FUTURA

Paralysé par une cyberattaque, cet hôpital français refuse de payer la rançon

Podcast écrit et lu par Emma Hollen

[*Générique d'intro, une musique énergique et vitaminée.*]

Un hôpital paralysé par des pirates virtuels, c'est l'actu de la semaine, dans Vitamine Tech.

[*Fin du générique.*]

Dix millions de dollars, c'est la somme que des pirates ont récemment réclamée au Centre hospitalier de Corbeilles-Essonne. Mais si leur ransomware a bel et bien paralysé les services de l'hôpital, ce dernier ne semble pas prêt pour autant à céder au chantage.

[*Une musique électronique calme.*]

Dans la nuit de samedi à dimanche dernier, une cyberattaque a frappé le Centre hospitalier sud francilien, ou CHSF, situé à Corbeil-Essonnes. D'abord prise pour une panne, c'est lorsque la demande de rançon de 10 millions de dollars est tombée que la direction a dû se rendre à l'évidence que l'hôpital venait d'être victime d'une attaque de ransomware (ou rançongiciel), une application malveillante déployée par les hackers pour paralyser les systèmes informatiques. Celle-ci en l'occurrence a eu pour effet de bloquer complètement l'accès aux logiciels métiers de l'hôpital, aux systèmes de stockage (entre autres d'imagerie médicale) et aux services permettant d'enregistrer les nouvelles admissions. Le personnel se voit donc obligé d'en revenir au papier et au stylo pour conserver la trace des patients entrants. Le centre hospitalier fonctionne actuellement en mode dégradé, notamment au niveau des urgences adultes, pédiatriques et gynécologiques, et un plan d'urgence baptisé « plan blanc » a dû être enclenché pour tenter de gérer au mieux l'afflux de nouveaux patients, dispatchés désormais vers d'autres hôpitaux. L'Autorité Nationale en matière de Sécurité et de Défense des Systèmes d'Information – plus connue sous le nom d'Anssi – a été pour sa part saisie par la cellule de crise du CHSF, et la section cybercriminalité du parquet de Paris enquête d'ores et déjà pour retrouver la trace des criminels. Une chose est sûre en tout cas, l'hôpital ne cédera pas au chantage. Outre le fait que son statut d'établissement public l'en empêche, Medhy Zeghouf, président du conseil de surveillance du CHSF, affirme dans les colonnes du Parisien qu'il serait tout bonnement contre-productif de payer cette rançon. Bien que cette décision soit entièrement justifiée, elle signifie du même coup qu'il faudra sûrement des semaines pour remettre les systèmes informatiques du centre hospitalier sur pied. L'hôpital n'est pas pour autant laissé à la merci des hackers. Cette attaque n'est en effet pas la première de son genre parmi les établissements de santé, et une procédure a été aussitôt mise en place par l'Agence régionale de santé (ou ARS)

pour soulager le CHSF dans cette période de crise. Mais aider les hôpitaux une fois l'attaque survenue ne sera pas suffisant pour garantir leur sécurité sur le long terme et risque de coûter malgré tout une petite fortune à l'État.

[*Virgule sonore, une cassette que l'on accélère puis rembobine*.]
[*Une musique de hip-hop expérimental calme*.]

Confrontées à des situations similaires, des villes comme Annecy, La Rochelle ou encore Dax avaient elles aussi fait le choix de ne pas céder au chantage des hackers. Et cette décision, bien que moins coûteuse que le versement intégral d'une rançon, n'avait pas été sans impact financier. Ainsi l'attaque informatique perpétrée contre l'hôpital de Dax en 2021 avait occasionné des frais estimés à 2,3 millions d'euros. Pris en charge par l'ARS Nouvelle-Aquitaine, il fallait compter sur 174.000 euros d'investissements matériels pour reconstruire le réseau, 546.000 euros pour les prestations en cybersécurité et les réinstallations, mais aussi et surtout 1,48 million d'euros engagés sur le plan humain, avec les renforts et les heures supplémentaires engendrés par tous ces dysfonctionnements. À l'époque, il avait fallu des mois pour que le service fonctionne à nouveau normalement. Dans un cas comme dans l'autre, les hôpitaux sont donc perdants face à ces attaques et malheureusement, l'avenir ne promet pas d'amélioration puisque le dernier rapport d'Avast fait état d'une augmentation de 42 % des attaques par ransomware en France. Fin 2021, l'Anssi révélait aussi que le nombre de cyberattaques avait été multiplié par quatre en un an, et que le système de santé restait une cible privilégiée des hackers. Enfin, au-delà de la paralysie des systèmes d'informations qui met bien souvent en danger la vie des patients, la fuite des données médicales à caractère individuel reste une préoccupation majeure face à laquelle les établissements de santé devront apprendre à s'armer. On souhaite au centre hospitalier de Corbeil-Essonnes un prompt et rapide rétablissement et aux spécialistes en cybersécurité bien du courage pour les années à venir.

[*Virgule sonore, un grésillement électronique*.]

C'est tout pour cet épisode de Vitamine Tech. Si ce podcast vous plaît, n'hésitez pas à nous retrouver sur vos applications d'écoute préférées pour vous abonner et ne manquer aucun épisode à venir. Cette semaine j'en appelle aux auditeurs et auditrices qui nous écoutent sur Podchaser : n'hésitez pas à nous laisser une note et un commentaire pour nous dire ce que vous pensez de ce format. Pour le reste, je vous souhaite à toutes et tous une excellente soirée ou une très bonne journée et je vous dis à la semaine prochaine, dans Vitamine Tech.

[*Un glitch électronique ferme l'épisode*.]