CYBERCERCLE

Petit déjeuner débat du **3 février 2016**

CYBERSECURITE & SANTE

avec

Philippe LOUDENOT

FSSI du ministère des Affaires sociales, de la Santé et du Droit des femmes

sous la présidence de

Gérard BAPT

Député de la Haute-Garonne

et

Pierre MORANGE

Député des Yvelines

COMPTE RENDU



Le digital bouscule aujourd'hui le système de santé français, et repose au centre des débats la question éthique de la collecte et l'utilisation des données personnelles des utilisateurs.
A l'heure actuelle, nous assistons à une révolution de la santé connectée par le biais de dispositifs utilisés par des dizaines de millions de personnes dans le cadre de leurs activités personnelles, ayant ainsi accepté que leurs données soient recueillies par Google. Alors, l'accès aux données qui, anonymisées, sont de grande utilité pour la recherche publique et privée, mais aussi pour les activités de R&D, doit faire l'objet d'un encadrement précis et sécurisé.

L'écriture initiale de l'article 47 de la Loi de santé, qui organise l'accès aux données qui ne sont pas directement accessibles, était très bureaucratique. Cet article a alors été réécrit pour garantir à la fois l'anonymisation des données, mais aussi leur accès. La sécurité des données, lorsqu'elles sont hébergées, est aussi problématique en raison de la multitude d'hébergeurs existant. Alors que la préoccupation principale était d'assurer la sécurité de la transmission des données, la sécurité de l'accès des données chez ces hébergeurs, elle, n'était pas assurée. Afin de pallier cette insécurité, une coopération entre les différents acteurs en charge de ces questions a été instaurée et a abouti à un amendement renforçant la sécurité chez l'ensemble des hébergeurs.

La question de la gestion des systèmes d'information des établissements médicaux a également été une préoccupation majeure du domaine de la santé. Il est possible de recenser aujourd'hui plusieurs pannes et bugs informatiques, ayant pu provoquer l'arrêt de certains services comme par exemple en Gironde, où le fonctionnement d'un établissement hospitalier a été interrompu pendant plusieurs jours.
Considérant ces incidents ou accidents, il est apparu inapproprié de ne pas tirer d'analyses pour améliorer la prévention en amont, et l'intervention en cas d'incident. A ce titre, il a été décidé que les organismes compétents doivent analyser les incidents les plus graves et mettre en place des mesures de précaution.

A partir de ces éléments d'actualité législatives, la question de la collecte et de l'utilisation des données de santé demeure. Par vengeance, attaque ciblée, ou erreur humaine, des données collectées peuvent être mises en accès libre sur internet, ce qui est un dommage grave. A titre d'exemple, le hack de Primera Blue Cross, en 2015, a entraîné la fuite de données de plus de 11 millions d'utilisateurs.
A cet égard, on peut penser que des terroristes, à l'avenir, puissent désorganiser un pays en mettant à mal le système d'information de ses secours ou son système de santé. Cet aspect de la sécurité dans le domaine de la santé doit être approfondi davantage pour être mieux appréhendé par les personnels hospitaliers et les médecins.

Le temps numérique est différent du temps politique. Dans le temps numérique, les évolutions sont rapides et concernent la masse d'information produite, la multiplicité des sources, des technologies etc… En parallèle, le temps politique lui, court après son « centre de gravité ». Cela correspond à la différence entre le temps technologique et le temps où les responsables politiques s'adaptent. Les moyens consacrés à la sécurisation des systèmes d'information du secteur de la santé doivent impérativement être rationnalisés.

Le monde de la santé peut être divisé en trois sous-secteurs principaux, tous confrontés au risque numérique :

- La branche « recouvrement », caractérisée par une dichotomie entre RSSI et les autres métiers. Cela entraine une difficulté à appréhender toute la partie fraude car il y a un problème de discours

entre les uns et les autres. Des efforts sont néanmoins réalisés dans ce secteur car les fraudes sont un phénomène global qu'il faut traiter avec les différents organismes et composantes d'un secteur.

- L'appui logistique, tel que les établissements français du sang par exemple. Une attaque informatique sur les groupes sanguins répertoriés pourrait avoir des conséquences sécuritaires et sanitaires majeures.
- Les établissements médicaux-sociaux, qui subissent une importante progression en termes de fraudes, d'effacement des paramétrages souhaités ou dans l'interruption du fonctionnement du matériel.

Suite au constat de l'augmentation des attaques et fraudes dirigées contre le secteur de la santé, une chaîne d'alerte a été mise en place et permet de souligner trois grandes catégories de perturbation des systèmes d'information médicaux :

- Le piratage direct, interne ou externe, par vengeance, malveillance ou volonté de déstabiliser un Etat (exemple de l'Estonie en 2007 qui a vu ses systèmes d'urgence bloqués suite à une attaque informatique).
- Attaques par rebonds ou par porosité : alors que l'attention s'est focalisée sur la confidentialité des données, la disponibilité et l'intégrité sont des éléments complémentaires à ne pas négliger.
- Par manque d'accompagnement, de vision ou de veille, mésusage des systèmes d'information. Avec l'arrivée des appareils connectés, de bien-être ou médicaux, de nouveaux risques ont été introduits et ne sont pas toujours appréhendés correctement par les personnels du secteur médical.

De nouvelles difficultés sont apparues également suite à l'interconnexion des objets connectés, qui peut entrainer la perte de données médicales importantes, impactant ainsi le patient.

Le travail principal aujourd'hui est d'acculturer la population à la sécurité des systèmes d'information. Pour précision, il existe trois types de systèmes d'information dans le domaine de la santé :

- Le traitement oral ;
- Le traitement papier ;
- Les systèmes d'informations biologiques.

Ces trois systèmes d'information convergent tous vers le numérique, ses bienfaits et ses dangers. Il faut prendre conscience que nous sommes dans de la gestion de risque, voir ce qu'on doit sécuriser et la manière de le faire.

Questions – réponses :

Mme Bénédicte PILLIET, directeur du CyberCercle
Est-il possible de faire un point sur la LPM et la sécurité des OIV dans le secteur de la santé ?

Philippe LOUDENOT : Le secteur de la santé est touché sur deux types d'OIV :

- Tout ce qui relève des appuis : fournir des prestations et médicaments rapidement en cas de crises majeures ;
- Certains établissements de santé, eux-mêmes caractérisés d'OIV, qui doivent être davantage sécurisés.

Gal DE CREMIERS, haut fonctionnaire de Défense et de Sécurité adjoint
Les fuites de données de santé n'ont jamais fait de morts et la sécurité des patients demeure la priorité. Ne faut-il donc pas d'abord s'occuper de sécurité physique du patient plutôt que de la sécurité de ses données ?

Pierre MORANGE : La sécurité du patient est bien sûr une priorité mais dépend de plusieurs éléments. Par exemple, la sécurité financière est fondamentale car les fraudes peuvent induire des risques sanitaires dans la mesure où des moyens initialement consacrés ne pourront être disponibles pour les patients.

M. Larazo PEJSACHOWICZ, Président du CLUSIF
Le temps politique diffère du temps numérique mais il n'a pas non-plus besoin d'autant de précisions que le discours technique. Au CLUSIF, on relève des imprécisions : l'assuré est concerné par la confidentialité des données alors que le patient a pour intérêt d'être soigné. Pour cela, la sécurité des données est essentielle. Néanmoins, il n'y a pas de données anonymisées du côté de la santé en France, et même s'il y en avait, nous savons qu'il est possible de désanonymiser une base de données. Il est donc important de faire comprendre qu'il n'existe pas d'anonymat dans le Big Data, sans pour autant dispenser un discours anxiogène favorisant l'immobilité.

Philippe LOUDENOT : Les objectifs de sécurité diffèrent effectivement selon les secteurs et l'analyse de risque. C'est le métier qui analyse ce qu'on doit protéger, en coopération avec les acteurs en charge de la sécurité, pour savoir comment donner confiance aux traitements digitaux pour les citoyens, les administrations, et l'Etat.

Pierre MORANGE : Face au risque d'incertitude sur la sécurisation des données, il peut y avoir une tétanisation des esprits, ce qui est préjudiciable à la défense de la sécurité sanitaire des patients. Il y a un risque minimum qu'il faut accepter et c'est l'identification des risques qui doit amener à prioriser les différents sujets afin d'en tirer les conséquences.

Mme Bénédicte PILLIET, directeur du CyberCercle
Les fabricants de matériels de santé sont-ils plus attentifs aux dangers liés à la sécurité ?

Philippe LOUDENOT : Ces notions de sécurité commencent à entrer dans les esprits même s'il reste encore du chemin à faire. Maintenant que la prise de conscience s'est effectuée, il faut aider les constructeurs qui ne sont pas spécialisés dans le domaine de la sécurité pour qu'elle soit inclue en amont et que les constructeurs aient les moyens de faire du maintien en condition de sécurité.

M. SAINT YVES, Engie Ineo
Est-il envisagé aujourd'hui de mettre en place une normalisation, une classification, des sociétés capables de vérifier l'intégrité et la sécurité des matériels utilisés dans le domaine de la santé ?

Philippe LOUDENOT : La normalisation fait partie des objectifs prioritaires : il faut être présent dans les instances normatives et arrêter de ne penser que franco-français. En effet, la plupart des constructeurs sont étrangers et leurs normes diffèrent. La France doit donc penser au niveau européen et être présente dans les instances de normalisation.

Pour nous contacter
Tél : 09 83 04 05 37
contact@cybercercle.com

LES PARTENAIRES DU CYBERCERCLE