Les établissements de santé ont leur plan de sécurité des SI

Annoncé par la ministre des affaires sociales et de la santé, Marisol Touraine, le 3 octobre dernier, le plan d'action sur la sécurité des systèmes d'information (« plan d'action SSI ») est diffusé. Il s'adresse aux établissements de santé, laboratoires de biologie médicale, centres de radiothérapie et centres d'imagerie et de radiologie, qu'ils soient publics ou privés. Une instruction datée du 14 octobre, et validée en novembre, présente le plan et ses priorités.

« Le plan d'action SSI ne se substitue pas aux obligations de sécurité que doivent mettre en place les structures, mais il propose un calendrier à 6, 12 et 18 mois de réalisation de mesures prioritaires en termes d'efficacité par rapport, notamment, au risque de piratage informatique », précise le ministère de la Santé. Il revient aux Agences régionales de santé (ARS) d'assurer la diffusion large du plan.

Trois séries de mesures prioritaires

Une première série de mesures est à mettre en place dans les six mois. Parmi ces mesures figurent : l'identification de la fonction RSSI, une charte utilisateur, une procédure de signalement, la sécurisation des comptes par mots de passe robustes ou encore des sauvegardes testées.

La deuxième série d'actions doit être déployée dans les 12 mois. Ces mesures couvrent, entre autres : l'appréciation du risque avant mise en production d'un SI, les mises à jour régulières (OS, terminaux, serveurs et équipements biomédicaux), la protection de tous les accès à Internet, la gestion des comptes utilisateurs. Et, enfin, la sensibilisation à la SSI des personnels.

La troisième batterie de mesures doit être initiée dans les 18 mois. Elle inclut : le cloisonnement du réseau par départements (administration, paie, plateau technique…), l'encadrement contractuel de tous les accès et la réalisation d'une analyse de risque SI de la structure concernée.

Réglementation applicable

Les mesures pour sécuriser les SI des établissements de santé sont associées à des références réglementaires. C'est notamment le cas de la politique de sécurité des SI pour les ministères chargés des affaires sociales (PSSI-MCAS) et de la politique de sécurité des SI de santé (PGSSI-S). Le programme hôpital numérique piloté par la Direction générale de l'offre de soins (DGOS) et les guides de l'Agence nationale de sécurité des systèmes d'information (ANSSI) en font partie également.

Aux États-Unis, les cyberattaques dans le monde hospitalier se multiplient. La France n'est pas à l'abri. Selon Symantec, l'Hexagone est entré en 2015 dans le top 10 des pays les plus touchés par le piratage informatique. Tous les secteurs d'activité sont concernés.

Lire aussi :

Ransomware, haro sur le monde hospitalier
Un hôpital anglais ferme pour traiter son virus… informatique
Nos données de santé (mal) protégées par l’indésirable SHA-1