Au CHRU de Montpellier, **une SSI externalisée pour mieux garantir la conformité**

Dans un contexte de certifications et d'exigences réglementaires multiples, le CHRU de Montpellier a décidé d'externaliser sa fonction de responsable de la sécurité des systèmes d'information (RSSI). Deux experts du groupement d'intérêt public (GIP) Midi Picardie informatique hospitalière (Mipih) ont présenté cette démarche au nom de l'Asinhpa (Association des structures d'informatique hospitalière publiques autonomes) lors du 4e congrès de l'Association pour la promotion de la sécurité des systèmes d'Information de santé (Apssis), le 5 avril au Mans.


© Morgan Bourven

Nicole Genotelle et Benoît Dulondel interviennent pour le Mipih au CHRU de Montpellier.

De la certification de la Haute autorité de santé (HAS) aux prérequis du programme Hôpital numérique, en passant par la politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI-MCAS), la sécurisation des systèmes d'information (SI) s'apparente à un labyrinthe réglementaire pour les établissements de santé.

– *Il est parfois difficile de distinguer ce qui relève des bonnes pratiques, du 'presque opposable' ou du non-négociable* », a indiqué Benoît Dulondel, consultant SSI au Mipih, lors de la présentation de la stratégie du CHRU de Montpellier. « *La sécurisation des systèmes d'information en santé aurait-elle échappé au choc de simplification ?* », s'est-il interrogé. Le RSSI s'est néanmoins félicité que le contexte réglementaire « *a changé le regard des établissements sur la sécurité, en la portant à un niveau plus stratégique* ».

Benoit Dulondel intervient auprès des établissements adhérents du MiPih pour les accompagner dans différentes démarches (certification des comptes, sécurité du SI, etc.). Il est aussi membre du groupe de travail sécurité de sécurité de l'Asinhpa. Il intervient, dans sa mission au CHRU de Montpellier, avec Nicole Genotelle, consultante en SSI au MiPih depuis 2014. Elle y met en pratique plus de dix ans d'expérience dans le renforcement de la sécurité des SI d'organismes publics et privés.

Pour Nicole Genotelle, les mesures de sécurité prioritaires à mettre en œuvre sur le SI, doivent, pour être efficaces, s'adapter aux chantiers en cours. « *Les RSSI ne doivent pas apparaître comme des censeurs,* estime-t-elle, *mais au contraire être des facilitateurs de tous les projets en relation avec le SI.* »

A Montpellier, les deux RSSI du MiPih coopèrent avec Jean-Michel Kermarrec, responsable de la protection des SI au sein du CHU, « *qui est un lien fonctionnel entre la direction générale et la direction des systèmes d'information* », a souligné Benoît Dulondel.

Une sécurité améliorée au fil de l'eau

C'est le contexte de certifications multiples auquel il faisait face qui a poussé le CHRU à faire appel au Mipih. Après une démarche initiale de diagnostic, les deux experts ont très rapidement proposé un plan d'action au comité de direction de l'établissement. « *L'idée était qu'au bout de trois mois, nous ayons une politique de sécurité et une organisation de la SSI, afin d'avoir les moyens de travailler et mettre en place les actions* », a témoigné Nicole Genotelle. Ces trois premiers mois ont aussi vu l'implémentation « *de mesures rapides et simples* » pour que « *l'évolution de la sécurité se voit rapidement* ».

La philosophie des deux RSSI est que toute évolution des pratiques sur le SI est un pas en avant qui doit contribuer à l'amélioration de la sécurité globale. Le plan d'action présenté au comité de direction n'avait donc pas vocation à être suivi à la lettre. « *C'était un guide, mais nous avons aussi voulu au maximum être opportunistes* », a précisé Mme Genotelle. Chaque nouveau projet lié au SI, à la fonction achat et aux appareils biomédicaux était une chance à saisir pour y associer un aspect sécurité, « *même si ce n'était pas dans le plan d'action défini au départ* ».

L'outil de diagnostic développé par le MiPih a été mis une nouvelle fois à profit un an après le début du projet pour dresser un premier bilan de l'impact des actions sur les indicateurs des différentes certifications visées, avec le cas échéant des mises à jour des priorités. Ce fonctionnement a permis d'éviter un des écueils de la SSI : traiter les écarts normatifs, mais pas les causes réelles des dysfonctionnements.

Morgan BOURVEN,
journaliste spécialisé en informatique de santé

« Il faut dé-corréler la SSI des différents volets 'certifications', car ils sont gérés en mode projet, ce qui est bien pour traiter l'urgence mais ne permet pas de maintenir les actions dans le temps », a analysé Benoît Dulondel.

La direction fortement impliquée

Les deux témoins ont souligné l'entière implication de la direction de l'établissement dans le processus. *« Toutes les instances du comité de direction ont souhaité être impliquées dans le comité de pilotage sécurité*, a insisté Nicole Genotelle. *C'était vraiment une impulsion et une volonté de la direction de se voir rattacher la sécurité »*. Son confrère estime quant à lui que c'est la pression réglementaire qui *« a changé le regard des professionnels. Ils ont compris que la SSI est un métier réel, transverse, comme l'est la gestion de la qualité et des risques »*. La stratégie est déployée sur le terrain par une délégation informatique hospitalière (DIH) chargée de coordonner les correspondants sécurité métiers. Ces derniers sont en charge de la sensibilisation des équipes, de la mise en place des préconisations, de la surveillance et du contrôle. Des correspondants sécurité technique ont aussi été formés. Ils sont chacun experts sur un sujet précis (les codes malveillants, les habilitations, les vulnérabilités, etc.) et ont pour mission de *« prêcher la bonne parole »* concernant leurs domaines respectifs.

© Morgan Bourven

La complexité de la réglementation a été un des sujets majeurs du congrès.

L'ensemble de ces professionnels dispose d'un corpus documentaire *« allant du stratégique à l'opérationnel »*. Chartes des bons usages du SIH, matrices de conformité aux référentiels, tableaux de bord de suivi des risques, fiches réflexes... Autant d'outils déclinés au niveau opérationnel dont il faut *« user et abuser »*. Le fait d'avoir des documents de qualité *« a permis de créer de la dynamique de groupe »*, a noté Benoît Dulondel, avant de *« féliciter les tutelles pour la qualité des livrables actuellement produits »*. ■