GROUPE DE TRAVAIL **AFIB 2019–2020** : SÉCURITÉ NUMÉRIQUE DES ÉQUIPEMENTS BIOMÉDICAUX

[a] **V. Boissart** (ingénieure biomédicale), [b] **D. Laurent** (ingénieur biomédical) [c] **L. Monnin** (ingénieur biomédical) [d] **M.-J. Ory** (ingénieure biomédicale) [e] **F. Raji** (ingénieur biomédical) [f] **S. Roussel** (ingénieure biomédicale, coordinatrice du groupe de travail)*

[a] CHL - Centre Hospitalier de Luxembourg, Luxembourg, Luxembourg
[b] CHU de Grenoble, Grenoble, France
[c] Hôpital Nord Franche-Comté, Trévenans, FranceHôpital
[d] CHR de Metz-Thionville, Metz Thionville, France
[e] CHU Dijon Bourgogne, Dijon, France
[f] CHU de Besançon, Besançon, France

Définir la vulnérabilité des équipements biomédicaux au regard de la sécurité numérique

Il convient d'évaluer, équipement par équipement, la vulnérabilité des dispositifs médicaux. Pour cela, il faut utiliser une échelle de cotation permettant de pointer les caractéristiques liées au système informatique qui constituent des portes d'entrées ou des faiblesses permettant l'accès aux données personnelles des patients, la modification de ces données, d'interférer sur le fonctionnement du dispositif médical ou de constituer un point d'entrée vers les autres équipements.

QUESTIONNAIRE DE VULNERABILTÉ

Dans la perspective d'une analyse de risque dédiées aux équipements, les éléments les plus couramment identi-fiées, et pouvant être utilisés pour défi¬nir un score de vulnérabilité sont listés dans le tableau 1.

Cette évaluation concerne l'ensemble des équipements embarquant ou associés à des systèmes informatiques, qu'ils soient connectés sur le réseau informatique ou non. Les critères et leur niveau d'acceptabilité pourront être précisés en amont avec le service informatique et le RSSI afin de défi¬nir un niveau d'exigence plausible et en accord avec la politique de sécu¬rité numérique de l'établissement. La cotation sera réalisée avec l'aide du service informatique qui dispose des éléments sur la structuration du réseau, les patchs et mises à jour, le stockage, les flux…

Tableau 1 : notation en 10 points de la vulnérabilité numérique des équipements biomédicaux

Critères	Réponse OUI	Réponse NON	Points à préciser avec les utilisateurs et le service informatique
Equipement sur un réseau segmenté	0	1	Le bon niveau de segmentation
Système d'exploitation supporté, mises à jour de sécurité réalisées	0	1	Définir précisément l'obsolescence et le maintien en condition de sécurité
Code d'accès sécurisé	0	1	Définition d'un accès sécurisé en rapport avec la politique de l'établissement
Pas de communication Wifi du DM ou communication sur un réseau Wifi sécurisé	0	1	Degré de sécurité acceptable de la communication Wifi
Stockage et sauvegarde délocalisée des données	0	1	Définir ce qui doit être sauvegardé et le temps de conservation
Blocage des ports d'entrée non utilisés ou sécurisation des ports	0	1	Utilité de garder des ports fonctionnels ou pas. Niveau de sécurité acceptable
Interfaces entre des applications externes au dispositif médical connues, sécurisées et limitées au strict nécessaire	0	1	Nécessité de ses interfaces, sécurisation des interfaces externes
Système d'information inventorié et suivi	0	1	Qui conserve la fiche d'identification, qui suit les mises à jour
Patch de sécurité installé et mis à jour	0	1	
Audits de sécurité, tests d'intrusions réalisés	0	1	Fréquence minimum des tests d'intrusion
Score de vulnérabilité		/10	

SCORE DE VULNERABILITÉ

Le score de vulnérabilité sert ensuite à calculer un niveau de vulnérabilité qui permettra une priorisation des actions. La proposition du groupe de travail est une cotation en trois niveaux de vulnérabilité, évaluée selon le tableau.
L'objectif est d'identifier les équipements vulnérables puis d'établir un plan d'action et de faire baisser le score de vulnérabilité à un niveau acceptable pour l'ensemble des équipements.

	Scores de vulnérabilité				
Vulnérabilité forte	6	7	8	9	10
Vulnérabilité modérée	3	4	5		
Vulnérabilité acceptable	1	2			

(En rouge : niveau d'action prioritaire ; en orange : niveau d'action conseillé ; en vert : simple surveillance.)

EXEMPLES D'ACTIONS CORRECTIVES

Les actions listées dans le tableau 2 peuvent être entreprises, en concertation avec le service informatique pour faire baisser le niveau de vulnérabilité numérique. Le plus adapté est de réaliser ces actions à l'installation du dispositif médical, en ayant pris soin de les préparer et de les inscrire dans les documents de consultation.

Tableau 2 : exemple d'actions à mettre en place pour abaisser le niveau de vulnérabilité numérique des équipements biomédicaux.

Critères	Actions
Equipement sur un réseau non segmenté	Segmentation du réseau et déplacement des équipements sur le réseau
IOS obsolète	Upgrade de l'IOS, renouvellement partiel ou total de l'équipement
Code d'accès non sécurisé	Modification des codes d'accès, instauration de règles
Communication en Wifi	Mise en place d'une communication Wifi sécurisé
Stockage–sauvegarde délocalisée	Mise en place de sauvegardes
Un ou plusieurs ports d'entrée fonctionnels	Blocage des ports non utilisés, blocage de l'AutoRun Utilisation de stations blanches
Interface avec d'autres applications	Couper les interfaces non nécessaires à la prise en charge médicale
Système d'information non inventorié, non suivi	Inventorier les logiciels et postes informatiques, suivre les maintenances et mises à jour
Patch de sécurité non installé	Inscrire les mises à jour de sécurité dans les contrats de maintenance, privilégier un poste informatique de l'établissement, géré par le service informatique
Audit, test d'intrusion non réalisé	Instaurer des tests d'intrusion réguliers

L'intégralité du cahier technique est à retrouver sur le site de l'AFIB.

IRBM News 2021 ; 42 (1) : 100298 https://doi.org/10.1016/j. irbmnw.2021. 07.001