GESTION DES DMi ET DM EN CAS DE CYBERATTAQUE : ÉLABORATION D'UN PLAN DE CONTINUITÉ ET DE REPRISE D'ACTIVITÉ (PCRA)

N°23

D. SOULIES, M. JUGAIN, M-A. BAUDONNET

MOTS CLÉS : CYBERMENACE - CIRCUIT - DÉGRADÉ

SERVICE PUI ET STÉRILISATION
Maison de Santé Protestante Bordeaux-Bagatelle - 33400 Talence
pharmaciens@mspb.com

INTRODUCTION

- Selon un rapport de l'ENISA (Agence de l'Union Européenne pour la Cybersécurité), les hôpitaux ont été la cible de 42 % des cyberincidents survenus dans le secteur de la santé de janvier 2021 à mars 2023.
- La survenue d'uneattaque informatique impacte l'ensemble de la continuité d'activité d'un établissement de santé. Coupure exceptionnelle des logiciels de gestion de la PUI, accès aux dossiers patients informatisés impossibles, communications extérieures avec les différents acteurs du circuit des DM rompues, etc. la paralysie est immédiate.
- Dans le cadre de l'organisation des Jeux Olympiques 2024 en France, les établissements de santé identifiés comme essentiels ont l'obligation d'établir un plan d'action en cas de crise cyber. L'un des axes de ce plan est de rédiger, diffuser et promouvoir un PCRA spécifique à chaque service.

OBJECTIFS

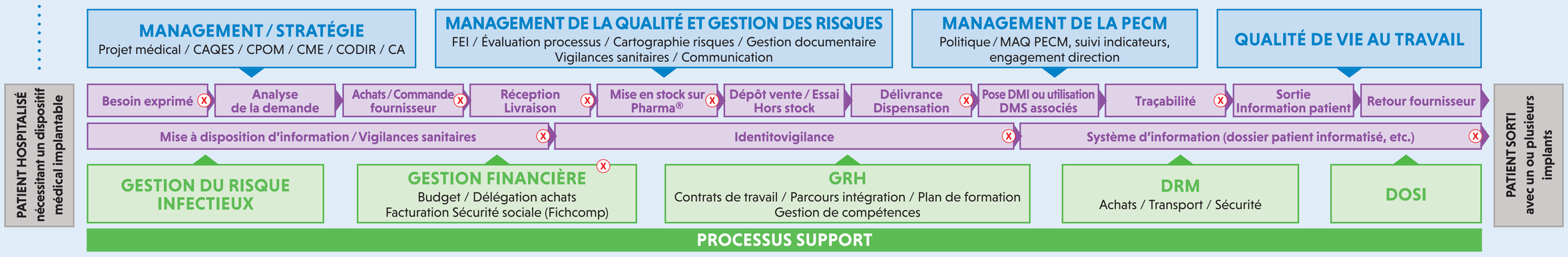
Élaborer des protocoles de gestion du circuit des DM et DMi en mode dégradé afin de garantir la continuité des soins ainsi que la sécurité de la prise en charge des patients, en cas de cyberattaque de l'hôpital.

MATÉRIEL ET MÉTHODES

- Réalisation, en interne, d'un exercice de crise cyber par une société privée qui nous a permis de mettre en pratique les procédures existantes dans le but d'y apporter les modifications nécessaires pour mieux gérer une potentielle cybercrise.
- Mise en œuvre du projet en plusieurs étapes :

1 CARTOGRAPHIE DES PROCESSUS DE GESTION DM ET DMI

Identification des sous-processus impactés par l'arrêt du système informatique



2 ANALYSE GLOBALE DES RISQUES SELON LA MÉTHODE AMDEC

(Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité)
Identification des processus prioritaires à mettre en place, en mode dégradé, selon leur criticité initiale

3 MISE EN PLACE D'UN SYSTÈME DOCUMENTAIRE NON INFORMATISÉ DE SECOURS

- Sur la base de l'analyse des risques et leur niveau de maitrise attribué
- En complément des documents déjà édités et/ou utilisés
- Classé en fonction de l'organisation du circuit des DM et DMi

4 RÉDACTION D'UN PLAN DE CONTINUITÉ ET DE REPRISE D'ACTIVITÉ

Diffusion et formations continues des acteurs concernés

RÉSULTATS

Sur les 10 sous-processus impactés, **4 relèvent d'une**

CRITICITÉ À RISQUE IMPORTANT

Criticité initiale des sous-processus

Faible ***1 à 4*** *Moyenne* ***5 à 10*** *Élevée* ***>11***

CRITICITÉ INITIALE = **PROBABILITÉ DE SURVENUE X GRAVITÉ**

SOUS-PROCESSUS CONCERNÉS ET SOLUTIONS PROPOSÉES

Besoins exprimés / Demande du chirurgien

- Copie papier du Dossier Patient Informatisé
- Prescriptions pré-imprimées
- Communication entre professionnel de santé par des canaux de communications alternatifs

Achat et commande fournisseurs

- Création d'une liste des principaux fournisseurs selon le principe Pareto « 80 % des flux financiers DM et DMi proviennent de 20 % des fournisseurs totaux »
- Demande d'une procédure dégradée de commande aux fournisseurs : constitution d'un répertoire avec les contacts de secours (fax,téléphone,mail)

Renouvellement de dotation / Envoi des demandes aux services et blocs

- Impression papier d'un livret de géolocalisation des stocks pour faciliter le picking
- Renouvellement des dotations des services sur formulaire papier

Facturation : Paiement fournisseurs / Envoi FichComp à la sécurité sociale

- Travail en interface avec le service comptabilité et lemédecin responsable de l'information médicale de l'établissement

DISCUSSION / CONCLUSION

- La liste des documents à conserver sous format papier est **non exhaustive**, et devra être tenue à jour selon les évolutions de gestion de la PUI et devra être facilement accessible en cas de cyberincidents.
- Un travail collaboratif institutionnel entre les différents services de soins et de support de l'hôpital doit être entrepris afin de mettre en commun la gestion de certaines étapes mais également de définir clairement les interlocuteurs référents, pour chaque mission en cas de cyberattaque.
- Limites rencontrées : manque de réponses de certains fournisseurs, démarche récente et novatrice donc peu de recul sur les procédures à mettre en œuvre.

Graphisme : Pierrick Boisard - Juillet 2024