Médecine de Catastrophe - Urgences Collectives 2024;8(1):8–11

Communiquer dans une situation dégradée : se préparer à une cyber-attaque

Communicating in a compromised situation: Preparing for a cyber-attack

Mathieu Raux [a]
Nicolas Lot [b]

[a] *Département d'anesthésie-réanimation, site Pitié-Salpêtrière, groupe hospitalier universitaire, AP–HP, GRC29, Sorbonne université, 75013 Paris, France*
[b] *R&D Lab, Paris-Saclay, boulevard Gaspard-Monge, 91120 Palaiseau, France*

RÉSUMÉ

On désigne par cyber-attaque l'intrusion au sein d'un système d'information (SI), dans le but de voler des données puis d'encrypter les fichiers et serveurs, avant de demander une rançon en échange de la remise de la clef de décryptage. Pareille crise au sein d'un hôpital provoque immédiatement une paralysie totale et très prolongée. Cette paralysie vient de l'incapacité à accéder aux données médicales mais aussi de fonctionnement de l'hôpital comme de l'incapacité à communiquer, car les canaux numériques habituels ne peuvent plus fonctionner. Il n'existe pas de plan de prévention commun à tous les hôpitaux. Chaque établissement de santé doit identifier ses propres besoins. Ce travail d'identification ne peut être effectué que par les acteurs de terrain, coordonnés par une cellule ad hoc. Ceci garantit une parfaite conformité aux exigences des services et directions, et d'autre part permet de faire appel à l'intelligence collective de celles et ceux qui utilisent l'outil informatique au quotidien, en connaissent les failles et ont une idée de comment s'en sortir le jour où le SI dysfonctionne. La poursuite de l'activité en cas d'incapacité du SI impose de pouvoir accéder aux données indispensables au fonctionnement, et donc d'avoir pensé, en amont de la crise, aux moyens de les rendre accessibles. Une partie des données non confidentielles peut être sauvegardée. Les données médicales, désormais dématérialisées, peuvent être remises au patient sous forme papier ou numérique dans « mon espace santé ». Certaines données peuvent être stockées sur les serveurs sécurisés des fournisseurs de matériel. La communication orale passe par l'utilisation de réseau 4/5G, malheureusement souvent difficilement accessible au sein des bâtiments modernes. Ce même réseau permettra de connecter des ordinateurs portables à internet au moyen de clefs adaptées, autorisant l'utilisation d'outils collaboratifs hors SI. La communication par messagerie instantanée doit respecter la confidentialité des données. Ces dernières ne peuvent être transférées que par des applications certifiées pour cet usage. Le recours à la messagerie ordinale permet d'échanger des données médicales en toute sécurité. Les patients et usagers seront informés au moyen des réseaux sociaux, des médias, des institutions, des associations d'usagers, des communautés professionnelles territoriales de santé.

MOTS CLÉS

Cyber-attaque
Communication
Sauvegarde
Plan de continuité d'activité

KEYWORDS

Cyber-attack
Communication
Backup
Continuity plan

SUMMARY

A cyber-attack is an intrusion into an information system (IS), with the aim of stealing data and then encrypting files and servers, before requesting a ransom in exchange for handing over the decryption key. Such a crisis in a hospital immediately leads to total and prolonged paralysis. This paralysis stems from the inability to access medical data, but also from the hospital's inability to communicate, as the usual digital channels can no longer operate. There is no common

Auteur correspondant.
M. Raux,
Département d'anesthésie-réanimation, Hôpital Pitié-Salpêtrière, SSPIAP, 47-83, boulevard de l'Hôpital, 75651 Paris cedex 13, France.
Adresse e-mail :
mathieu.raux@aphp.fr

doi:10.1016/j.pxur.2024.01.002

prevention plan for all hospitals. Each hospital must identify its own needs. This identification work can only be carried out by the stakeholders in the field, coordinated by an ad hoc unit. This guarantees perfect compliance with the requirements of departments and divisions, and also makes it possible to call on the collective intelligence of those who use IT tools on a daily basis, are familiar with their shortcomings and have an idea of how to get out of them on the day when the IS malfunctions. If operations are to continue in the event of IS incapacitation, it is essential to be able to access the data that is essential to operations, and therefore to have thought, in advance of the crisis, about how to make it accessible. Some non-confidential data can be saved. Medical data, now dematerialized, can be given to the patient in paper or digital form in "my health space". Some data can be stored on the secure servers of equipment suppliers. Oral communication requires the use of a 4/5G network, which is unfortunately often difficult to access in modern buildings. The same network can be used to connect laptops to the Internet using appropriate keys, enabling the use of non-IS collaborative tools. Instant messaging must respect data confidentiality. Data can only be transferred using applications certified for this purpose. Medical data can be exchanged in complete security using the professional messaging system. Patients and users will be kept informed by means of social networks, the media, institutions, user associations and local healthcare professional communities.

INTRODUCTION

Les cyber-attaques constituent, avec l'incendie et la panne électrique, l'un des risques les plus importants qui pèsent sur les établissements de santé (ES). Cette menace procède de l'extrême vulnérabilité de leurs systèmes d'information (SI), de la facilité à opérer dans l'ombre avec la quasi-certitude de ne pas être identifié, de la valeur des données contenues dans les SI et de l'impact majeur sur les capacités de résilience sanitaire, impact pouvant être recherché par un groupe terroriste ou dans le cadre d'un conflit hybride. La question qui se pose aux gouvernances de nos ES n'est plus « si » mais « quand surviendra une cyber-attaque ? ». Il leur appartient donc de prendre les dispositions pour minimiser la survenue de ce type de catastrophe, que ce soit via des mesures de protection numériques (matérielles ou d'hygiène informatique) ou la préparation d'un plan de continuité d'activité.

CYBER-ATTAQUE ET CONSÉQUENCES SUR LA COMMUNICATION

Les cyber-attaques sont menées par des *hackers* ou pirates, qui recourent à des logiciels disponibles sur le *darknet*. Après avoir identifié une cible, dans le cas présent un ES, ils cherchent à en pénétrer le SI, le plus souvent à l'aide d'un des personnels de cet ES. Ce personnel, en ouvrant malencontreusement un mail de *phishing*, devient complice des pirates, malgré lui. Après avoir cartographié le système d'information, le pirate copie des données qui lui serviront une fois l'attaque lancée, à exercer une pression sur l'équipe de direction en vue d'obtenir le paiement d'une rançon. Pendant cette phase, la plupart du temps indétectable, le pirate réplique le logiciel d'encodage sur l'ensemble des serveurs. Ces logiciels seront activés à un moment où les moyens de sécurité informatique sont les plus faibles (en soirée et jour de week-end). Il s'ensuit un encodage de l'ensemble des serveurs, et par voie de conséquence, une inaccessibilité du SI. Après quelques signaux faibles, rendant difficile le diagnostic de cyber-attaque, le SI s'interrompt. Cette interruption est en général suivi d'une demande de rançon de la part des pirates. Comme preuve de leur maîtrise du SI, ces derniers peuvent exhiber à la direction du site concerné quelques éléments de dossiers médicaux comme preuve de leur maîtrise de la situation. Cette preuve cherche à exercer une pression psychologique sur les équipes de direction dans le but de les inciter à payer la rançon demandée par les pirates en échange de la clef de déchiffrement. Par ailleurs, ces données pourront être blanchies, c'est-à-dire anonymisées avant d'être revendues via des *data-brokers*. Une cyber-attaque est donc constituée de deux phases : la première parfaitement silencieuse qui précède une phase clastique de blocage immédiat, total et très prolongé du SI et de ce qui en dépend (téléphonie, messagerie, applications internes, etc.).

IDENTIFICATION DES BESOINS

Les conséquences d'une cyber-attaque sur le fonctionnement d'un établissement diffèrent selon l'architecture informatique de ce dernier. Il n'existe pas de plan de continuité d'activité générique, c'est-à-dire commun à tous les établissements de santé. De fait, la rédaction du plan de continuité d'activité (PCA) doit être précédée d'une identification précise des besoins propres à l'établissement. Cette identification des besoins ne peut être opérée que par un personnel de terrain. Ce personnel associe des experts des différents corps de métiers ayant en charge les unités permettant le fonctionnement de l'hôpital (service, pharmacie, laboratoire, direction, etc.). Pour ce faire, ces personnels doivent identifier les étapes du parcours de soins ou du *process* de direction nécessitant, pour leur réalisation, l'informatique ou un produit de l'informatique. Ces éléments sont colligés dans un tableur. Pour chaque étape, ils identifient : le ou les logiciels utilisés ; leur perception de la criticité de cette étape ; une description de la solution utilisée ou connue en cas de panne ; et des propositions de ce qu'il conviendrait de faire en cas de panne prolongée ou de solution non prévue. En faisant appel à une intelligence collective de terrain, cette approche maximalise les chances de produire un PCA conforme aux exigences de la mission de l'ES.

Ces mêmes binômes procèdent à un inventaire et à une priorisation des besoins, qu'il s'agisse de besoins informatiques (matériel, licence, etc.), bureautiques ou téléphoniques. Dans ce domaine, ils évaluent la couverture réseau au sein des bâtiments, souvent insuffisante. Ils créent des groupes de discussion activables en cas de cyber-attaque au moyen d'applications communes (WhatsApp, Signal, etc.). Notons que ces applications ne doivent pas être utilisées pour l'échange de données confidentielles, a fortiori médicales.

SAUVEGARDE ET ACCÈS AUX DONNÉES

Un certain nombre de données doivent être sauvegardées afin de pouvoir être récupérées et utilisées pendant la crise. Malheureusement ces processus de sauvegarde sont chronophages et à risque de corruption comme de vol. Pour finir, ils doivent utiliser des moyens cohérents avec ceux qui seront disponibles pendant la cyber-attaque donc ne pas sauvegarder sur le SI. Il existe schématiquement deux modalités de sauvegarde. La première d'entre elles est la sauvegarde sur papier, à l'image de ce qu'étaient les dossiers médicaux avant déploiement des SI. S'il n'est pas cohérent de revenir au tout papier c'est-à-dire de reconstituer en totalité un dossier avec des pochettes en carton là où il a disparu, il semble pertinent de le réserver à des besoins particuliers comme les hôpitaux de jours en oncologie ou les maternités. Compte-rendu et courriers devront être remis aux patients afin qu'ils soient toujours accessibles, y compris lorsque les dossiers papiers seront stockés et inaccessibles. Au-delà des données purement médicales, certaines informations de fonctionnement devront être sauvegardées sur papier comme les plannings de personnel et de soins, les annuaires, les formulaires, les inventaires, etc. La seconde modalité est une sauvegarde sur support numérique. Il est inenvisageable de stocker ces données sur un support matériel tel qu'une clé USB ou un disque dur externe en raison du risque de corruption et de vol de ces supports. L'application nationale « mon espace santé » permet le stockage sécurisé de sauvegardes de données médicales au format numérique [1]. Ces sauvegardes peuvent être opérées de manière automatique par les SI, qui seront paramétrés pour envoyer automatiquement des éléments jugés pertinents vers ce coffre-fort numérique accessible aussi bien par les patients que par ces médecins et le SAMU. Cette application dispose par ailleurs d'une messagerie sécurisée permettant les échanges de données médicales avec les médecins. Les données non médicales pourront être sauvegardées sur des supports numériques sécurisés non connectés au système d'information, comme les plateformes institutionnelles de partage de documents, les *clouds* des fournisseurs (radiologie, biologie, dialyse, imagerie, etc.) ou les outils collaboratifs pour peu qu'ils soient déjà utilisés hors crise.
Si l'accès aux données au format papier ne pose pas de problème pendant la cyber-attaque (à condition qu'elles ne soient pas stockées dans un endroit inaccessible), l'accès aux données numériques nécessite de disposer d'outils de communication permettant un ordinateur portable non infecté de se connecter à l'application « mon espace santé », ainsi que d'une imprimante permettant leur matérialisation. En l'absence de ces outils, le patient consultant ou se rendant aux urgences peut aisément accéder à son espace santé à l'aide de son smartphone. Certaines données sauvegardées sur des outils institutionnels tels qu'un SI miroir pourraient être récupérées au moyen d'une procédure ad hoc.

COMMUNICATION

La communication téléphonique se fait au moyen de téléphones portables personnels ou professionnels. Comme mentionné, précédemment le principal écueil est l'architecture des bâtiments qui se comportent comme de parfaites cages de Faraday, rendant certaines pièces imperméables aux signaux téléphoniques. La persistance de téléphone analogique au sein des hôpitaux, a fortiori dans ces pièces « blanches », permet de garantir la résilience des moyens de communication, en particulier s'agissant des lignes permettant de transmettre une demande de prise en charge d'urgence vitale.
Les informations non confidentielles peuvent être échangées au moyen des outils collaboratifs choisis par l'ES, par des boîtes mails commerciales et enfin des messageries instantanées. N'étant pas protégés, ces outils ne doivent pas être utilisés pour échanger des données confidentielles. L'échange de données confidentielles peut se faire par téléphone ou au moyen d'une boîte mail sécurisée. Les Ordres de santé (médecins, pharmaciens, infirmiers, sage-femmes, dentistes, etc.) mettent à disposition un système de messagerie sécurisée gratuite autorisant l'échange de données entre professionnels de santé et avec le patient [2]. Cette messagerie nécessite une inscription ordinale. Il existe par ailleurs des messageries instantanées labellisées « hébergeur de données de santé » qui peuvent être utilisées pour échanger des informations confidentielles et a fortiori médicales en cas de cyber-attaque.
La communication vers les patients nécessite de disposer de leurs coordonnées mail ou téléphonique. Elle nécessite par ailleurs de dédier du temps de secrétariat pour passer les appels téléphoniques, envoyer des messages textes ou des mails. Cette communication vers les patients peut revêtir un caractère collectif. Elle peut ainsi être réalisée via les communautés dont les contacts sont préalablement identifiés comme les médias, les réseaux sociaux, les institutions, les mairies, les associations de patients et les communautés professionnelles territoriales de santé (CPTS).

CONCLUSION

Une cyber-attaque induit une crise brutale totale et très prolongée. La préparation de l'ES à ce type d'événement impose une évaluation précise des besoins par les personnels de terrain. Ce qui n'a pas été prévu avant ne pourra être réalisé pendant, justifiant l'anticipation de sauvegardes et l'utilisation de moyens de communication robustes à la cyber-attaque. La réponse de l'institution impose l'utilisation d'outils permettant de garantir la sécurité des transferts de données en particulier médicales. L'ensemble de ces mesures ne constitue que le socle de la réponse, laquelle devra être adaptée par la cellule de crise hospitalière aux exigences de la crise.

Déclaration de liens d'intérêts
Mathieu Raux est chargé de mission à l'Assistance publique–Hôpitaux de Paris, en charge de la rédaction du plan de cyber-résilience hospitalière de l'AP–HP. Il est par ailleurs responsable pédagogique au sein

de la faculté de santé Sorbonne université d'un programme de formation des directrices et directeurs médicaux de crise à se préparer à une cyber-attaque au sein d'un établissement de santé.
Nicolas Lot est membre du COPIL plan de cyber-résilience hospitalière de l'AP–HP. Il est par ailleurs enseignant pédagogique du programme de la faculté de santé Sorbonne université de formation des directrices et directeurs médicaux de crise à se préparer à une cyber-attaque au sein d'un établissement de santé.

RÉFÉRENCES

[1] Mon espace santé. https://monespacesante.fr. Dernier accès le 26 décembre 2023.
[2] Mailiz. La messagerie sécurisée Santé. https://mailiz.mssante.fr. Dernier accès le 26 décembre 2023.