© Istock

**Les données de santé valent de l'or, comment les protéger ? A l'Université de la e-santé, des experts ont débattu autour de la cybersécurité.**

« *C'était le 31 mars à 4h. Les équipes asiatiques ont détecté l'intrusion. La première réaction a été de bloquer le périphérique, les accès internet. On voit les serveurs qui s'éteignent. On sait que quelque chose de grave se passe mais on ne sait pas dans quelle mesure. A 6h30 on a décidé de tout couper* », se souvient Olivier Siegler, Directeur Digital, Orga & Process, Système d'Information des laboratoires Pierre Fabre, qui ont été victimes d'une cyberattaque. Avant d'ajouter : « *c'est un réveil que je ne souhaite à personne* ».

Pierre Fabre a décidé de tout reconstruire, quitte à mettre plus de temps pour redevenir opérationnel. « *On était en train de cloisonner le système d'information. Le pirate a pu diffuser assez largement car ce n'était pas encore cloisonné, on était focalisé sur la protection périmétrique mais une fois que l'on a pénétré le serveur, il est facile de lancer du cryptage. Là, on a cherché un cloisonnement, si on est piraté, seul un petit bout tombe* », ajoute Olivier Siegler qui précise que repenser l'architecture d'un système est un travail colossal. Avant d'ajouter : « *la sécurité 100% n'existe pas, le cloisonnement permet de limiter l'impact* ».

Et pour cause, cette attaque de grande ampleur n'est pas un exemple isolé et les cas se multiplient à grande vitesse : Villefranche-sur-Saône, Dax, Arles… Les cas ont fait la Une ces derniers temps. « *Il faut expliquer aux gens que la donnée de santé est une donnée qui vaut de l'or. Et on ne met pas une pièce d'or à disposition dans la rue. Là c'est la même chose* », lance Vincent Templier, responsable de la sécurité des systèmes d'informations (RSSI) au CHU de Montpellier. Il rappelle que les soignants n'ont pas toujours conscience de leur rôle dans cette cyber-chaîne. « *Leur préoccupation principale, c'est de soigner. Au niveau culturel, il faut*

*que cela évolue. La sécurité est un frein au fonctionnel, mais si on le fait ce n'est pas de gaieté de cœur, mais pour protéger les établissements. On travaille sur deux aspects, la protection technique et le changement culturel.* »

Problème : tous les établissements n'ont pas les mêmes moyens à accorder à cette mise aux normes. Des structures étatiques sont alors là pour les accompagner « *avec des guides de bonnes pratiques, des échanges réguliers, et un soutien s'ils sont victimes d'un incident* », assure Charlotte Drapeau, cheffe de bureau à l'Anssi. « *La cybersécurité est l'affaire de tous, c'est important de sensibiliser les usagers aux risques du numérique pour garantir la sécurité au plus proche du patient. Une organisation est en place grâce aux actions du ministère de la Santé, on collabore quasiment quotidiennement. Il est important d'avoir une coordination au niveau national puis au niveau local.* »

Et chez nos voisins européens ? Le Dr Saif Abed travaille au NHS. Il se souvient de l'attaque massive subie par les hôpitaux anglais en 2017. « *L'accent a été mis par le NHS sur l'organisation de l'hôpital en cas d'attaque, on a insisté sur la continuité et non la protection. Si les gens ne sont pas prêts à réagir en cas d'attaque, ça ne sert à rien d'investir dans de super logiciels. Si un système s'écroule, il faut pouvoir quand même s'occuper de nos patients.* » Pour ce médecin britannique, « *la perte de confidentialité ne tue pas mais la perte de continuité des soins, oui.* »

Une vision qui ne trouve pas forcément écho au sein de la table ronde. « *On voit là une différence culturelle. On considère en France que si, la perte de confidentialité peut tuer. C'est peut-être une mort indirecte mais on y fait très attention en France* », clarifie Vincent Templier.

Autre élément à prendre en compte, l'ennemi s'adapte, lui aussi. « *Sans être anxiogène, le temps des 'attaquants-ados-sweat à capuche' est fini, aujourd'hui ce sont des gangs qui gèrent de grandes sommes d'argent. C'est un système très industrialisé. Sur le dark net, il y a même des trophées d'innovation. On ne peut pas voir le monde des pirates comme des individus isolés* », met en garde Bruno Charrat, Directeur Délégué Cyber Security Institut. *« Il faut anticiper des solutions dès maintenant. Il ne faut pas juste résister à la menace mais être un leader.* »

On le comprend, la cybersécurité est l'affaire de tous. « *Chaque personne est première responsable de sa propre sécurité et celle de l'ensemble* », conclut Olivier Siegler.