dispose de multiples services spécialisés — cardiologie, psychiatrie, gynécologie, pneumologie, pédiatrie, entre autres — et bénéficie d'équipements de pointe, dont un héliport, témoignant de son rôle central dans l'offre de soins du territoire.

Avec 853 lits, il constitue un acteur majeur du système de santé.

Tableau T1			CLASSIFICATION DES DONNÉES																				
Processus métier, domaine applicatif ou domaine d'activité Services communs à particulariser	FONCTION (descriptif)	Sélection si 1	Données applicativ. (bases de données)			Fichiers bureaut.			Inform. Écrite ou imprimée			Courrier postal ou électronique			Archives, document. ou informat.		Données publiées (web ou interne)		Données externalisées sur le cloud		
			D	I	C	D	I	C	D	I	C	D	I	C	D	C	D	I	D	I	C
Types d'actifs =>			D01	D01	D01	D02	D02	D02	D04	D04	D04	D05	D05	D05	D06	D06	D06	D06	D07	D07	D07
Processus métiers																					
Domaine 1 : Administratif		1	4	3	4	2	2	4	2	2	4	3	3	4	4	4	1	2			
Domaine 2 : service medical		1	3	4	4	3	4	4	2	3	4	1	4	4	4	4	3	3			
Domaine 3 : Informatique		1	4	4	4	3	2	3	1	1	1	2	2	3	3	3	1	1			
Domaine 4 : finance		1	2	3	3	2	2	2	2	1	1	2	2	2	3	3	1	1			
Domaine 5 : Logistique		1	3	3	4	3	3	4	2	2	2	3	3	3	3	3	1	1			
Domaine 6 : urgence		1	4	4	4	4	3	3	3	3	4	4	4	4	3	3	3	3			
Domaine 7 : Pharmacie		1	3	3	4	3	3	4	3	4	4	3	4	4	3	4	2	2			
Domaine 8 :		1																			
Domaine 9 :		1																			
Domaine 10 :		1																			
Processus transverses		1																			
Processus 1 :		1																			
Processus 2 :		1																			
Processus 3 :		1																			
Administration/ politique d'ensemble		1																			
Classification d'ensemble			4	4	4	4	4	4	3	4	4	4	4	4	4	4	3	3			
Classification pour les activités sélcionnées			4	4	4	4	4	4	3	4	4	4	4	4	4	4	3	3			

Tableau T2		CLASSIFICATION DES SERVICES ET PROCESSUS								
Processus métier, application ou domaine applicatif Services communs	FONCTION (descriptif)	Sélection si	Services applicatifs			Services externalisés ou hébergés sur le cloud		Services de publication sur site web		Processus de gestion de la conformité	Processus de gouvernance et de prise de décision
			D	I	C	D	I	D	I	E	E
Types d'actifs =>			S01	S01	S01	S02	S02	S03	S03	P01	P02
Processus métiers											
Domaine 1 : Administratif		1	2	3	4			1	2	4	2
Domaine 2 : service medical		1	3	3	4			2	2	4	3
Domaine 3 : Informatique		1	3	3	4			1	1	3	2
Domaine 4 : finance		1	3	3	4			1	1	3	2
Domaine 5 : Logistique		1	3	3	3			1	1	3	1
Domaine 6 : urgence		1	4	4	4			2	4	4	3
Domaine 7 : Pharmacie		1	3	3	3			1	1	4	2

Les processus métiers ont donc été répartis en sept parties afin de simplifier la structure par rapport à notre organigramme :

- Administratif : Regroupe les secrétaires médicales ainsi que le personnel chargé de l'admission des patients dans les chambres.

- Service médical : Comprend la radiologie, la neurologie, la maternité et d'autres spécialités.

- Informatique : Inclut le support technique et les équipes en charge des logiciels annexes (par exemple, le logiciel HM pour centraliser les données patientes et faciliter la coordination entre les services).

- Finance : Concerne les personnes responsables de la gestion des achats de matériel, de logiciels et d'équipements pour l'établissement

- Logistique : Assure la réception des colis, l'envoi d'échantillons (par exemple de sang ou d'organes) et la gestion de la chaîne du froid.

- Urgences : Englobe le centre d'urgence et la prise en charge immédiate des patients.

- Pharmacie : Gère la réception, l'étiquetage et la distribution des médicaments aux patients ou aux différents services.

Thomas GRZESINSKI

Analyse intrasec :

En principe, dans l'hôpital, 90% des données qui circulent sont des données sensibles car elles incluent des données de santé, administratives et de traçabilité soumises au RGPD , tandis que les 10% restantes concernent des informations non sensibles, comme les données d'achats, de logistique ou autres, qui n'ont pas de lien direct avec un patient ou un professionnel de santé.
La majorité de nos processus métiers présentent un niveau 4 en Disponibilité, Intégrité et Confidentialité, car ils manipulent très souvent des données sensibles de santé ou des données personnelles.
À l'inverse, certains éléments sont classés en catégorie 1, comme le site internet de l'établissement, car aucune donnée sensible n'y transite et les informations publiées sont destinées au public (communication externe).
Le logiciel HM permet aux patients de consulter et de récupérer eux-mêmes certaines de leurs données, ce qui renforce la disponibilité de l'information tout en nécessitant des mesures de sécurité adaptées pour protéger l'intégrité et la confidentialité de ces données de santé.

Choix Intrasec :

Pour le T1 ,le choix d’affecter un niveau 4 à la disponibilité, l’intégrité et la confidentialité pour la majorité des processus métiers repose sur la nature même des activités hospitalières. Les services médicaux, les urgences et l’informatique occupent une place centrale dans l’établissement, car ils sont directement liés à la prise en charge des patients et au bon fonctionnement des soins quotidiens. Il serait inconcevable de laisser circuler ou traiter des données sans contrôle strict, car la moindre faille pourrait compromettre la sécurité des informations sensibles, entraîner une perte de chance, ou retarder la prise en charge des malades.
En cas d’incident majeur (ransomware, panne, cyberattaque), la priorité doit être donnée à ces métiers critiques pour assurer la continuité des soins. Il est essentiel que les dossiers patients, les comptes-rendus médicaux et l’accès aux outils informatiques restent disponibles et protégés. Des mesures comme le mode dégradé, le Plan de Continuité d’Activité (PCA) et le Plan de Reprise d’Activité (PRA) seront déployées de manière prioritaire pour permettre aux équipes médicales de poursuivre leur mission, même si des services comme la finance doivent momentanément passer au second plan, l’activité de soin demeurant la raison d’être fondamentale de l’hôpital.

Pour le tableau T2, il apparaît que les processus comme les urgences ou la gestion de la conformité nécessitent impérativement un niveau 4 en confidentialité, car une compromission de ces secteurs mettrait en danger la sécurité des patients ou la conformité légale de l'établissement. Par conséquent, l'accès aux services applicatifs doit toujours être garanti en situation critique, notamment pour pouvoir enregistrer un patient dès son arrivée et recueillir des informations vitales.

Les autres domaines, tels que la logistique ou la pharmacie, bien qu'importants, se voient parfois attribuer un niveau 3 : cela signifie qu'une atteinte à la confidentialité ou à la disponibilité pourrait causer des problèmes, mais n'aurait pas le même impact vital immédiat que pour la prise en charge médicale ou la gestion réglementaire. Les tâches de support peuvent continuer à fonctionner en mode dégradé, tandis que la priorité en cas de crise doit être donnée à la continuité du soin et au respect strict des obligations de confidentialité dans les processus les plus critiques.

Commentaire classif :

Tableau d'Impact Intrinsèque

			D	I	C	E	Sélection d'actifs	Commentaire
Actifs de type Données et informations								
Données et informations								
D01	Données applicatives	Données contenues dans des fichiers ou bases de données utilisés par les appplications	4	4	4		1	
D02	Données bureautiques	Données contenues dans des fichiers personnels ou partagés, incluant les fichiers d'agenda ou de contacts	4	4	4		1	
D03	Informations écrites ou imprimées	détenues par les utilisateurs, archives personnelles, listings et états imprimés issus des applications informatiques, et la documentation des processus et autres actifs pouvant être nécessaire à l'activité.	3	4	4		1	
D04	Courrier électronique ou postal	Courrier électronique, postal ou télécopies	4	4	4		1	
D05	Archives	patrimoniales, documentaires ou informatiques	4		4		1	
D06	Données et informations publiées	sur des sites publics ou internes	3	3			1	
D07	Données externalisées	sur le cloud					1	
Actifs de type Processus (Services)			D	I	C			
Services des technologies de l'information								
S01	Services applicatifs	applications métiers, services bureautiques ou systèmes communs	4	4	4		1	
S02	Services externalisés	ou hébergés sur le cloud					1	
S03	Services de publication d'informations	sur un site web interne ou public	2	4			1	
Processus de management							1	
P01	Processus de gestion de la conformité	aux exigences légales ou contractuelles ou de l'entité				4	1	
P02	Processus de gouvernance et de prise de décision	dans la gouvernance de l'entité (pouvant conduire à un dysfonctionnement redouté) y compris la gouvernance de la sécurité				3	1	

À partir des tableaux de classification, on constate que l'hôpital doit prioriser la protection et la disponibilité de la majorité de ses services informatiques et métiers critiques : la plupart des actifs et processus essentiels (données applicatives, services médicaux, urgences, conformité) affichent systématiquement des valeurs au plus haut niveau (4/4/4), illustrant l'interdépendance et l'importance vitale de ces fonctions. Si un service critique devenait

indisponible ou compromis, il en résulterait un effet domino les autres domaines, fortement connectés, pourraient être affectés à leur tour, mettant en danger la capacité de l'établissement à assurer sa mission de soin et de prise en charge des patients.

Cette stratégie de priorisation s'explique par le fait que les établissements de santé sont particulièrement vulnérables aux cyberattaques pouvant paralyser les systèmes, exposer les données et compromettre la continuité des soins. Par conséquent, les plans de continuité et de reprise d'activité doivent reposer sur cette hiérarchie d'exigences : les métiers les plus critiques doivent rester opérationnels en toutes circonstances, tandis que les fonctions de support pourront être restaurées dans un second temps si nécessaire

Résultat service et sous-services

Après la définition des niveaux pour le questionnaire d'audit portant sur la sécurité des systèmes et de leur architecture, l'exploitation et l'administration des systèmes, ainsi que la protection des postes de travail utilisateurs, nous observons que les services ou questions évalués obtiennent majoritairement des scores de 5 ou de 10, en cohérence avec les restrictions très précises en place.

Sur la mesure technologique, le score est de 10 : l'accès aux ressources et la sécurité sont des points particulièrement sensibles dans notre infrastructure, et la moindre modification ou installation logicielle déclenche une démarche formalisée (réunions, validations) afin de sécuriser les changements et d'anticiper les problèmes potentiels liés aux applications. Pour les mêmes raisons, les mesures organisationnelles présentent également un score élevé, traduisant la présence de processus, responsabilités et contrôles clairement définis en matière de sécurité de l'information

On a cependant un score très faible de 2 et de 4 pour la séparation des environnements de développement, de test et de production ainsi que pour la gestion des changements. Avec les mesures actuellement en place, nous faisons face à une contrainte importante sur les aspects technologiques, où les changements doivent souvent être effectués rapidement en raison de manque de temps ou de budget, ce qui peut engendrer des problèmes potentiels.

Exposition des risques

Les hôpitaux sont exposés à plusieurs risques majeurs en matière de sécurité informatique. Le premier concerne le manque de suivi des mises à jour logicielles, qui crée des vulnérabilités exploitables par des cyberattaques, compromettant les données sensibles. Un autre risque important est l'incendie : même si les salles serveurs disposent d'azote pour couper l'oxygène, un sinistre survenant dans un autre service peut affecter tout l'établissement, provoquant la perte des serveurs et des données critiques. Cette vulnérabilité est renforcée par des contraintes budgétaires post-COVID qui limitent la possibilité de recourir à des prestataires cloud pour les sauvegardes. Pour limiter ces risques, les

établissements s'organisent en groupements hospitaliers de territoire (GHT), ce qui permet de mutualiser les compétences et les connaissances. Le risque biologique est aussi notable : la circulation d'un pathogène pouvant nécessiter un confinement interne constitue une menace pour la continuité des opérations informatiques et des services.

Enfin, un risque d'ingénierie sociale est identifié. En effet, toute personne dans l'établissement, quel que soit son service, pourrait potentiellement introduire une clé USB malveillante déclenchant un ransomware. Ce vecteur d'attaque reste une menace importante à surveiller par des mesures de sensibilisation et des politiques de sécurité internes strictes.

Les risques géographiques identifiés par GEORISQUES comprennent une remontée de nappe existante, un séisme modéré, ainsi que des mouvements de terrain existants. Un retrait-gonflement des argiles est jugé faible, tandis qu'une pollution des sols est concernée. Ces aléas naturels soulignent la nécessité d'évaluer précisément la localisation de l'établissement via les cartes interactives de GEORISQUES pour adapter les mesures de prévention.

Amélioration

4A02	***Protection contre les malwares***	
4A02-01	Une protection contre les programmes malveillants, appuyée par la sensibilisation des utilisateurs concernés, a-t-elle été mise en place ?	1
4A02-02	La protection mise en œuvre permet-elle que l'information et les autres actifs associés soient protégés contre les programmes malveillants.	1
4A02-03	A-t-on défini les actions à mener par le personnel informatique, pour prévenir, détecter et corriger les attaques par des codes malveillants (virus, spyware, autres) ?	x
4A02-04	Les patchs de sécurité publiés par les fournisseurs font-ils l'objet d'une mise à jour systématique tant des serveurs que des postes de travail et des appareils mobiles, et ceci sans délai notable ?	1
4A02-05	Les solutions de protection contre les programmes malveillants sont-elles régulièrement (quotidiennement) et automatiquement mis à jour ?	1
4A02-06	Est-on abonné à une centrale d'alerte permettant d'être prévenu et d'anticiper certaines attaques massives pour lesquelles les antivirus ne sont pas encore à jour ?	1
4A02-07	Existe-t-il une cellule de crise pouvant être mise en place très rapidement en cas d'alerte ou de détection d'infection ?	1
4A02-08	La gestion, l'activation et la mise à jour des solutions de protection contre les programmes malveillants-font-elles l'objet d'un audit régulier ?	0
4A02-09	Les diverses préconisations de la norme ISO 27002:2022 relatives à la protection contre les programmes malveillants ont-elles été prises en compte ?	1

Concernant la protection contre les malwares, nous pouvons constater que nous disposons déjà d'une base solide. Toutefois, certains correctifs peuvent être apportés. En effet, il serait pertinent de définir les actions à mener par le service informatique, éventuellement en faisant appel à un prestataire externe, sachant qu'aucun développeur n'est prévu sur place.

Nous pourrions également nous abonner à une centrale d’alerte afin de renforcer notre veille de sécurité. Par ailleurs, la mise en place d’un audit régulier sur les mises à jour permettrait d’éviter l’installation de logiciels obsolètes et de suivre les applications ainsi que les éventuels correctifs ou patchs déployés. Cela permettrait aussi d’informer nos utilisateurs des problèmes déjà identifiés et corrigés, afin de réduire les appels répétitifs et de gagner du temps dans la résolution des incidents.