Table ronde :
PUI, faire face à une cyberattaque

Webinaire PUI du 14 avril 2023

Dans la nuit du samedi au dimanche 21 août 2022, le centre hospitalier Sud-Francilien (CHSF) de Corbeil-Essonnes est victime d'un rançongiciel. Moins de 6 mois plus tard, le 3 décembre 2022, c'est, l'hôpital André-Mignot de Versailles (CHV) qui à son tour est frappé par une cyberattaque. Dans les deux cas, l'attaque survient un samedi soir. Aucune rançon ne sera versée.

Services fermés, Patients transférés, soignants désemparés, la paralysie est immédiate. 4 à 10 mois plus tard, les établissements se relèvent difficilement. Une cyberattaque, comme celles vécues au CHSF, Versailles mais aussi aux Bluets, impacte l'ensemble de la continuité d'activité de l'établissement.

Parmi les services hospitaliers, la Pharmacie à usage intérieur (PUI) est un opérateur essentiel. Quel est l'impact de ces cyberattaques sur son activité ? Comment réorganise-t-elle son activité en interne et avec les services ? Enfin, comment s'en prémunir ?

La table ronde organisée le 14 avril 2023 par l'ARS d'Île de France lors du webinaire d'échanges et de retours d'expérience autour de l'organisation et la gestion des risques en (PUI) permet de mieux cerner le retentissement d'une cyberattaque sur l'établissement. Animée par Bénédicte Dragne-Ebrardt, directrice du pôle efficience à la direction de l'offre de soins de l'ARS, les intervenants ont table ronde a réuni :

- *Pour le CHSF : le Dr Marie-Laure MAESTRONI, chef de service PUI et monsieur Patrice GARCIA, directeur du Système d'Information*
- *Pour le CHV, le Dr Farahna SAMDJEE, chef de service PUI - madame Charlotte FORTIN, cadre de la pharmacie et le Dr Sophie RIGAUDEAU, hématologue –*
- *Monsieur Christian LEMAIRE, Chargé de mission numérique et cybersécurité à la direction de l'innovation à l'ARS*

Gérer les premiers temps de l'attaque : pour le système d'information (SI), l'enjeu numéro 1 est d'éviter la propagation

Pour Monsieur Patrice Garcia qui a vécu les premiers temps de l'attaque au sein de l'hôpital CHSF, les premières heures sont cruciales. Peu de signes précurseurs sont apparus hormis une panne initialement considérée comme liée au cœur de réseau. Une fois, la demande de rançon découverte sur le serveur, les premières décisions sont alors rapidement prises : déconnecter tous les câbles pour éviter la propagation, couper le site de l'extérieur, et mettre en place le plan blanc avec une cellule de crise pour mesurer l'ampleur des dégâts. Trois secteurs clés sont identifiés la biologie, la radiologie et la PUI. Les numéros de téléphone à contacter avaient heureusement été sauvegardés. Des cellules de crise de l'ARS et de l'APHP sont mises en place pour aider l'hôpital et organiser l'appui au niveau régional. En parallèle, une cellule de crise informatique avec deux consultants et l'Agence nationales de la sécurité des systèmes d'information (ANSSI), se réunit. Une alerte par circuit papier est mise en place pour interdire de rallumer les ordinateurs.

Pour les soignants, les deux objectifs prioritaires sont de mettre en sécurité les patients et d'assurer la continuité des soins

Pour les soignants, la mise en sécurité des patients et leur information est le premier réflexe adopté. Le Dr Sophie Rigaudeau cite parmi les réponses pragmatiques immédiatement adoptées par le corps médical : des transferts préventifs vers d'autres établissements, la fermeture de certains services et urgences, l'annulation de certaines greffes, et la reprogrammation des consultations et des hospitalisations. Informer et rassurer les patients s'avère incontournable avant que l'incident ne passe dans la presse. Cela concerne également l'information des patients de soins programmés afin de replanifier les rendez-vous.

Pour garantir la continuité des soins, la PUI récupère les sauvegardes des dotations sur les ordinateurs qui ne sont pas touchés par la cyberattaque dans tous les services. Certaines mesures utiles avaient été anticipées : la pharmacie dispose sur un ordinateur de sécurité des sauvegardes des chimiothérapies (logiciel chimio) et des prescriptions (logiciel Pharma). En interne, l'application WhatsApp se révèle bien utile pour communiquer entre les membres du personnel privés d'internet. Les pancartes papier et les formulaires manuels fleurissement. Le soir même de l'attaque, la redistribution des tâches est préparée afin d'avertir et d'organiser le retour des membres du personnel absents le weekend.

Un point essentiel est la solidarité qui est de mise entre les services cliniques et les services support (biologie, radiologie et pharmacie). Toutes les bonnes volontés, y compris l'aide des familles, des conjoints, sont mises à contribution.

En PUI, il faut réinventer les tâches essentielles : le stockage, la distribution, la logistique et les commandes fournisseurs

Le Dr Marie-Laure Maestroni se rappelle de cette la situation difficile en raison de l'indisponibilité des outils numériques habituels, des logiciels de gestion de stock, des automates de stockage, du dossier patient informatisé (DPI), de l'internet et du fax. « En l'espace d'un instant, on s'est retrouvé sans système d'information. C'est-à-dire, qu'on n'avait même pas accès aux médicaments et aux dispositifs médicaux. On n'avait pas de moyen de communication avec les services. Les services ne pouvaient plus faire leur demande de médicaments ou dispositifs médicaux, ils ne pouvaient plus prescrire et on ne pouvait pas non plus faire d'analyse pharmaceutique. […] On n'avait accès à rien du tout. On a décidé de fermer la pharmacie 48h […] et de ne dépanner que les urgences transmises par téléphone.»

La première priorité est de garantir la distribution des médicaments et des dispositifs médicaux. Le stockeur est hors service. Une cartographie des emplacements de stockage et des dispositifs médicaux qui fait défaut est établie. Les listings de dotations des services sont reconstitués et sont créés des formulaires qui viendront remplacer l'informatique pour réaliser les demandes de services. La distribution est organisée sur un fichier excel. Des procédures dégradées de prescription et de distribution des produits de santé sont élaborées. Il faut maintenir la cadence et les équipes sont mises à l'épreuve.

L'apport de l'informatique, lorsqu'il fait défaut, apparait clairement. Heureusement les pneumatiques/tortues qui sont utilisés pour envoyer les demandes des services n'ont pas été endommagés par l'attaque.

La deuxième priorité est de relancer les commandes. Là encore, la situation est complexe : le logiciel de transmission des commandes est inaccessible, avec un changement de marché en cours et l'absence

d'accès aux informations du RESAH qui pénalise la reprise. Les contacts fournisseurs sont récupérés à partir des anciennes commandes papier. Un formulaire pour les commandes vers les fournisseurs est réalisé. Les liquidations de facture sont interrompues jusqu'à ce que plus tard le flux soit rétabli pour sécuriser les approvisionnements.

Les suivis des températures ne peuvent plus être tracés entraînant une mise en quarantaine des médicaments froids et certains médicaments pour essais cliniques. L'historique des patients pour la rétrocession est inaccessible. Au CHSF, les activités de pharmacie clinique, de reconditionnement, de dispensation nominative sont arrêtées sauf pour les médicaments prioritaires, stupéfiants, médicaments remboursés en sus, et à dispensation contrôlée.

La situation génère beaucoup de désorganisation et de stress dans l'exécution des tâches. Les messages clés sont de renforcer la résilience. Pour éviter les erreurs médicamenteuses et rassurer les équipes sur la qualité de leur travail, un contrôle supplémentaire est mis en place.

La présence et la participation aux cellules de crise est essentielle pour la biologie, la PUI et l'imagerie : « il faut se faire entendre » souligne le Dr Marie-Laure Maestroni. Les besoins sont listés au fur et à mesure et sont transmis en cellule de crise. La direction générale écoute les recommandations. Des soutiens sont apportés.

L'apport d'ordinateurs personnels et de connexions internet avec des téléphones portables sont utilisés en urgence. Puis, la récupération d'une clé 4G restaure la communication vers l'extérieur. Travailler sur un ordinateur, en local, connecté à une imprimante est rapidement rendu possible. La récupération des sauvegardes n'est effective qu'au 5ème jour. Des renforts RH internes sont déployés pour aider aux saisies des demandes, et de la facturation, au secrétariat. L'aide est venue également de l'extérieur avec un préparateur et un pharmacien du CH de Melun

Si la première semaine est consacrée à la phase de diagnostic, la deuxième semaine est dédiée au redémarrage progressif de la messagerie et des applications. À 10 jours de l'attaque, dix postes pour la pharmacie sont installés sur un total de 60 en temps normal. Une clé USB est récupérée pour imprimer.

Sans informatique, les activités à risque et la pharmacotechnie doivent être sécurisées par un renfort en personnel

Le Dr Farahna Samdjee du centre hospitalier de Versailles partage l'expérience de son établissement qui dispose d'une Pharmacie 2.0. Dans cet environnement ultra connecté, personne n'avait connu l'époque sans informatique. Si d'anciennes fiches de fabrication papier ont été utilisées au CHSF, cette option est inenvisageable au CHV qui n'en dispose pas. Fort de la cyberattaque survenue 3 mois plus tôt au CHSF, le CHV avait heureusement réalisé une sauvegarde de son logiciel de chimiothérapie qui lui a permis de maintenir à un niveau élevé la production de poches même pendant la crise. Un ordinateur est utilisé pour prescrire et valider les prescriptions. Les médecins viennent prescrire à la pharmacie sur le logiciel de chimiothérapie qui a été restauré en priorité par la DSI. Les équipes ont été doublées pour assurer le contrôle visuel des préparations en l'absence de « DrugCam® ».

Pour les autres activités à risque, la situation est plus critique. En stérilisation, la traçabilité ne fonctionne plus. Une fiche navette papier est utilisée. Pour valider les cycles, se pose la question de récupérer les données des cycles : « C'est un travail qu'on a fait à froid, en amont avec les équipementiers. Ils expliquent comment récupérer un cycle en manuel, le télécharger et le valider avec une procédure pour les équipes qui se retrouvent du jour au lendemain sans leur outil de travail » précise le Dr Farahna Samdjee. Tout s'avère plus compliqué jusqu'à l'impression des étiquettes. « Bien

évidemment le bloc a moins fonctionné, les choix qui avaient été fait en hématologie ont aussi été fait en chirurgie. Il y a des patients qui ne pouvaient plus être pris en charge donc on a fonctionné avec un peu moins de salles, ce qui a aussi permis de limiter l'activité. »

Pour la radiopharmacie, le logiciel n'a toujours pas été remis à jour 4 mois après l'incident. Les prescriptions sont manuelles ou orales. Du renfort en ressources humaines est là aussi indispensable pour compenser l'absence de logiciel et sécuriser l'activité.

Au CHV comme au CHSF, la pharmacie clinique et la préparation des doses à administrer sont interrompues. Le Dr Farahna Samdjee revient sur l'importance d'être solidaires et de maintenir une très bonne communication avec les services cliniques. La PUI est ainsi sollicitée par les internes en médecine qui avaient toujours connu des logiciels d'aide à la prescription pour les aider sur les posologies.

Comme au CHSF, la PUI du CHV est toujours présente en cellule de crise. Le Dr Farahna Samdjee insiste sur le partage de l'information. Il est important dans ces moments d'assurer la transparence avec l'équipe et de mettre en place une organisation : « A chaque retour de cellule de crise (deux fois par jour), on rassemblait tout le personnel, on expliquait où on en était et il fallait rassurer. »

Au sein de l'établissement de Versailles, l'accent a été mis sur la radiologie et la biologie, qui étaient complétement immobilisés. Aucun préjudice initial pour la pharmacie qui avait anticipé mais à distance de l'attaque, la PUI ressent une double peine. Non prioritaire au démarrage, le retard s'est accumulé alors que les activités des autres services qui ont, eux, été accompagnés sont presque restaurés. Un sujet éminemment critique est celui de la gestion économique et financière. Les factures non payées mettent désormais à mal l'approvisionnement par les laboratoires et la récupération de l'historique (facturation, liste en sus ..) va nécessiter des efforts considérables et du temps. Anticiper le rattrapage des données s'avère un enjeu crucial.

Accompagner les équipes et prendre en compte le risque psychosocial

Madame Fortin aborde sans détour la question du retentissement de la cyberattaque sur « le moral des troupes ». L'émotion peut submerger à tout moment. Pour prendre en compte les risques psychosociaux, l'équipe managériale doit être très présente et doit s'adapter. Des messages clairs doivent être donnés en termes de redistribution des tâches. La crise oblige à abandonner certaines missions et à redéployer le personnel sur d'autres activités. L'adaptabilité de tous est nécessaire notamment face aux ordres et contre-ordres qui, sont fréquents à tous les niveaux.

Comment prépare-t-on le retour à la normalité ?

Le retour à la normale est très progressif. Il nécessite des choix stratégiques. Certaines opérations sont à maintenir, d'autres à abandonner temporairement pour dégager des ressources. Le travail est réalisé main dans la main avec le service informatique pour identifier les logiciels incontournables et définir les délais de remise en état. Des sauvegardes hors ligne sont utilisées. Pour madame Fortin qui anticipe la sortie définitive de la crise, l'occasion est peut-être aussi offerte de sortir grandi de cette crise : « Il y a du bon dans le mauvais. On ne met jamais nos PUI à l'arrêt, là on a pas eu le choix, tout s'est arrêté. On va reconstruire différemment parce qu'on apprend aussi de nos erreurs, dans le but d'améliorer et gagner en conditions de travail. »

Au CHSF, la reconstruction du système d'information (SI) a été entreprise par Mr Patrice Garcia en deux phases : la première phase consiste à reconstruire le SI à l'identique, tandis que la deuxième phase implique une mise à jour complète. Pour le CHV, la stratégie a été différente. Il a été choisi d'emblée de reconstruire un nouveau système car celui qui pré-existait ne pouvait pas être remis en

état. Identifier les parties de l'organisation qui n'ont pas été impactées par la cyberattaque devient un enjeu afin d'approfondir la résilience de l'établissement et pour s'assurer de leur continuité dans le futur.

Comment se prémunir face à ce risque ?

Pour gérer les vulnérabilités, des mesures techniques peuvent être mises en place au niveau de la DSI. Elles doivent être accompagnées d'un respect strict des principes de sécurité informatique par le personnel y compris par les prestataires extérieurs. Des solutions full-web sont plébiscitées pour minimiser les risques de cyberattaques.

L'anticipation est essentielle. Des exercices peuvent aider à surmonter les situations de crise. Lister et archiver les documents papiers essentiels, demander des procédures dégradées aux équipementiers,

Au niveau régional, l'ARS se mobilise. La création d'un groupe de travail pour remettre en place des moyens de communication, ainsi qu'un plan pluriannuel de financement national pour faire face à ces risques sont en cours d'élaboration. Chaque attaque est différente, chaque établissement a ses vulnérabilités. Les recommandations portent sur le dénominateur commun en termes de prévention / gestion de crise/ reconstruction.

L'ARS d'Île de France remercie encore le CHSF et le CHV et l'ensemble des participants pour la qualité et la transparence de leur témoignage.

En conclusion, l'anticipation revient en leitmotiv de cette table ronde avec quelques messages clés et des solutions communes qui permettront aux PUI de bénéficier du retour d'expérience du CHSF et du CHV :

1. **Respecter les consignes de sécurité informatique**
2. **Prévoir des sauvegardes hors réseau des logiciels informatiques indispensables et les contacts (numéros de téléphone, mails) des personnes indispensables à contacter**
3. **Prévoir une cartographie du système de stockage des produits de santé**
4. **Demander des procédures dégradées et manuels aux fabricants de tous les équipements de la PUI**
5. **Inscrire la PUI dans la liste des systèmes essentiels en cas de cyberattaque**
6. **Choisir des équipements full-web si possible**
7. **Rédiger des modes dégradés organisationnels de la PUI sur une longue durée, suivant différents scénarii, en cas de perte partielle ou totale du SI (ne pas oublier la collecte des éléments de facturation dès le début de la crise)**
8. **Faire des exercices pour se préparer en interne à la PUI, de manière transversale avec les autres services, et coordonnée avec la cellule de crise**
9. **Prévoir dans les marchés, des modes dégradés de commandes auprès des fournisseurs**
10. **Préparer des kits de communications vers les services, la cellule de crise, les prestataires, voire établissements clients ou membre du GHT**

En cas d'attaque :

1. **Enclencher le plan blanc**
2. **Débrancher du réseau (maintenir l'alimentation électrique) l'ensemble des systèmes informatiques afin d'isoler l'attaque**

3. **Analyser l'ampleur des dégâts (ce qui fonctionne et ce qui ne fonctionne pas)**
4. **Demander de l'aide : ANSSI, ARS, ES du territoires etc**
5. **Récupérer les sauvegardes des logiciels informatiques et tester l'intégrité**
6. **Appliquer la méthode de communication décidée en cellule de crise aux professionnels des services**
7. **Mettre en place des procédures dégradées de prescription et de distribution des produits de santé, de commande auprès des fournisseurs, et maintenir la collecte des éléments de facturation**
8. **Prendre en compte les risques psycho-sociaux des professionnels et instaurer une bonne communication au sein de l'équipe et entre les équipes**
9. **Anticiper le redémarrage et le rattrapage des données (y compris celles de facturation)**