Premiers résultats d'une analyse conjointe FOH et cyber sécurité d'une cyberattaque en milieu hospitalier

Nora Oufi, Cecilia DE LA GARZA, Jingxuan MA, Franck Bouzon, Nicolas LOT

Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Premiers résultats d'une analyse conjointe FOH et cyber sécurité d'une cyberattaque en milieu hospitalier

OUFI Nora
CNAM
41, rue Gay Lussac, Paris
Nora.oufi@edf.fr

DE LA GARZA Cecilia
EDF Lab Paris-Saclay
7, BD Gaspard Monge cecilia.de-la-garza@edf.fr

MA Jingxuan
EDF Lab Paris-Saclay
7, BD Gaspard Monge
jingxuan.ma@edf.fr

BOUZON Franck
EDF Lab Paris-Saclay
7, BD Gaspard Monge
franck.bouzon@edf.fr

LOT Nicolas
EDF Lab Paris-Saclay
7, BD Gaspard Monge
Nicolas.lot@edf.fr

Résumé — Nous proposons une approche pluridisciplinaire pour l'analyse d'une cyber-attaque associant les FOH et des experts de la cybersécurité. L'analyse s'intéresse aux différentes phases de gestion d'une crise cyber dans un hôpital : le diagnostic, la gestion à différents niveaux et par différents acteurs et compétences, la reprise de l'activité. Le but est de mettre en évidence la résilience organisationnelle d'un hôpital face à une cyber-attaque, ainsi que les difficultés et limites rencontrées, en vue de renforcer la prévention et la gestion d'une future cyber-attaque dans le milieu hospitalier.

Mots-clefs — hôpital, cyber-attaque, facteurs humains, cybersécurité, résilience

Abstract— We propose a multidisciplinary approach for the analysis of a cyberattack involving HOF's and cybersecurity experts to focus on diverse phases of management of a cyber crisis in the hospital: diagnosis, management at different levels and by different actors and skills, business resumption. The aim is to highlight the organizational resilience of a hospital facing a cyberattack and its difficulties and limitations in order to make feedbacks to strengthen the prevention and management of a future cyberattack in the hospital environment.

Keywords — hospital, cyberattack, human factors, cybersecurity, resilience

I. INTRODUCTION

Dès 2020, pendant la pandémie, les établissements de santé ont connu un accroissement important d'incidents en termes de cyber-attaques. D'ailleurs, en 2021 celles-ci ont doublé. Les experts en sécurité informatique de l'Agence du numérique en santé (ANS) déplorent 730 incidents (Le Figaro, 15 février 2022) [1]. Ces cyber-attaques ont des conséquences diverses, dont certaines très graves :

- Un risque de décès des patients ;
- L'impossibilité d'accueillir et de dispenser les soins nécessaires aux patients ;
- Un fonctionnement en mode dégradé nécessitant des adaptations, engendrant une charge de travail accrue des personnels, et pouvant durer plusieurs semaines ;
- Une reprise d'activité pouvant nécessiter des mois selon la gravité de la cyber-attaque ;
- Des impacts émotionnels sur les personnels hospitaliers du fait d'un choc, d'une charge de travail plus importante, de la modification des activités, etc.
- Des coûts économiques pouvant être très élevés pour récupérer les données médicales et remettre les activités en service.

Analyser ces événements et comprendre les failles du système socio-technique comme les points forts ayant permis de faire face est donc primordial en termes de prévention.

Intégrer la prise de risque cyber dans le quotidien et réfléchir à un cumul de risques sont des enjeux stratégiques pour la maîtrise des risques et un avenir durable dans ce monde numérique en pleine expansion. Or, lorsqu'il s'agit de sécurité numérique, les recommandations sont généralement axées sur des moyens d'endiguer « l'erreur humaine », partant du principe que l'humain est le maillon faible au sein de la chaîne de cybersécurité. Bien que certains biais cognitifs ou biais de jugement puissent mener à des comportements potentiellement délétères s'agissant de la sécurité numérique, cette conception est réductrice.

Ces considérations renvoient, d'une certaine manière, aux travaux de Brangier, Hammes-Adelé et Bastien, 2010 [2] qui abordent de façon critique les approches opératoires de l'interaction homme-machine. Ces auteurs invitent à compléter cette perspective par la prise en considération des aspects organisationnels dans la relation entre l'Homme et la Machine. Ainsi, nous proposons une approche systémique et empirique dépassant le cadre de l'erreur humaine centrée exclusivement sur l'individu. En effet, dans le domaine de la

sécurité industrielle celle-ci a largement été dépassée, car la prévention nécessite d'aller au-delà pour être efficace [3]. Le but est alors de comprendre les contextes d'utilisation des systèmes interactifs, les contextes dans lesquels ces cyberattaques surviennent et leurs conséquences. Une approche compréhensive de la cybersécurité nécessite d'identifier les différents personnels impliqués dans la conception des Systèmes Interactifs (SI) à la gestion d'une cyberattaque, en passant par les situations d'utilisation des outils informatiques. Ainsi, organisation du travail et activité doivent être prises en compte du fait de leurs potentiels impacts sur les différents utilisateurs des SI.

De même, Weber et Commandant [4] invitent à prendre en considération *« le poids des cultures professionnelles* » dans les interactions entre les travailleurs et les outils numériques, considérant les effets que ces dernières font peser sur les comportements, les prises de décision et les capacités d'adaptations. Cette notion renvoie également à la culture de sécurité qui, en fonction du type d'organisation, prendra des formes différentes en termes de prévention et de gestion des risques liés à la sécurité.

Nous proposons en outre, une approche pluridisciplinaire pour l'analyse d'une cyber-attaque associant les FOH et des experts de la cybersécurité pour s'intéresser aux différentes phases de gestion d'une crise cyber à l'hôpital :

- Le diagnostic de la cyber-attaque ;
- Le pilotage de la crise par différents acteurs ;
- La gestion des impacts i.e., l'identification des conséquences pour les personnels soignants et les patients et le fonctionnement en mode dégradé ; l'anticipation dans le milieu hospitalier de ce type d'événement.

Dans la partie suivante, nos propos sont illustrés par un cas concret, en cours d'analyse en milieu hospitalier, qui a cumulé en 2021 la crise sanitaire et une cyber-attaque.

II. Gestion d'une cyberattaque en milieu hospitalier

Dans cette partie nous allons illustrer comment la cyber-attaque a été identifiée, prise en charge et gérée par différents acteurs.

A. Diagnostic

Il s'agit d'une cyber-attaque qui a eu lieu en 2021. Elle a été identifiée durant la nuit en début d'année 2021. Dans un premier temps, elle s'est manifestée comme une « panne » au niveau du standard téléphonique : les téléphones et ordinateurs ont cessé de fonctionner. L'alerte a été donnée au service informatique d'astreinte qui a rapidement identifié un fichier connu des informaticiens, ayant pour extension «.*ryk*». Ce fichier est associé au ransomware Ryuk, à l'origine de plusieurs cyberattaques dans les établissements de santé. Une fois sur place les informaticiens diagnostiquent une cyber-attaque totale, impactant l'intégralité des données. En outre, le système de sauvegarde avait été chiffré. Peu d'activités restaient possibles. L'ensemble du personnel l'a rapidement compris : « *c'était le black-out total en dix min…* ». Le service informatique a alors coupé Internet et interdit aux personnels d'utiliser leurs ordinateurs pour éviter une propagation du virus.

B. Pilotage de la crise

Du point de vue du pilotage de la crise, la cellule de crise s'est montée dans la nuit, un dialogue constant et une coordination ont été mis en place entre le service informatique et la direction de l'hôpital pour s'organiser face à la cyberattaque.

En parallèle de cette cellule de crise sont intervenues d'autres entités : l'ANSSI, la Cellule cyber défense de l'opérateur téléphonique et l'ARS, la préfecture et la police.

Cette crise a été d'autant plus difficile à gérer pour l'établissement de santé, qu'elle se cumulait avec la crise sanitaire, présente depuis pratiquement un an. Les personnels étaient sous tension face un manque de ressources humaines et à une gestion quotidienne des lits les mettant parfois dans des situations « d'impasse » comme certains l'ont formulé.

C. Impacts sur les soins et le suivi des patients et stratégies mises en place

Un des problèmes principaux a été de ne plus avoir accès aux données médicales des patients ni à l'agenda. Il était donc impossible de savoir pourquoi les gens venaient à l'hôpital, pour quel soin ou quelle intervention chirurgicale. Des interventions ont donc été déprogrammées et des patients ont été redirigés dans d'autres hôpitaux. Un axe critique a été la radiothérapie concernant les patients atteints de cancer, dont le traitement ne doit pas être interrompu, ces patients ont dû être transférés dans d'autres hôpitaux.

Pour illustrer les impacts, nous citerons ici les principaux identifiés au travers de nos premières analyses dans le service des urgences :

- Perte totale des communications et des moyens informatiques.
- Plus de moyens de gestions des flux de patients entrants et sortants de l'hôpital, qui devait se faire manuellement : un passage donc au « tout papier ».
- Difficultés à transcrire et assurer la complétion exhaustive des documents d'admission et de suivi aux urgences sur papier.
- Allongement du temps de retour des bilans faits aux urgences et qui permettent de guider les soins : il fallait 5h pour avoir un bilan sanguin, par rapport à 1h habituellement, situation qui a duré un mois et demi.
- Rallongement du temps de prise en charge des patients.
- Une seule console de radiologie utilisable pour tout l'hôpital : beaucoup d'attente pour faire passer les radios, accumulation des comptes rendus de radio et ce pendant 4 mois.
- Plus de radiothérapie possible et plus de possibilités de prendre de nouveaux patients.
- Annulation de la programmation au bloc opératoire, car impossibilité d'utiliser les machines à stériliser (cette situation a duré une vingtaine de jours).
- Impossibilité de passer des commandes en pharmacie.
- Impossibilité de gérer la logistique (commande de repas, de matériel...).

D. Adaptations et construction de nouveaux modes opératoires pour assurer une continuité d'activité

Les personnels ont dû trouver des stratégies à tous les niveaux pour faire face à la cyberattaque. Des stratégies adaptations individuelles et collectives ont été construites sur-le-champ. Celles-ci témoignent de formes de résilience organisationnelle de l'hôpital en fonctionnement en mode dégradé. Les exemples suivants rendent compte de ces pratiques et stratégies déployées pour assurer néanmoins une continuité de l'activité, ou du moins de certaines activités.

Du point de vue du pilotage, quatre points peuvent être signalés.

- Création de cellules de crises institutionnelles.
- Une communication de crise dans les médias pour signaler l'incapacité de l'hôpital à prendre en charge des malades afin de limiter le nombre de patients aux urgences.
- La cellule de crise et les services identifiaient les tâches prioritaires au jour le jour.
- Mise en place d'une cellule de crise « dynamique » au sein des services (par exemple, 3 fois par semaine dans le service des urgences).

Du point de vue de la gestion de la crise par les services opérationnels, quatre exemples retiennent notre attention.

- Les personnels des différents services se sont échangé leurs numéros de portables et ont créé des groupes WhatsApp pour pouvoir communiquer rapidement.
- Ils ont établi une mailing liste sur les ordinateurs personnels pour pouvoir communiquer entre services.
- L'usage de post-it pour le suivi du parcours des patients au sein de l'hôpital ou des tableaux Veleda pour traduire l'architecture du service, sont des exemples de stratégies pour pallier l'absence d'informatique.
- Des radiothérapeutes se sont déplacés avec les patients dans d'autres hôpitaux et ont géré de mémoire les doses et pathologies afin de ne pas interrompre les traitements.

E. Facteurs de résilience pour la gestion d'une crise

Nous pouvons constater d'un point de vue des Facteurs organisationnels et Humains, des facteurs de résilience facilitant la gestion de crise. Il est intéressant de les signaler, car ils ne sont pas propres à la gestion d'une cyberattaque, mais ils ont été observés auparavant dans la gestion de la crise sanitaire et nucléaire par exemple [5]. Nous en citerons cinq :

- Réactivité des personnels à tous les niveaux : décisions opérationnelles rapidement mises en place pour assurer les soins dans les meilleurs délais et conditions.
- Engagement et solidarité des personnels (cf. l'exemple des radiologues cité ci-dessus).
- Mobilisation collective pour la mise en place de solutions avec des réussites et des échecs, et ce pendant plusieurs mois, afin que la prise en charge des patients se passe au mieux.
- Expérience des personnels, qui a eu des impacts à différents niveaux. D'une part, certains services, comme les urgences, ont une expérience des situations critiques et inattendues, ce qui permet le développement de compétences à la gestion de crise. D'autre part, l'expérience de médecins plus anciens qui a favorisé l'établissement de certains diagnostics sans avoir des résultats de bilans ou autres, facilitant la prise en charge des patients dans des délais plus courts.
- La solidarité des autres hôpitaux a permis le transfert et la prise en charge de patients au niveau des urgences et d'autres services de médecine.

Cette étude nécessite d'être finalisée, mais d'ores et déjà l'analyse en cours du fonctionnement en mode dégradé est riche d'enseignements et témoigne d'une résilience organisationnelle de l'hôpital dont il est intéressant de faire un retour d'expérience pour mieux prévenir et renfoncer les organisations de crise par rapport aux crises cyber. Dans cette résilience entre peut-être en ligne de compte un sentiment de révolte exprimé par certains des personnels : « *comment on peut faire ça à une population* ? » Autrement dit, c'est ce sentiment, entre autres, qui les a aidés à trouver la force de faire face à une situation aussi dégradée.

Les résultats montrent des similitudes avec la crise sanitaire qui ont été étudiées de façon plus approfondie [4]. Une crise cyber comme une crise sanitaire sont toute les deux des crises longues et qui concernent tout le personnel de l'hôpital et peuvent mettre en cause les soins envers les patients.

Aussi, les deux crises, pour des raisons différentes, nécessitent une réorganisation des activités et le transfert des patients dans d'autres hôpitaux. La gestion des flux et des lits reste un enjeu fort dans les deux cas, en interaction avec les ressources humaines, techniques et matérielles disponibles au sein de l'hôpital.

Dans les deux cas, l'expertise et l'expérience de certains personnels apparaissent comme un facteur de résilience individuel et collectif.

F. Facteurs de difficulté

Si l'hôpital a pu faire face à cette situation critique, il ressort néanmoins que les personnels ont rencontré des difficultés importantes qu'il faudrait approfondir dans la suite de nos analyses. Nous en citerons quatre dans ce papier.

- Le patient a été un peu « perdu de vue ». En effet, le suivi avec du papier et des post-it n'est pas simple. Un patient pouvait se retrouver dans un box et sans identification, car le personnel soignant était tellement sollicité qu'il n'avait pas le temps de tout gérer correctement. Aussi, il y a eu des moments où cela a été difficile de savoir exactement qui rentrait et sortait de l'hôpital. Il semblerait que rien ne soit prévu pour un fonctionnement en mode dégradé à l'hôpital.
- A posteriori, certains personnels considèrent qu'il n'y a pas eu assez d'informations diffusées à la presse pour informer la population locale des difficultés rencontrées par l'hôpital et pour ainsi éventuellement diminuer le nombre de passages par jour, notamment aux urgences, et ce pendant une période longue.

- Des difficultés pour les personnels et des impacts pour les patients : au-delà du fait que les personnels soignants étaient déjà très fatigués, cette crise accroît considérablement leur charge de travail et a eu pour effet de créer des tensions supplémentaires. La prise en charge des patients est beaucoup plus longue, ceux-ci s'accumulent et doivent patienter. Les personnels médicaux travaillent un peu « *à l'aveugle* » comme ils l'ont exprimé et doivent prendre des décisions importantes pour le patient.
- Le pilotage, pour certaines tâches, était toujours porté par la même personne. Au sein de la cellule de crise, il n'y avait pas de « relève » par exemple, ce qui n'est pas tenable dans la durée.

Dans la suite de l'étude, il s'avérera intéressant d'explorer aussi bien avec les personnels soignants qu'avec les experts cyber, les moyens pour faire faire face à ce type de difficultés. Il s'agirait, par exemple, soit de limiter les impacts, soit d'anticiper des ressources spécifiques pour ces types de situations en mode de fonctionnement dégradé.

III. PERSPECTIVES EN TERMES DE PREVENTION

Dans cette partie seront discutés deux approches complémentaires pour renforcer la cybersécurité : l'approche d'experts cyber et celle d'experts FOH.

A. Renforcer la cybersécurité

Selon l'Agence du Numérique en Santé et le Ministère des Solidarités et de la Santé [9], en 2021 les incidents de cybersécurité déclarés par les établissements de santé ont pratiquement doublé par rapport à 2020. Par ailleurs, il arrive que des structures soient des victimes collatérales d'incidents de prestataires, eux-mêmes directement victimes d'attaques par rançongiciel. En effet, des prestataires peuvent être contraints d'interrompre leur service pour répondre à l'incident, mais aussi pour bloquer toute propagation de l'attaque vers le SI de leurs clients.

a.1. Ryuk et son déroulement habituel

Le rançongiciel Ryuk au centre de cette attaque est un malware apparu en 2018 responsable de nombreuses attaques en 2019 et 2020, notamment dans le secteur de la santé de différents pays (*France, États-Unis, Canada, etc.*). L'objectif principal de Ryuk, comme tous autres rançongiciels, est d'empêcher la victime d'accéder à ses données pour des raisons lucratives, le plus souvent par le chiffrement des données.

Ryuk peut rester inactif pendant plusieurs mois avant de se déclencher [6], cependant, le délai le plus court observé entre l'infection initiale et la fin du déploiement est de 2h avec l'ensemble des objectifs atteints en 3h [8].

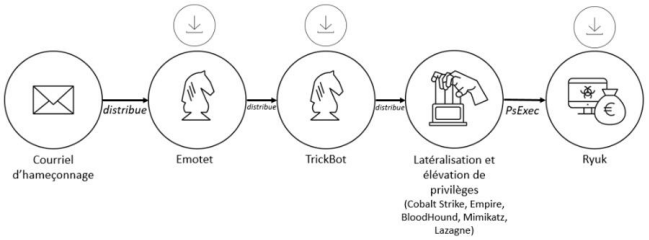

Figure 1 : déroulement simplifié d'une attaque par rançongiciel [7]

Le déroulement [Figure 1] le plus souvent de cette attaque est le suivant : l'attaque commence par l'ouverture d'une pièce jointe piégée ou la consultation d'une page web malveillante provenant d'un mail d'hameçonnage (Phishing) qui délivrera un malware « Loader » comme Emotet ou TrickBot. Le loader distribue/installe ensuite des outils pour obtenir des accès privilégies, comme BloodHound, Mimikatz. Une fois des accès privilégies obtenus, le rançongiciel sera téléchargé et déployé au sein du système d'information de sa victime. Une fois activé/déclenché, Ryuk recherche des machines ayant des partages réseau et tente de monter de volumes réseau aux machines identifiées. Il parcourt ensuite la table ARP[1] de sa victime et envoie à chaque machine un paquet « Wake-On-LAN [2]» pour allumer les postes éteints sur le réseau afin d'accroître la surface d'attaque. Il se propage alors automatiquement sur toutes les machines joignables avec les accès RPC [3] Windows, arrête de nombreux processus légitimes (*sécurité, accès à distance, accès aux serveurs de base de données pour empêcher la prise en main du service IT de la victime*), encrypte les fichiers, détruit toutes les copies présentes sur le système (*pour empêcher la restauration*) et demande une rançon. Il peut créer également à distance une tâche planifiée pour s'exécuter sur cet hôte.

Généralement, les opérations de Ryuk sont identifiables dans des journaux réseau et de la machine.

a.2. Constats et hypothèses d'un point de vue cyber

Basés sur les premières informations de cette attaque, quelques constats et hypothèses d'une perspective cybersécurité sont mis en avant dans le tableau 1.

TABLEAU 1 : LES PREMIERS CONSTATS ET HYPOTHESES DU POINT DE VUE CYBERSECURITE

Constats	Hypothèses
Une « Panne » technique au service « Standard » constatée durant la nuit	Ce DoS[4] au standard signifie que le début de l'attaque commence au moins quelques heures plus tôt.
L'alerte signalée au service informatique d'astreinte après le constat de la panne technique	Faille dans la gestion ou configuration des événements de sécurité des journaux réseaux/postes/serveurs
	Ignorance sur les alertes
	Moyens d'alerte non efficace
L'attaque par Ryuk identifiée rapidement par le service IT Le système de sauvegarde a été également chiffré	La signature de l'attaque par Ryuk est évidente, mais elle n'a pas été mise dans les règles de détection
	La signature de l'attaque par Ryuk a été mise dans les règles de détection, mais le moyen d'alerte inefficace
	Le serveur de sauvegarde est sur la même segmentation réseau

[1] ARP : Address Resolution Protocol

[2] Depuis octobre 2019, Ryuk dispose d'une fonctionnalité lui permettant d'allumer les postes éteints présents sur le réseau local (Wake-on-LAN) afin d'accroître sa surface de chiffrement.

[3] RPC : Remote Procedure Call

[4] DoS : Déni de service

	Le système de sauvegarde est en connexion permanente aux systèmes de données « vives »
	Manque de filtre de flux réseau pour le système de sauvegarde
	Manque de durcissement sur le système de sauvegarde
Une seule console de radiologie utilisable	La connexion de cette console avec la machine est dans une segmentation de réseau isolée
	La connexion de la console avec la machine est une connexion physique point à point et sans centralisation de données aux serveurs
Échange de numéro de portables entre les services	Toutes les communications fix internes sont via VoIP[5]
Utilisation de WhatsApp pour communiquer	WhatsApp étant une application américaine, l'échange de données médicales peuvent engendrer d'autres crises par exemple du fait de la fuite de données suite à une violation du RGPD
Une mailing liste entre les ordinateurs personnels	Aucun moyen informatique professionnel fonctionnel
	Pas d'accès web aux mails professionnels
L'attaque via des accès VPN compromit [9]	Vulnérabilité de VPN non corrigée
	Usurpation d'identité légale

a.3. Des mesures de renforcement de cybersécurité

Les premiers constats et hypothèses synthétisés dans le tableau précèdent nous conduisent à proposer les mesures de renforcement de cybersécurité, complétant les recommandations de l'ANSSI [8] afin d'augmenter la résilience du système d'information et réduire le risque d'infection et de propagation de ce type d'attaque :

- Diversifier les technologies utilisées en termes de supports informatiques en mettant en place par exemple, les tablettes Android, des serveurs de sauvegarde sous Windows et/ou linux etc., notamment pour les services critiques ;
- Segmenter le réseau par zones de sensibilité et d'exposition aux risques ;
- Attribuer des droits d'accès aux besoins strictement nécessaires des utilisateurs (postes de travail, zones réseau, etc.) ;
- Sensibiliser régulièrement les utilisateurs aux risques numériques ;
- Clarifier les périmètres et responsabiliser ;
- Tenir une vigilance particulière à la surface d'attaque provenant de la chaîne de confiance : prestataires, fournisseurs de logiciels, etc.

Les rançongiciels utilisent souvent les accès Internet des entités pour communiquer avec une infrastructure hébergée en ligne par les cybercriminels. En naviguant sur un site web compromis, un collaborateur pourra sans le savoir télécharger et provoquer l'installation automatique du programme malveillant sur son poste de travail.

- En parallèle des moyens de communication VoIP, mettre en place également des moyens de communication mobiles et des lignes téléphoniques physiques et les entretenir régulièrement ;
- Mettre en place de moyens d'alerte plus efficace ;
- Sensibiliser les personnels aux cyber-attaques notamment à l'hameçonnage (Phishing) qui est la première phase de différentes cyber-attaques et les premiers gestes en cas d'une cyber-attaque ; effectuer des campagnes de sensibilisation régulièrement et sous différents formats ;
- Automatiser les filtrages et blocages de tous mails suspects dans des serveurs dédiés et effectuer systématiquement une analyse ;
- Distinguer et restreindre les droits d'accès aux utilisateurs strictement nécessaires sur les postes et zones segmentés ;
- Prévoir une segmentation réseau par zone de sensibilité et d'exposition aux risques ;
- Réaliser les sauvegardes de données régulièrement sur les moyens de support informatiques diversifiés et durcis, qui sont hébergés dans des segmentations différentes de réseaux, avec des moyens installés pour détecter l'intrusion et filtrer le flux réseau ;
- Effectuer des analyses des virus des données (logiciels compris) provenant d'un tiers dans un serveur dédié sur une segmentation réseau isolée avant les intégrer dans le système d'information.

B. Renforcer l'organisation de crise et la gestion d'une crise cyber

L'analyse en cours de cet évènement permet d'envisager quatre niveaux de prévention à investiguer avec la cybersécurité.

- *La conception des systèmes d'information*. Il s'agit de réfléchir à comment introduire la sécurité pour minimiser les actions considérées comme des « erreurs » de la part de l'utilisateur final non professionnel de l'informatique. D'une certaine manière, il est intéressant d'explorer le concept de tolérance à l'erreur utilisé dans d'autres systèmes. Autrement dit, que l'utilisateur final soit averti que son action est peut-être risquée, ou bien qu'elle puisse être annulée.
- *La gestion du risque dans le quotidien*. Divers points sont à étudier en lien avec les pratiques des différents utilisateurs et leurs connaissances des risques. La sensibilisation est en effet un des leviers, mais pas le seul. La sécurité informatique est parfois vécue comme une contrainte supplémentaire, et ce d'autant plus si la charge de travail est importante. Du point de vue organisationnel, la pression temporelle et une charge de travail accrue sont des facteurs pouvant favoriser une action inadéquate de la part d'un utilisateur, ou au contraire la non-réalisation d'une action importante de sécurité. Ce dernier point peut concerner différentes catégories d'utilisateurs, voire les responsables de l'informatique également.
- *La gestion d'une crise cyber*. En effet, les cyberattaques vont continuer de se produire, il faut donc envisager comment limiter leurs impacts d'une part, et comment pouvoir continuer à assurer la continuité de service d'autre part. Se préparer à

[5] VoIP : Voice over Internet Protocol

fonctionner en mode dégradé est tout aussi important, et cet évènement permet de commencer à réfléchir à ce point.

- *L'établissement de plans de reprise d'activité* qui nécessitent également d'être anticipés et qui devront d'être adaptés certainement. Mais une base de travail est indispensable.

Enfin, en fonction des types de cyberattaque, d'autres modalités de prévention doivent pouvoir être considérées, car ce type de virus n'est qu'une forme d'attaque parmi d'autres. Dans la suite de nos travaux, nous investiguerons ce domaine de façon plus large.

IV. CONCLUSION

Une des premières leçons qu'il est possible de tirer, à la suite de ce début d'analyse de cyberattaque au sein de l'hôpital, est l'importance du contexte dans lequel la cybercrise survient, car celui-ci peut avoir des effets sur la gestion de celle-ci ou sur l'aggravation d'une crise préexistante. Par ailleurs, l'importance du contexte dans lequel s'inscrit une cybercrise peut être à la fois un facteur explicatif d'une attaque ou la conséquence d'une situation existante. Dans l'exemple exposé dans le cadre de cette communication, la cyberattaque lancée à l'encontre de cet hôpital pourrait être une conséquence de cette perception de fragilisation du système par les attaquants du fait de la pandémie de COVID19. De même, il ne serait pas erroné de considérer que la situation de crise rencontrée par l'hôpital au moment du COVID19 ait accaparé les ressources et les préoccupations de l'organisation, ce qui aurait potentiellement eu pour effet une fragilisation du système au niveau de sa cyber sûreté.

Le renforcement de la cyber sûreté passe donc *a minima* par trois axes. En premier lieu, une prise en considération de la potentielle fragilisation du système informatique lors de la survenue d'autres crises. Des éléments de surveillances et des stratégies d'adaptation seraient potentiellement salutaires dans ces contextes pour éviter les cumuls de crises.

En deuxième lieu, le renforcement de la gestion de la cybercrise passe par des éléments d'anticipation. Ces éléments consisteraient, d'abord, en la prise de conscience par l'organisation des risques de cyberattaques qui sont parfois méconnus ou négligés et où les services chargés d'assurer cette sécurité disposent de très peu de moyens pour y faire face.

Enfin, le renforcement de la gestion de la cybercrise passe également par la prise en considération du fait qu'un système technique reste néanmoins faillible, ce qui invite les organisations à repenser l'adaptabilité de leurs organisations en cas de cyberattaque. En effet, les attaquent potentiellement graves sont souvent celles qui n'ont pas été anticipées. L'identification de fonctions informatiques clés permettant la continuité des activités et la construction collective de solutions palliatives en cas de perte de ces fonctions est une des démarches qui peuvent être prises par les organisations en vue de développer leur résilience en cas de cyberattaque.

Pour conclure, si l'hôpital a été vu comme une cible privilégiée par les attaquants, celui-ci n'a pas payé la rançon. L'hypothèse faite de la part des attaquants est probablement que l'hôpital, déjà fragilisé par la crise sanitaire, aurait de toute façon besoin des données des patients pour la continuité de l'activité en termes de soins. La réalité des faits montre que l'hôpital est toujours debout et a réussi à faire face, à maintenir une continuité d'activité et mettre en place un plan de reprise d'activité. Aucun décès lié à la cyberattaque ne peut être déploré. Certes, le coût est élevé pour les personnels soignants déjà très fatigués, voire « usés » par la crise sanitaire. Il est donc crucial de mieux protéger les établissements de santé des cyberattaques et de mieux anticiper les fonctionnements en mode dégradé.

REFERENCES

[1] Le Figaro. « *Les cyberattaques contre les établissements de santé ont doublé en 2021* ». Publié le 15/02/2022. https://www.lefigaro.fr/secteur/high-tech/les-cyberattaques-contre-les-etablissements-de-sante-ont-double-en-2021-20220215 (consulté le 4/05/2022)

[2] E. Brangier, S. Hammes-Adelé, and J-MC Bastien. "Analyse critique des approches de l'acceptation des technologies: de l'utilisabilité à la symbiose humain-technologie-organisation." *European review of applied psychology* 60.2 (2010): 129-146.

[3] E. Fadier, and C. De la Garza. "Towards a proactive safety approach in the design process: The case of printing machinery". *Safety science* 45(1-2): 199-229.

[4] C., Weber, et J-P., Commandant. « De l'importance du facteur humain », Stéphane Taillat éd., La Cyberdéfense. Politique de l'espace numérique. Armand Colin, 2018, pp. 52-59.

[5] C. De la Garza, and N. Lot. « The socio-organizational and human dynamics of resilience: the COVID 19 crisis management in a hospital », *Journal of Contingencies and Crisis Management*, (2022) in press.

[6] ZDNet. « *Ryuk : Un ransomware qui détonne* ». Publié le 01/12/2020. https://www.zdnet.fr/actualites/ryuk-un-ransomware-qui-detonne-39914041.htm (consulté le 20/05/2022)

[7] The DFIR Report. « *Ryuk Speed Run, 2 Hours to Ransom* ». Publié le 05/11/2020. https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/ (consulté le 20/05/2022)

[8] ANSSI. « *CERTFR-2020-CTI-011 : Le rançongiciel Ryuk* ». Publié le 30/11/2020. https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-011/ (consulté le 20/05/2022)

[9] Agence du Numérique en Santé. « *Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé* ». Publié le 21/04/2022. https://esante.gouv.fr/sites/default/files/media_entity/documents/mss_ans_rapport_public_observatoire_signalements_issis_2021_vf.pdf (consulté le 20/05/2022)