

## FACE À L'AUGMENTATION DE LA CYBERCRIMINALITÉ, COMMENT BIEN SÉCURISER SES DONNÉES ?

*Tous les quinze jours environ, un hôpital français est victime d'une cyberattaque. Le chiffrement ou l'extraction des données engendré par l'intrusion peut mettre à mal un système d'information pendant plusieurs jours, voire plusieurs semaines, et fréquemment plusieurs mois. De plus, ces attaques peuvent engendrer des coûts considérables pour les établissements touchés, pouvant s'élever jusqu'à plusieurs millions d'euros pour rétablir leur système d'information sur des bases saines. Pour y faire face, certains hébergeurs tels que le Mipih propose de mettre en œuvre une sauvegarde externalisée en s'appuyant sur la technologie du stockage objet afin de mieux gérer et protéger ses données.*



Crédit photo : DR

**David Héliot**

Adjoint au Directeur de l'offre hébergement des données de santé du Mipih

Crédit photo : DR



### QUAND LA SAUVEGARDE NE SUFFIT PLUS À SE PROTÉGER DES ATTAQUES

Si protéger ses données est devenu une norme dans le domaine de la santé, « les sauvegarder uniquement, ne suffit plus », souligne David Héliot, Adjoint au Directeur de l'offre hébergement des données de santé du Mipih. « Malheureusement, quand les hôpitaux se font cryptolocker ou qu'ils sont victimes de malwares, même la sauvegarde est une cible. Pour avoir une réassurance, il faut pouvoir changer le type de support et l'externaliser », conseille-t-il.

### STANDARDISER LA SAUVEGARDE POUR MIEUX L'EXTERNALISER

Face à ce constat, le Mipih utilise le stockage objet, pour permettre à ses adhérents de sanctuariser leurs données. Ce protocole universel, standardisé et compatible avec les principales solutions de sauvegarde du marché, permet aux hôpitaux de découpler et d'externaliser simplement leurs sauvegardes. Grâce à cette méthode, « un hôpital qui a déjà son programme de sauvegarde en place peut facilement, en activant une fonction additionnelle sur son outil initial, avoir une autre copie chez un hébergeur certifié HDS (Hébergeur de Données de Santé) et souverain », explique David Héliot. Cette stratégie n'est pas uniquement nécessaire face aux risques d'attaques, elle l'est également face aux événements ou aux risques techniques pouvant impacter un établissement (incendies, inondations, dégradations, catastrophes naturelles, ...). En plus de garantir un accès rapide aux informations, ce protocole permet « de prendre en charge des volumétries très importantes telles que le pétaoctet », souligne David Héliot. Aussi, « une fois que la donnée a été déposée, il n'est plus possible de la modifier, elle devient inaltérable », précise-t-il.

### OÙ SAUVEGARDER SES DONNÉES ?

Sauvegarder son système d'information en plusieurs versions implique forcément de s'interroger sur le lieu de son stockage. En tant que groupement d'intérêt public, cet hébergeur a choisi

d'être un cloud souverain et possède ces propres datacenters ; deux : à Amiens et à Toulouse, certifiés HDS. Cette solution garantie par conséquent que les données de ses adhérents soient hébergées, préservées et sécurisées de façon souveraine.

### EXTERNALISER SON SYSTÈME D'INFORMATION POUR MIEUX SE PROTÉGER

Au-delà du simple hébergement de données, David Héliot rappelle qu'il est important pour les hôpitaux de réfléchir à la possibilité « d'externaliser l'ensemble de leur système d'information chez un hébergeur certifié HDS et souverain ». Cette solution permet de facto de bénéficier d'un plan de reprise d'activité. Les contraintes matérielles sont allégées pour l'établissement de santé qui va s'appuyer sur une nouvelle infrastructure virtualisée chez l'hébergeur. L'équipe informatique du GHT peut ainsi se consacrer davantage à des projets avec des bénéfices plus direct pour les patients, tout en augmentant significativement le niveau de sécurité.

Acteur public du numérique en santé, éditeur et 1<sup>er</sup> hébergeur français certifié HDS, le Mipih accompagne les établissements de santé, les GHT, le médico-social et les médecins libéraux, dans leur digitalisation afin de répondre à leurs enjeux numériques. Avec quatre agences, à Toulouse, Amiens, Bordeaux, Reims et des bureaux à Parisanté Campus, le Mipih et ses 900 collaborateurs partagent leurs savoirs et expertises avec plus de 700 établissements adhérents et clients pour construire ensemble le système de santé de demain : performant, éthique, responsable et souverain.