CYBERATTAQUES DES HÔPITAUX
QUELLES CONSÉQUENCES POUR LES PATIENTS ?

Vincent Trely

Fondateur et président de l'Association pour la sécurité des systèmes d'information de santé

« Les cyberattaques mettent en péril la prise en charge des patients »

Lorsqu'un virus rentre dans le système informatique d'un hôpital, il bloque tout et plus rien ne fonctionne. Ce sont alors des centaines de médecins, d'infirmiers, d'aides-soignants qui n'ont plus accès aux données de suivis des patients : constantes, comptes rendus médicaux, prescriptions de traitements en cours... Cela désorganise complètement l'organisation des soins. Les urgences ne peuvent plus accueillir de patients et des interventions chirurgicales sont déprogrammées. Les moniteurs, les respirateurs ou les pompes à perfusion des patients notamment en réanimation et en néonatalogie, sont généralement gérés par des ordinateurs. En cas d'attaque, il faut donc vite transférer ces patients très vulnérables dans d'autres hôpitaux. Si les pirates ne cherchent pas à tuer, ces cyberattaques peuvent mettre en danger les malades et entraîner des décès. Face à ce péril, les professionnels de santé hospitaliers s'entraînent pour pouvoir réagir rapidement et efficacement. Et, la prévention s'organise afin d'assurer la sécurité des systèmes et empêcher et déjouer les attaques.

Gilles Calmes

Directeur du Centre hospitalier Sud francilien et du Centre hospitalier d'Arpajon, victime d'une cyberattaque, le 20 août 2022

« Une crise qui mobilise toutes les équipes et fait appel à la solidarité entre hôpitaux »

Les premières mesures prises dans la nuit du 20 août, dès le constat de la cyberattaque, ont bien entendu porté sur la sécurité des soins. Nous avons très vite décidé de transférer les patients instables ou qui nécessitaient des soins critiques spécifiques vers les autres hôpitaux dans notre territoire de santé. Ce fut notamment le cas pour certains services spécialisés de périnatalité franciliens qui ont accueilli les nourrissons hospitalisés en réanimation et en soins intensifs de néonatalogie, 48 heures après le déclenchement du plan blanc. Cette solidarité interhospitalière nous a permis de garantir la sécurité des soins durant cette période. Au plus fort de cette crise, nos urgences et tous les soins programmés en hôpital de jour ainsi que l'activité de notre bloc opératoire lourd ont pu être assurés grâce à la résilience de nos professionnels. Il a en effet fallu que tous s'adaptent. Par exemple, des équipements ont été commandés en urgence tels des CD permettant de partager les résultats d'imagerie ou encore des équipements pour délocaliser certains examens de biologie.

En France, en 2022, une dizaine d'hôpitaux et centres hospitaliers ont été victimes d'attaques informatiques mettant en péril des informations aussi vitales que sensibles. Mais, quels sont concrètement les risques pour les patients ? Nos experts font le point.

Propos recueillis par Laure Dasinières

Charles Blanc-Rolin

Chef de projet sécurité numérique en santé au GCS e-santé Pays de la Loire

« Il existe des risques d'usurpation d'identité »

Si plusieurs attaques ont été relayées par les médias ces derniers mois, le phénomène n'est pas nouveau. Toutefois, les pirates vont de plus en plus loin et leur principale motivation est l'argent. Lorsque les rançons qu'ils demandent ne sont pas payées, ils peuvent publier les données qu'ils récupèrent et/ou les vendre au détail. Parmi ces données, il y a souvent les coordonnées bancaires mais ce n'est pas le plus problématique. En effet, les bases de données des hôpitaux hébergent aussi et surtout toutes les informations qui relèvent de l'état civil des patients dont le numéro de Sécurité sociale ainsi que des photocopies de carte Vitale ainsi que de papiers d'identité et des photos. Il y a aussi le numéro de téléphone, l'adresse e-mail ou postale. Ce sont des informations qui se monnayent et qui peuvent conduire à des arnaques et à des usurpations d'identité. En outre, les pirates peuvent également essayer de revendre à des banquiers, à des assureurs ou à des cabinets de recrutement peu scrupuleux les dossiers médicaux des patients contenant des informations confidentielles.

CYBERATTAQUES quels hôpitaux ont-ils été touchés en 2022 ?

Deux autres attaques ont été déjouées en décembre 2022 : l'une au Centre hospitalier d'Argenteuil et l'autre, au CHU de Nice.

ANNÉE 2022

7 janvier Léonard de Vinci de Chambray-lès-Tours	**19 avril** Hôpitaux de Saint-Dizier et de Vitry-le-François	**12 septembre** Hôpital de Cahors
12 janvier Cité sanitaire de Saint-Nazaire	**27 mai** Centre hospitalier de Mâcon	**9 octobre** Maternité des Bluets, Paris
28 mars Hôpital de Castelluccio, Ajaccio	**20 août** Centre hospitalier de Corbeil-Essonnes	**3 décembre** Hôpital André Mignot, Versailles

QUE FAIRE si je suis concerné ?

Si vous avez consulté ou été hospitalisé dans un hôpital victime d'une cyberattaque, celui-ci est tenu de vous avertir afin que vous puissiez prendre vos dispositions.

- Redoublez de vigilance face aux tentatives de d'hameçonnage *via* des e-mails ou des SMS frauduleux (par exemple, faux courriel de votre médecin ou de l'Assurance-maladie). Ne répondez pas à ces messages.
- Suivez l'activité des comptes associés à votre numéro de Sécurité sociale et changez vos mots de passe.
- Si vous craignez être victime d'une usurpation d'identité, rendez-vous sur le site cybermalveillance.gouv.fr pour obtenir des conseils et portez plainte rapidement auprès d'un commissariat de police ou d'une gendarmerie.

RUDY BURBANT POUR SANTE MAGAZINE – EKATERINA CHEMAKINA / STOCK.ADOBE.COM