Santé : la sécurité numérique en question

Jusqu'à jeudi, au Carré Plantagenêt, 120 professionnels participent au congrès national de la sécurité des systèmes d'information de santé. Éclairage d'un expert.

Entretien

Vincent Trély, organisateur du congrès de la sécurité des systèmes d'information de santé.

Archives

L'hôpital du Mans s'est équipé de tablettes et ordinateurs permettant au personnel de suivre l'état des patients. Pratique, efficace, mais à condition de veiller à la confidentialité des informations transmises.

À quoi sert ce congrès sur la sécurité des systèmes d'information de santé ?

C'est le seul congrès en France qui réunit autant de professionnels du secteur : responsables de la Commission nationale de l'informatique et des libertés (Cnil), du ministère de la Santé, directeurs d'hôpitaux et de cliniques, responsables sécurité, avocats spécialisés, industriels, experts du numérique...

Le congrès permet à la fois de faire le point sur les avancées dans les établissements, l'évolution de la réglementation et l'offre des industriels : logiciels, méthodes, outils informatiques pour la surveillance du réseau, la remontée automatique des failles.

Quelles sont les principales menaces qui pèsent sur les données médicales numérisées ?

D'abord le « mésusage ». On est face à des professionnels très vite informatisés, mais qui n'ont pas tous conscience du danger que représente la technologie.

Quand des médecins s'échangent des données de santé via Gmail, ils ne voient pas le mal, alors qu'ils sont hors la loi. On ne peut échanger des données de santé que sur des systèmes de messagerie cryptés, toute personne qui accède à ces documents doit être authentifiée. Si l'information se retrouve sur le web, une personne peut porter plainte. L'établissement ou le médecin à l'origine de la fuite risque gros.

Les médecins sont-ils assez formés ?

Le personnel soignant dans son ensemble doit être mieux formé. L'État doit accompagner cet effort via la réglementation, avec un guide de bonnes pratiques et un contrôle de sa mise en application. On va dans ce sens : la Haute autorité de santé va s'en préoccuper. Il y aura des certifications, des protocoles, au même titre que les infections nosocomiales.

D'autres solutions face à ces évolutions technologiques permanentes ?

La solution, c'est 20 % de technique et 80 % de bon sens. Chacun doit prendre conscience de ses responsabilités. Quand on quitte la maison le matin, on ferme la porte à clé. Pourquoi laisse-t-on le PC allumé quand on va déjeuner ?

Le smartphone peut-être une arme de cybercriminel.

Hier, le fonctionnaire de sécurité du système d'information du ministère de la Santé nous a expliqué qu'aux États-Unis, une banque a été victime d'une attaque par SMS codés. Les messages ont permis de faire sortir des billets d'un distributeur. On peut aussi prendre la main sur un pacemaker. Tout objet communiquant est vulnérable.

Recueilli par
Jérôme LOURDAIS.