La nouvelle vient de fuiter dans la presse : des **failles de sécurité informatiques** auraient été repérées dans des
implants cardiaques
aux Etats Unis, les rendant facilement piratables selon les départements de la santé et de la sécurité intérieure américains.

La numérisation de la société et des services publics n'épargne pas les hôpitaux et maintenant les dispositifs sont au cœur du débat. Depuis plusieurs mois déjà, ces établissements sont la **cible de pirates**
dont les attaques représentent un vrai danger pour
l'intégrité de notre système de santé
et avec l'essor de l'IoT, nous sommes en droit de nous questionner sur leur
confidentialité
et leur
vulnérabilité
.

Très peu de personnes pensent que le **piratage d'un appareil connecté** peut représenter un danger réel, bien plus conséquent que le piratage d'un PC, et pourtant. La réalité est qu'il y a bien trop de fabricants qui conçoivent un trop grand nombre de systèmes incompatibles et qui ne sont **pas nécessairement sécurisés.**

Pour que la société bénéficie de ces nouvelles technologies, il convient de répondre à certaines questions en matière de sécurité informatique :

o *Quand allons-nous commencer à instaurer certaines normes de sécurité pour la technologie du domaine de la santé ?*

o *Le cryptage doit-il être obligatoire ?*

o *Comment protéger ces clés USB sur pattes ?*

o *Y a-t-il des risques d'infection ?*

o *Où commence et s'arrête la vie privée si nous sommes connectés à tout et à tout le monde ?*

Pour répondre à ces questions, Tanguy de Coatpont, Directeur général de Kaspersky Lab France et Afrique du Nord se tient à votre disposition.

Sergey Lozhkin, chercheur principal au GReAT de Kaspersky Lab avait par ailleurs enquêté sur les nombreuses vulnérabilités critiques trouvées dans l'infrastructure informatique d'un hôpital, une analyse que vous pouvez découvrir ici .