DÉPÊCHE - Mercredi 16 décembre 2020 - 18:41

Cybersécurité : "Les ingénieurs biomédicaux doivent augmenter leurs exigences en matière de sécurité" (Afib)

Mots-clés : #établissements de santé #informatique #CHU-CHR #hôpital #dispositifs médicaux #qualité-sécurité des soins #données de santé #patients-usagers

PARIS, 16 décembre 2020 (APMnews) - L'Association française des ingénieurs biomédicaux (Afib) a présenté ses recommandations pour améliorer la sécurité numérique des équipements biomédicaux, lors d'une conférence en ligne organisée mardi soir.

"Conscients des enjeux que représentent pour les ingénieurs biomédicaux les questions de la sécurité numérique des équipements biomédicaux", l'Afib a constitué un groupe de travail afin de réaliser "un état des lieux de l'intégration des systèmes informatiques dans les équipements biomédicaux", "clarifier le rôle de l'ingénieur ou responsable biomédical dans cette évolution" et "proposer des recommandations pour améliorer la sécurité numérique des équipements biomédicaux".

L'Afib a en effet décidé en 2019 de mettre en place un groupe de travail constitué de 6 ingénieurs biomédicaux et dirigé par Sandrine Roussel, ingénieure biomédicale au CHU de Besançon. L'objectif étant de renforcer la sécurité numérique des équipements biomédicaux mais aussi réfléchir aux enjeux de formation.

Les équipements biomédicaux ont ceci de particulier qu'ils sont commercialisés par" des fournisseurs qui n'offrent pas le niveau de prestation attendu", a souligné Sandrine Roussel. "Il faut être plus exigeant vis-à-vis de ces fournisseurs".

Autre caractéristique, la durée de vie de ces équipements est au minimum de 10 ans et les systèmes informatiques sont rapidement obsolètes. "En 2019, au CHU de Besançon nous avions encore des équipements fonctionnant sous Windows 7", a fait remarquer l'ingénieure biomédicale.

Le nombre d'équipement biomédicaux dans un établissement de santé peut s'avérer très important. A l'instar du CHU de Besançon où les 3 ingénieurs biomédicaux assurent la maintenance de 22.000 équipements. "Mais tous ne sont pas connectés", a-t-elle précisé.

Autre point à souligner, la diversité des équipements est un frein à la sécurisation des systèmes.

De plus, les équipements biomédicaux ont une ouverture croissante vers l'extérieur. Et s'exposent donc de plus en plus à des attaques potentielles.

Enfin, la prise de conscience des enjeux de cybersécurité est tardive parmi les ingénieurs biomédicaux. "On s'est un peu trop reposé sur les responsables informatiques", a fait remarquer Sandrine Roussel. "Nous devons augmenter nos exigences en matière de sécurité des équipements auprès des fournisseurs."

Si isoler les équipements biomédicaux de l'environnement informatique de l'hôpital est une aberration, quelles sont alors les mesures à mettre en place pour mieux maîtriser cette sécurité ?

Les 5 recommandations de l'Afib

Après avoir travaillé pendant une année, les 6 experts de l'Afib ont rédigé un rapport de 20 pages. L'état des lieux et les 5 recommandations feront l'objet d'un article qui sera publié au premier trimestre 2021 dans la revue *IRBM News* (Innovation et technologie en biologie et médecine).

L'Afib propose **en premier lieu** d'intégrer la sécurité numérique dans les procédures d'acquisition des équipements biomédicaux et pour ce faire, elle recommande d'envoyer un questionnaire standardisé, d'environ 160 questions, aux fournisseurs.

"Ces questions permettent d'évaluer le degré de conformité des fournisseurs par rapport à la réglementation et leur degré de maturité. Il permet de recueillir les renseignements nécessaires à l'installation et à la gestion de la vie de l'équipement (sauvegardes, accès, codes génériques). L'avantage d'un questionnaire standardisé, c'est que les fournisseurs seront prêts à y répondre quel que soit l'établissement demandeur", a précisé Sandrine Roussel.

Deuxième recommandation, l'Afib propose de définir la collaboration dans les établissements de santé. "La gestion de la sécurité numérique ne se fait pas par le service biomédical seul dans son coin", a fait remarquer l'ingénieure. L'Afib propose donc que le service biomédical signe un "contrat de collaboration" à formaliser avec le service informatique, en définissant les équipements concernés, les renseignements nécessaires aux installations et la politique de sécurité numérique spécifique de l'établissement. Elle propose une revue régulière de ce contrat pour le faire évoluer. "Dans notre rapport, nous n'avons pas fourni de contrat type mais identifié des points de vigilance", a-t-elle précisé.

Elle recommande aussi d'établir une politique de sécurité numérique spécifique en lien avec la politique de l'établissement.

Troisième point, l'Afib recommande d'assurer la sécurité autour des équipements biomédicaux, en vérifiant qu'ils ont le marquage CE, que les accès sont gérés, que les sauvegardes réalisées, etc. "Ce sont des points de vigilance à destination des ingénieurs biomédicaux pour s'assurer que les dispositifs sont bien maîtrisés".

Quatrième point, les ingénieurs vont devoir définir la criticité des équipements biomédicaux vis à vis de la sécurité informatique. "Nous proposons une nouvelle notation de la vulnérabilité informatique en 10 points: est-ce que l'équipement est sur un réseau segmenté, est-ce que le système d'exploitation est à jour, y a-t-il un code d'accès sécurisé, est-ce que les données sont sauvegardées, est-ce que les ports USB sont bloqués, le dispositif est-il en interface avec d'autres applications, ou encore est-ce que les tests d'intrusion sont réalisés, etc."

Il faut donc identifier dans l'inventaire les équipements qui embarquent de l'informatique et pour chacun établir un score de vulnérabilité. L'objectif étant d'arriver à une vulnérabilité acceptable. "Le travail étant gigantesque, "nous allons d'abord noter les équipements nouvellement acquis".

La **cinquième recommandation** consiste à agir rapidement en cas de cyberattaque, car "il est impossible d'avoir un système 100% sécurisé". L'Afib relaie les recommandations faites par l'Agence nationale de la sécurité des systèmes d'informations (Anssi): "ne pas éteindre l'appareil, débrancher le réseau, s'assurer que les sauvegardes sont bien connectées au réseau et signaler l'incident."

A noter qu'il existe enfin un réel besoin de formation en matière de sécurité informatique. Si l'Anssi a travaillé sur un label de cybersécurité, "des formations en interne dans les établissements de santé sont également nécessaires", a conclu Sandrine Roussel.

"La prise de conscience étant récente, il est nécessaire de diffuser la culture informatique au sein des services biomédicaux afin d'augmenter nos exigences en matière de sécurité", a rappelé David Laurent, ingénieur biomédical au CHU de Grenoble.

gdl/ab/APMnews

[GDL1QLFWTJ]

POLSAN - ETABLISSEMENTS