Morgan BOURVEN,
journaliste spécialisé en informatique de santé

Sécurité des systèmes d'information hospitaliers : une prise de conscience qui tarde

Chaque jour, un établissement de santé français est confronté à une cyber-attaque. La sécurité des systèmes d'informations hospitaliers (SIH) n'est pourtant toujours pas considérée comme une priorité des dirigeants hospitaliers, ont expliqué plusieurs intervenants au 4e congrès national de l'Association pour la promotion de la sécurité des systèmes d'information de santé (Apssis), qui s'est tenu au Mans du 4 au 6 avril.

© Morgan Bourven

150 personnes se sont réunies au Mans pour le 4e congrès de l'Apssis

Hospital!9. *« Cet utilisateur a mis une majuscule, un chiffre et un caractère spécial dans son mot de passe, mais ça ne va pas suffire »*, s'amuse Monsieur X, en plein « hack » d'un SI. Il ne lui faudra que quelques minutes pour aspirer ses dossiers patients (fictifs), avant d'en prendre le contrôle total. Cette scène s'est déroulée le 4 avril au Mans, devant 150 responsables informatique et référents sécurité d'établissements de santé. Objectif : leur montrer le retard pris par le secteur hospitalier dans ce domaine.

« Le niveau de prise de conscience est catastrophique », a alerté Philippe Loudenot, fonctionnaire de sécurité des systèmes d'information (FSSI) pour les ministères des affaires sociales et de la santé. Les responsables sécurité des hôpitaux ont tout simplement *« loupé le virage de la révolution numérique »*, a-t-il assené. Alors que les établissements de santé sont de plus en plus connectés, les *« référents sécurité »* n'y sont que 552. Moins d'une cinquantaine ont le titre de *« responsable de la sécurité des systèmes d'information »* (RSSI). Or, en 2015, plus de 1 300 incidents ont été signalés au FSSI. Ces remontées sont volontaires et ne représentent pas une liste exhaustive des incidents, a-t-il précisé. 816 étaient des attaques par opportunisme - *« c'est-à-dire que le système est tellement poreux que le pirate y pénètre »* - et 498 étaient liés à des « mésusages » du SI. Cet état de fait est en partie dû au manque d'investissement : les SI ne représentent que 2 % des dépenses des établissements de santé, selon l'Atlas 2015 des SIH. Les experts préconisent d'atteindre 5 %. En 2015, 18 des incidents signalés étaient des attaques ciblées, *« avec une réelle volonté de nuire »*. *Si Philippe Loudenot n'a pas eu écho d'hôpitaux français évacués suite à une malveillance, comme ce fut le cas à six reprises en février et mars aux Etats-Unis,* il a rappelé que *« chaque attaque a des conséquences, a minima financières »*. Le 1er avril, un établissement de 60 lits a signalé une attaque ayant entraîné 5 jours d'interruption du SI. Coût de la remise à niveau : 50 000 euros.

© Morgan Bourven

Loïc Guezo, de la société Trendmicro, et Philippe Loudenot, FSSI, ont présenté le paysage actuel du cybercrime.

L'inquiétude actuelle la plus forte est liée aux *« ransomwares »*. Il s'agit de logiciels malveillants qui, après avoir chiffré les données du système, réclament une rançon à l'utilisateur en échange de la clé de déchiffrement. *« Chaque jour, un hôpital français est touché ; 365 par an »*, a confié Vincent Trely, président de l'Apssis, à Biologiste infos.

Au-delà des cyber-extorsions, toutes les attaques doivent être traitées avec prudence. *« Un défacement de site [ndlr : le remplacement de sa page d'accueil] peut paraître anodin, mais il est possible qu'il soit lié au SI »*, a mis en garde Philippe Loudenot. Pour limiter les risques, il a appelé les responsables informatiques à créer des « bulles » indépendantes autour de leurs systèmes.

Concrètement, il s'agit par exemple de connecter les appareils biomédicaux à un réseau dédié, distinct de celui du SIH, du wifi patient ou des logiciels techniques. Ceci afin d'éviter qu'un pirate ne pénètre dans l'hôpital via le système de climatisation avant de se faufiler vers les pompes à morphine. ■