# LA CYBERSÉCURITÉ DES DISPOSITIFS MÉDICAUX SOUS LA LOUPE DE L'AFIB

**Par Joëlle Hayek** / Longtemps considérée comme un angle mort, la sécurité numérique des équipements biomédicaux mobilise désormais toutes les attentions. L'Association française des ingénieurs biomédicaux (AFIB), notamment, s'est saisie de cet enjeu stratégique et recherche désormais un consensus avec toutes les parties prenantes pour dévoiler, courant 2024, les conclusions de travaux qui entendent fonder une nouvelle approche de la cybersécurité dans le monde du dispositif médical.

« *Nous constatons, aujourd'hui, un certain décalage entre la manière dont les équipements biomédicaux sont perçus par les responsables de la sécurité des systèmes d'information (RSSI) dans les établissements de santé, et leur réalité* », explique Benoît Fondeur, ingénieur biomédical aux Hospices Civils de Lyon et co-pilote du groupe de travail Cybersécurité de l'AFIB. De nombreux RSSI les considèrent en effet comme des dispositifs purement informatiques et devant à ce titre être traités comme tels, cherchant par exemple à y intégrer des antivirus, ce qui serait pourtant en contradiction avec les exigences propres au marquage CE. « *Qui porterait alors la responsabilité d'un dysfonctionnement du système d'exploitation ?* », poursuit-il. La temporalité même des équipements biomédicaux n'est pas celle de l'informatique hospitalière : « *Un poste de travail est changé tous les 3 à 5 ans, et un dispositif biomédical tous les 7 à 10 ans. Son système d'exploitation devient donc obsolète bien avant la période de renouvellement, et le marquage CE laisse dans tous les cas peu de marge de manœuvre pour effectuer des mises à jour* », ajoute Sandrine Roussel, pour sa part ingénieure biomédicale au CHU de Besançon et co-pilote du même groupe de travail. Évoquant la nécessité de mener une réflexion à l'échelle européenne pour faire évoluer cette règlementation, elle souligne également l'urgence d'agir sans attendre de potentiels assouplissements : « *Il nous faut identifier dès à présent des exigences communes sur le plan de la cybersécurité des équipements biomédicaux, vers lesquelles nous pourrions tendre en collaboration étroite avec ces partenaires que sont les constructeurs* ».

**Une réflexion transversale**

Car l'évolution des pratiques sur le terrain avance, elle, à vitesse grand V : les médecins, notamment, sont très demandeurs d'une connectivité accrue des dispositifs biomédicaux. « *Ils réclament, avec raison, des résultats directement intégrés à leurs outils métiers* », indique Sandrine Roussel. Or le statu quo est souvent privilégié pour prévenir tout cyber-risque. « *Ce n'est pas à notre sens la bonne approche. Nous sommes d'ailleurs convaincus qu'il est possible de mettre en œuvre une stratégie de cybersécurité transversale, qui permettra à la fois de tirer pleinement profit des dernières avancées* ●●●

« **L'IDÉE EST SURTOUT DE PERMETTRE À UN ÉTABLISSEMENT DE SAVOIR À QUOI S'EN TENIR LORSQU'IL ACQUIERT UN ÉQUIPEMENT BIOMÉDICAL**, POUR POUVOIR METTRE EN ŒUVRE UNE STRATÉGIE ADAPTÉE »

*technologiques et de maîtriser les risques informatiques* », note-t-elle en rappelant qu'un système d'exploitation à jour ne constitue pas, pour autant, un totem d'immunité. « *Cela est important, et nous devons trouver le moyen de contractualiser cette obligation avec les constructeurs. Mais il faut également que les DSI/RSSI et les ingénieurs biomédicaux travaillent de concert pour appliquer les bonnes pratiques d'hygiène informatique aux dispositifs biomédicaux – fragmentation des réseaux, surveillance des vulnérabilités, élaboration d'un mode dégradé, etc. Les premiers construisent les routes, les seconds roulent dessus* », insiste Sandrine Roussel.

**Un document pour évaluer la maturité numérique des équipements**

Prenant la problématique à bras-le-corps, l'AFIB a créé dès 2019 un premier groupe de travail, alors dirigé par Sandrine Roussel et associant uniquement des ingénieurs biomédicaux. Un an plus tard, l'association dévoilait un questionnaire recensant les principaux points de vigilance pour évaluer la sécurité numérique d'un dispositif biomédical. Face à l'intérêt suscité par la démarche, un deuxième groupe de travail, cette fois-ci co-piloté par Sandrine Roussel, Benoît Fondeur, Akselle Godin (CHU de Bordeaux) et Loïc Dubois (GH Sud Île-de-France), voit le jour. Ses travaux, qui font l'objet d'un financement par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et l'Agence du numérique en santé (ANS), font également participer l'Association pour la sécurité des systèmes d'information de santé (APSSIS), le Service de santé des armées (SSA), le Commissariat à l'énergie atomique et aux énergies alternatives (CEA), et la centrale d'achat Uni.H.A. « *Nous avons pu faire évoluer le format du questionnaire, qui propose désormais, face à chaque exigence informatique, trois à quatre questions auxquelles le constructeur est appelé à répondre. La note attribuée permet ainsi d'évaluer la maturité informatique de l'équipement, pour appuyer le processus de décision lors d'un achat. Ce document a donc vocation à trouver sa place dans les cahiers des charges des appels d'offres publics* », explique Benoît Fondeur.

**De possibles mesures compensatoires**

« *Nous avons plus particulièrement identifié trois niveaux de maturité : le niveau 0, lorsque les exigences de cybersécurité n'ont pas été prises en compte lors de la conception de l'équipement ; le niveau 1, lorsqu'elles l'ont été mais que le constructeur n'est pas en mesure d'en fournir les preuves ; et le niveau 2, lorsque ces preuves existent et peuvent être consultées* », détaille Sandrine Roussel. Elle précise néanmoins que l'initiative ne cherche pas à « *punir* » ceux n'ayant pas intégré de démarche cybersécurité : « *Les constructeurs n'ont pas tous les mêmes ressources pour faire face à cet enjeu. Or l'existence d'un marché très concurrentiel doit à notre sens être préservée. L'idée est donc surtout de permettre à un établissement de savoir à quoi s'en tenir lorsqu'il acquiert un équipement biomédical, pour pouvoir mettre en œuvre une stratégie adaptée. Par exemple, lorsqu'un fournisseur est au niveau 0, nous suggérons des mesures compensatoires à déployer au niveau des interfaces techniques* ».

**Une consultation des constructeurs en cours**

L'AFIB continue d'ailleurs de réfléchir au bon positionnement du curseur pour trouver le meilleur équilibre entre contraintes et exigences. « *La tentation est grande de décorréler l'équipement de son système logiciel. Or, lorsque nous achetons un dispositif biomédical, nous achetons par la même occasion son système d'exploitation. Il s'agit d'un ensemble, que nous gérons comme tel. Aussi exigeons-nous que toute mise à jour de sécurité soit effectuée gratuitement dans le cadre des contrats de maintenance, car elle contribue au maintien en condition opérationnelle de nos équipements* », insiste Benoît Fondeur. Sandrine Roussel abonde : « *Nous sommes tout à fait disposés à chercher un terrain d'entente avec les constructeurs, mais nous n'abaisserons pas pour autant nos exigences. Par exemple, nous réfléchissons également à la mise en place d'un circuit de cybervigilance pour les équipements biomédicaux, sur le modèle de celui existant pour la matériovigilance. Un fournisseur ayant connaissance d'une faille de cybersécurité aura ainsi l'obligation d'en informer ses clients et d'agir en conséquence* ».

Pour justement nourrir cette réflexion, l'AFIB s'est rapprochée du SNITEM, le Syndicat national de l'industrie des technologies médicales, où la nouvelle mouture du questionnaire est en relecture. « *Nous attendons un retour courant 2024 pour apporter éventuellement des ajustements et diffuser le document à plus large échelle. Mais cette version intermédiaire est déjà connue des adhérents de l'AFIB, et nos prochaines journées nationales, qui se tiendront fin septembre à Bordeaux, seront l'occasion d'en discuter entre nous* », conclut-elle. En tout état de cause, la dynamique semble bel et bien lancée pour que la cybersécurité des équipements biomédicaux ne soit justement plus source d'inquiétudes.