L'Agence nationale de sécurité du médicament et des produits de santé (ANSM) a créé le premier comité scientifique spécialisé temporaire (CSST) sur la cybersécurité des logiciels dispositifs médicaux (DM). Les experts externes qui le composent sont chargés de proposer des recommandations pour garantir un niveau minimum de sécurité des logiciels utilisés dans le domaine médical face aux menaces de malveillance numérique.

Un nombre croissant de dispositifs médicaux, qu'ils soient utilisés par des professionnels de santé à l'hôpital ou à domicile par des patients, sont aujourd'hui connectés. Ils peuvent donc partager des informations à travers des liaisons sans fil (Bluetooth, Wifi) ou par connexion physique à un réseau internet.

Les fonctionnalités de ces dispositifs couvrent l'échange de données (imagerie médicale, résultats de biologie), le pilotage du dispositif (programmation de pompes à perfusion ou de dispositifs implantables actifs), le suivi du patient à distance (surveillance de signes vitaux) ou la maintenance des produits.

En France, la sécurité informatique des DM est abordée dans différents textes liés à la santé connectée, mais le DM, bien que cité, n'est pas l'objet principal de ces textes. De la même manière, la réglementation Européenne des DM ne couvre pas, ou de façon insuffisante, le risque d'attaque informatique des DM.

L'ANSM a donc mis en place un CSST composé d'experts externes, choisis en raison de leurs compétences et expériences diverses sur le sujet de l'informatique et de la cybersécurité.

Il est chargé de proposer au directeur général de l'ANSM des recommandations à l'attention des fabricants de dispositifs médicaux de manière à ce qu'ils puissent prendre les mesures nécessaires pour prévenir toute attaque malveillante à l'encontre de leurs DM et ainsi empêcher la compromission des données et l'utilisation détournée des DM qu'ils mettent sur le marché.

Lire aussi

- CSST cybersécurité des logiciels DM