Une master class sur les DM connectés interroge les questions de sécurité (Afib 2022)

Master class DM connectés (Afib 2022). Photo: Geneviève De Lacour/TecHopital

(Par Geneviève DE LACOUR, aux journées de l'Afib à Lille)

LILLE, 30 septembre 2022 (TecHopital) - Pour relever le défi de la sécurité des dispositifs médicaux (DM) connectés, il faut travailler sur la formation des ingénieurs biomédicaux, sur le classement des DM ou encore les procédures d'achat, a relevé Valérie Moreno, présidente de l'Association française des ingénieurs biomédicaux (Afib), en conclusion d'une *master class* organisée le 28 septembre aux Journées de l'Afib.

Jessica Rat, ingénieure biomédicale à l'hôpital du Valais, en Suisse, a expliqué lors de la plénière des 26es journées de l'Afib, qui se déroulent à Lille jusqu'au 30 septembre, qu'un poste de référent spécialisé dans les DM connectés a été mis en place au service biomédical de son établissement et qu'il permet de bien adapter la réponse aux besoins.

"C'est un modèle que l'on voit aussi en France, dans de gros établissements tels le CHU de Lyon ou le CHU de Bordeaux", a fait remarquer Sandrine Roussel, ingénieure biomédicale au CHU de Besançon. "Cela apporte de la communication, de la porosité entre les équipes et c'est important pour la réussite des projets."

L'achat de DM

"Les arbitrages entre les fonctions biomédicales et informatiques, qui sont des fonctions support aux métiers du soin, doivent être opérés par ces derniers. C'est le métier qui est propriétaire, c'est-à-dire l'activité de soin, qui doit être informé des risques afin de les accepter ou les refuser en toute connaissance de cause. Et c'est au métier de décider sinon cela se transforme en querelles d'experts", a expliqué Christophe Millet, *cyber risk manager* chez Relyens.

"De nombreux équipements biomédicaux sont adossés au système informatique. J'ai pu constater qu'il existe une sorte de cloisonnement assez fort entre les impératifs métiers des SI et le biomédical. Il est nécessaire de mettre en place une collégialité pour des projets d'établissements", a expliqué Jean-Sylvain Chavanne, responsable de la sécurité des systèmes d'information (RSSI) au CHU de Brest et ancien membre de l'Agence nationale de la sécurité des systèmes d'information (Anssi).

"Dans le processus d'achat, il faut intégrer le risque cyber qui doit s'ajouter aux autres risques et non se substituer", a fait remarquer Sandrine Roussel.

"Les services informatiques devraient fournir aux services biomédicaux des *guidelines*, leur politique de sécurité, leurs prérequis minimums pour avoir un peu d'autonomie, sans solliciter systématiquement les services informatiques", a-t-elle ajouté. "D'où la nécessité de savoir comment fonctionne un SI, comment il s'intègre, quels sont les standards".

L'ingénieure biomédicale du CHU de Besançon a rappelé que le groupe de travail de l'Afib sur la cybersécurité des DM, qu'elle conduit, a émis quelques recommandations et a rédigé un questionnaire pour les fournisseurs. "Ce questionnaire a été adopté par UniHA."

A noter que l'ingénieur biomédical n'est pas le seul acheteur de DM. "Les DM peuvent arriver par le biais de la pharmacie et souvent sans clauses techniques."

pharmacie et souvent sans clauses techniques.

Classement des DM

Le RSSI du CHU de Brest a ensuite donné sa définition des DM selon quatre catégories. "Il y a d'abord les équipements qui fonctionnent en parfaite autonomie. Le fournisseur fournit le serveur, l'ordinateur et le DM. Pour la deuxième catégorie, le DM plus le PC sont à intégrer à la gestion de la DSI. La troisième catégorie est une catégorie hybride: le fournisseur donne le DM. Enfin en quatrième catégorie, il existe un DM qui envoie tout dans le cloud. Et comment on gère cela, c'est la question", a-t-il ajouté.

"En fonction de ces catégories, on ne gère pas la sécurité de la même façon", a-t-il complété.

"Le règlement européen impose des exigences en termes de sécurité pour les fabricants et ces exigences concernent aussi ce qui est délocalisé, dans le cloud", a tenu à souligner le représentant Syndicat national de l'industrie des technologies médicales (Snitem), William Rolland.

"L'industriel a aussi des responsabilités en termes d'expression des spécifications. Il est tenu d'écrire comment son DM doit être installé, sur quelles infrastructures. Il doit donner des préconisations d'installation", a complété William Rolland.

"Le règlement impose que tout DM soit interopérable. La réalité aujourd'hui c'est que l'interopérabilité n'est pas égale selon les DM mais c'est une exigence du règlement européen."

"On a un référentiel qui est en cours de concertation auprès de l'Agence du numérique en santé (ANS). Les choses avancent. On va vers une meilleure interopérabilité au fil des années."

"Entre marques différentes c'est un peu compliqué. C'est plus facile d'assurer l'interopérabilité entre plusieurs équipements d'une seule marque", a commenté Sandrine Roussel. Au final, il est clair que "ces problèmes d'interopérabilité peuvent conditionner le choix de certains équipements".

"Les référentiels d'interopérabilité sont de plus en plus connus au sein de mon établissement", a fait savoir le RSSI du CHU de Brest.

"L'éducation par le marché"

"Il existe une façon d'accepter ou de refuser des offres, des cahiers des charges qui font passer des messages.

"Vous avez cette force dans les établissements en constituant un collectif extrêmement important", a insisté Christophe Millet de chez Relyens, en évoquant la notion d'"éducation par le marché". "Cela prend du temps, mais l'éducation du marché fonctionne. Vous pouvez peser sur le marché", a martelé l'assureur.

"La notion de *security by design* doit être intégrée par tous les fournisseurs. Ce sont des exigences des Américains, de la Chine. Les fournisseurs doivent fournir des documents techniques intégrant la matrice des flux, la sécurité sur tous les accès, tous les composants intégrés dans le DM afin que les établissements puissent créer une base de données", a détaillé Frédéric Pegaz-Fiornet, responsable de l'activité informatique médicale et e-santé chez Siemens Healthineers.

Puis Jean-Sylvain Chavanne a parlé de "Log4j", une vulnérabilité découverte en décembre 2021 dans une bibliothèque de logiciels. "On ne maîtrise pas nos systèmes d'information en interne", a-t-il fait remarquer. "J'appelle à plus transparence sur les composants des éditeurs (pour le biomédical mais aussi la GTC, GTB) pour pouvoir réaliser rapidement une analyse de risque", a-t-il insisté.

"Que fait-on des éditeurs qui n'existent plus?", a-t-il interrogé ensuite.

"En matière de cybersécurité, le législateur n'impose rien, sauf si cela impacte le patient. Alors et seulement alors le fabricant doit agir", a indiqué Christophe Millet.

"Sur les DM, c'est une obligation des fabricants que de suivre les solutions de leur système après la mise sur le

marche. Le contrôleur c'est l'Agence nationale de sécurité du médicament (ANSM)", a rappelé William Rolland du Snitem.

Enfin, il existe des moyens de tester les systèmes. Siemens Healthineers par exemple dispose d'une équipe de hackers américains, qui testent tous les systèmes afin de mesurer les vulnérabilités. L'Anssi organise également des stress tests une fois par an sur les systèmes informatiques hospitaliers. "On fait venir une équipe de hackers qui viennent tester nos mesures et nous remontent des mesures d'amélioration ou de durcissement", a indiqué l'ex-expert de l'Anssi.

En conclusion de cette *master class*, la présidente de l'Afib a noté d'abord la nécessité de "travailler davantage sur la formation, la formation initiale et la formation continue des ingénieurs biomédicaux, pour s'approprier le vocabulaire des DSI, pour mieux discuter, se coordonner et se comprendre".

En second lieu, elle a relevé que le "classement des DM permettra de mesurer davantage les efforts à produire en fonction de leur classe".

Troisième point important, "il faut qu'on monte en compétence sur les exigences à imposer au moment de l'achat des DM, afin que tous les fournisseurs progressent en même temps que nous".
Enfin elle insiste sur la nécessité de communiquer [entre les services]. "Il faut que les directions permettent une certaine transversalité entre les services", a conclu la présidente de l'Afib.

A noter que le représentant du Snitem a proposé à l'Afib d'intégrer un groupe de travail qu'il a mis en place entre les établissements de santé et les fabricants.

gdl/nc

Geneviève De Lacour