Société | Cyberattaque : un « rançongiciel » perturbe durablement l'hôpital de Dax

Dans la nuit de lundi à mardi, les systèmes d'information du centre hospitalier de Dax ont été piratés, réduisant à l'écran noir le matériel informatique et impactant la prise en charge des patients. L'activité reprend progressivement mais le retour à la normale pourrait prendre plusieurs jours ou semaines. Le parquet de Paris, compétent en matière de cybercriminalité, a été saisi.

Les urgences continuent à fonctionner quasi-normalement, les soins en unité Covid et réa aussi, et les vaccinations se poursuivent. Le laboratoire et la pharmacie marchent, eux, en modes dégradés, sans conséquences notables sur les patients. En chimiothérapie, les séances sont toujours réalisées mais avec des décalages. Au bloc opératoire, sauf urgences, les activités programmées ont dû être annulées jusqu'à la fin de semaine. Spécialité la plus impactée : la radiothérapie avec quelque 70 patients qui ont été - et seront dans les prochains jours - réorientés sur les centres de Bordeaux, Bayonne ou Pau.

Arrivé le 1er février, le directeur par interim du CH de Dax, Michel Glanes, a tenu à saluer « la réactivité et le professionnalisme de toutes les équipes » ainsi que « l'élan de solidarité régionale » qui permettent aux patients de ne subir « aucune perte de chances » dans leur parcours de soin.

Aucune rançon ne sera payée

Pour faire face à cette cyberattaque apparue par un message en français sur les ordinateurs avec demande de rançon (le montant est resté secret), l'hôpital de Dax, en lien avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI), a fait appel à un prestataire spécialisé en cybercriminalité, Orange Cyberdefense. Mais la remise en état du système pourrait prendre « plusieurs jours ou semaines », a prédit Gilbert Martin, responsable des systèmes d'information du CH de Dax, sans « aucune certitude qu'il ne puisse pas y avoir d'autres attaques ou des rebonds » entre temps.

Pointant la « barbarie ignoble de personnes qui attaquent, en pandémie mondiale, un site hospitalier », Benoît Elleboode, directeur général de l'Agence régionale de santé (ARS), l'a assuré : « aucune rançon ne sera payée, car cela ne garantit pas de récupérer les codes et ça ne ferait qu'inciter les pirates ».

La logique du « rançongiciel », un type de logiciel malveillant qui avait déjà paralysé le CHU de Rouen en 2019, est de pénétrer le système, de chiffrer les données avant de tenter d'extorquer de l'argent en échange de la promesse d'un retour à la normale.

En attendant d'en venir à bout, le message des autorités est clair : « toutes les nouvelles prises en charge

d'urgences seront maintenues, soit sur place soit en étant transférées vers d'autres établissements ». Quant à ceux qui ont des rendez-vous prévus à l'hôpital, mieux vaut passer un coup de fil avant de venir, toutes ces données ayant été effacées par les cyberpirates.

Julie Ducourau

Crédit Photo : JD

Publié sur aqui.fr le 12/02/2021
Url de cet article