Healthcare Cybersecurity

Le contexte luxembourgeois

Dans le secteur de la santé le constat est simple mais pas forcément évident: le niveau de sensibilité des données de santé gérées par les établissements est supérieur à celui des autres données à caractère personnel. Ceci est ancré dans la loi de 2002 y relative et sera encore une fois renforcé dans le futur règlement européen. Un accès malveillant ou tout simplement non-autorisé aux informations contenues dans les systèmes d' information a un tout autre impact sur la vie des personnes qu'une carte de crédit perdue ou volée. Les moyens de blocage et de remédiation seront tout autre également.

Selon une étude de 2015 de KPMG Global (« KPMG Technology Industry Outlook Survey June 2015 ») , l'ensemble des informations liées à la santé et aux patients fait l'objet d'une réelle convoitise de la part de hackers ou autres personnes mal intentionnées, prêts à profiter de la faiblesse de certains points d'entrée dans les systèmes.

L'adoption de nouvelles technologies ainsi que de nouvelles pratiques (télémédecine, appareils mobiles pour les médecins ou le personnel, Dossier de Soins Partagés…) rendent toujours plus prégnant l'usage des outils informatiques. L'intégration des systèmes au sein des établissements est dorénavant très important voire un enjeu d'efficacité de prise en charge des patients - alors que souvent ces systèmes n'ont pas été conçus pour un tel niveau d'intégration au départ. A l'heure actuelle, les médecins ou le personnel sont amenés à utiliser des ressources informatiques contenant des données sensibles sans pour autant être rassuré sur le niveau de sécurité concernant l'accès aux données.
S'ajoute à cela les efforts menés afin de définir un cadre précis de la pratique de l'eHealthcare avec des attentes spécifiques en termes de sécurité, de gouvernance informatique, d'accès aux données…

> De par la nature de son activité, il existe un conflit moral entre investir dans un équipement IT et un équipement médical, ce qui peut expliquer que le monde médical investit moins que d'autres dans la sécurité IT compte tenu de la sensibilité des données traitées. Depuis quelques années déjà l'augmentation des attaques informatiques envers les établissements de santé est en forte hausse (40% des hôpitaux américains ont reportés une cyber attaque en 2013 ; 20% seulement en 2009) et le Luxembourg n'est pas épargné. Ceci n'est pas une spécificité du secteur et les soucis majeurs liés à ce type d'attaques sont qu'elles peuvent être difficilement identifiables et menées de l'extérieur comme de l'intérieur des établissements.
>
> Patrick Wies

Toutefois, le Luxembourg possède une compétence connue et reconnue à travers le monde en termes de sécurité de l'information puisque son secteur financier a su construire une expertise en la matière au cours des 20 dernières années. La maturité de ce secteur dans le domaine de la protection des données peut servir de levier pour d'autres acteurs nationaux qui souhaiteraient s'inspirer des pratiques existantes pour les adapter à leur contexte particulier. D'autant plus que la stratégie de diversification économique du pays tend à faire du Luxembourg un pôle international de services IT. C'est pourquoi il est dans l'intérêt de tous les acteurs de mutualiser les expériences déjà réalisées pour positionner nos compétences sur le plan international.
L'ensemble des acteurs luxembourgeois de la santé se retrouvent donc à évoluer dans un environnement en pleine mutation soumis à des risques et autres obligations légales dans lequel il est difficile d'avoir une vision claire tout en réalisant l'objectif premier des établissements de santé: une prise en charge optimale des patients.

Cybersécurité et Santé - Ce que KPMG Luxembourg peut vous offrir

KPMG Luxembourg accompagne les acteurs du secteur de la santé afin de relever tous leurs défis à travers les thématiques suivantes :

Governance IT

- Accompagnement de la Direction dans le cadre de projets de grande envergure
- Analyse et Gestion des risques
- Gestion de projet

Data Privacy

- Réglementation luxembourgeoise (CNPD)
- Réglementation européenne (en particulier le nouveau règlement européen sur la protection des données à caractère personnel)
- Méthodologie de « Privacy Impact Assement »
- Assistance dans la prise de fonction d'un chargé de la protection des données

Certification ISO

ou mise en place opérationnelle d'un système de gestion de la sécurité de l'information sur base des normes suivants:

- ISO 27001: Management de la sécurité de l'information
- ISO 27002:
  - Technologies de l'information
  - Techniques de sécurité
  - Code de bonne pratique pour le management de la sécurité de l'information
- ISO 27799:
  - Informatique de santé
  - Management de la sécurité de l'information relative à la santé

Revue Infrastructure

- Test de pénétration
- Sélection de systèmes IDS-IPS (Intrusion detecting system – Intrusion prévention system)
- Revue d'architecture réseau

Assistance dans le renforcement des opérations

- Gestion des accès logiques
- Gestion des accès physique
- Gestion des changements
- Gestion de projet
- Disponibilités des systèmes (BCP/DRP...)
- Archivage électronique

Nous avons également des experts dédiés au secteur de la Santé sur les sujets suivants:

Big Data

Gestion de BYOD

Opérations IT
(Job processing, back up)

Audit de sécurité informatique

Revue de processus et optimisation de coûts

Your dedicated contact at KPMG

Patrick Wies
Partner

T: +352 22 51 51 - 6305
E: patrick.wies@kpmg.lu

Anne Desfossez
Associate Partner

T: +352 22 51 51 - 7394
E: anne.desfossez@kpmg.lu

www.kpmg.lu