Sécurisation et Vigilance des DM et DMDIV

Réflexions et travaux de l'AFIB sur la cybersécurité des dispositifs médicaux

Le contexte

Le contexte

- Intégration de plus en plus fréquentes des équipements biomédicaux aux systèmes d'information hospitaliers
- Emergence d'innovations biomédicales (objets connectés, e-santé, télémédecine, intelligence artificielle, …) qui sont de véritables solutions informatiques intégrant des données sensibles à garder confidentielles
- Réglementation qui évolue (marquage CE, cyber Resilience Act, NIS 2…) avec nécessité de renforcer la sécurité informatique des équipements biomédicaux
- Attaques Cyber de plus en plus nombreuses et impactantes sur les hôpitaux,
- Besoin de faire évoluer les référentiels et les pratiques
- Besoin de mieux définir la collaboration entre DSI et biomédical

LA CYBERSECURITE
LES CONSTATS

CONTAT N° 1

Les équipements biomédicaux connectés augmentent la surface du risque d'attaque des hôpitaux.

CONSTAT N° 2

Les équipements biomédicaux ne répondent pas aux règles de sécurité numériques.

CONSTAT N° 3

La coopération entre la direction des services numériques et direction biomédical dans les établissements de santé doivent évoluer.

CONSTAT N° 4

Nos équipes ne sont pas suffisamment formées aux règles de sécurité numériques.

L'AFIB ET LA CYBERSECURITE
LES RELATIONS INSTITUTIONNELLES

APSSIS

Participation croisée aux différents congrès.
- Rencontres régulières.

Rencontre Annuelle avec:

L'Agence Nationale de la Sécurité des Systèmes d'Information

snitem
Syndicat National de l'Industrie des Technologies Médicales

Rencontre Annuelle avec:

Le SNITEM pour faire remonter nos problématiques liée à la vie des dispositifs biomédicaux . (et sur la prise en compte des aspects CYBER)

Groupe de travail du CA de l'AFIB composé de 4 Ingénieurs

CLUB RSSI SANTÉ

Création d'un groupe de travail commun AFIB-CLUB RSSI:
- Sur le Clausier RSSI

CONFÉRENCE DES DIRECTEURS GÉNÉRAUX DE CHRU

Création d'un groupe de travail spécifique sur le sujet de la Cybersécurité.

LES 3 ENJEUX MAJEURS POUR LE BIOMEDICAL

PREVENIR

Comprendre où se situent les failles potentielles et évaluer les risques associés

DETECTER

Mettre en place des outil de détection.
Une fois les risques identifiés, il est crucial de les prioriser.

REAGIR

Un plan d'action comprenant des mesures à court, moyen et long termes doit en découler.

Technicien : Personne majeur
Doit être impliqué dans cette démarche

Les actions réalisées

Démarche de l'AFIB en 2023 et 2024

- Constat 2022 : chaque établissement à (au mieux) son propre questionnaire d'une centaine de questions créé par son RSSI pour les achats de DM connecté
- 2023 : France relance finance des audits des services biomédicaux sur la question de la cybersécurité des DM: les constats sont similaires (et souvent décevant)
- Prise de contact entre AFIB et France relance/ANSSI pour avoir une action/réponse transverse et commune au même besoin
- Financement par France relance d'un travail commun géré par l'AFIB
- Groupe de travail RSSI+Biomédicaux+Advens. Objectif: avoir des objectifs cyber dans tous les futurs achats de DM et pouvoir opposer des pénalités dans les cahiers des charges aux fournisseurs

Les 4 solutions

Proposition 1 : Prévenir et agir dès l'achat des équipements biomédicaux

- Introduire les exigences de sécurité informatique dans les achats avec une harmonisation nationale tenant compte des évolutions (ex des questionnaires AFIB et clausier RSSI)

- Mettre en place la coordination : (RSSI / DPO / DSN / BIOMED)
  - Circuits rapides de validation des demandes
  - Coordination des installations d'équipements (RSSI / DPO / DSN / BIOMED)
  - Limiter l'intégration à ce qui est nécessaire

=> points à travailler avec la Commission des Systèmes d'Information et esanté

Proposition 2 : Collaborer

- Intégrer des compétences croisées DSN/BIOMED
- Proposer un contrat type de collaboration => point collab CSI
- Redéfinir les rôles et les responsabilités (équipements frontières, traçabilités, outils…) => point collab CSI
- Parler de la consommation de ressources
- Travailler en mode projet et anticiper les budgets des différentes directions
- Anticiper les modes de financement. Identifier les budgets
- Participer aux actions de formation internes et externes

Proposition 3 : Connaitre : gestion des actifs et cartographie

- Le service biomédical reste le garant du bon fonctionnement des équipements biomédicaux
- Cartographie des actifs est une obligation (directive 2016/309)
- Recommandations sur la connaissance des actifs et l'intégration à la GMAO => point collab CSI
- Contribution du service biomédical aux plans de continuité et de reprise de l'activité (PRA / PCA)
- Partager les outils de la DSN pour la sécurité des données, veiller aux clauses de confidentialité et RGPD dans les contrats

Proposition 4 : Détecter, réagir : être actif dans la recherche des failles et corriger

- Trouver des techniques informatiques pour compenser les manquements des équipements biomédicaux (ex EDR/XDR, antivirus)

- Le maintien en condition de sécurité est une obsolescence supplémentaire qui rend obligatoire les contrats de maintenances et qui pose la question de la pertinence des durées d'amortissement et des modèles d'achats

- Mettre en place des tests d'intrusion sur les équipements biomédicaux (en lien avec RSSI)

Pour aller plus loin

Et en Europe ? (le Cyber Resilience Act)

- Le CRA exclu les Dm et DMDIV de son champ d'application
- La directive NIS 2 organise la défense européenne face aux cyber-attaque et impose aux établissements des mesures préventives er réactives plus strictes ➔ Les RSSI sont de plus en plus exigeants, (et c'est normal).
- Le Marquage CE (selon le RE 2017/745 ou 746) ne traite qu'indirectement la cyber sur la base d'une analyse de risque :
  - Risque principal=risque direct sur patient
  - Le risque d'exploitation d'une faille est indirect (et dépend de l'environnement)
- Pour limiter les risques de dysfonctionnement, le fabriquant stabilise ses versions au maximum. Les mouvements peuvent même être antinomiques :
- La marque CE est jugé suffisante dans le CRA, mais insuffisante pour les RSSI