Master Ingénierie de la Santé - Technologies Biomédicales et Territoires de Santé - 2023/2024 - IDS 213
Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/
DOI : https://doi.org/10.34746/ids213

"LA CYBERSÉCURITÉ ET LES DISPOSITIF MÉDICAUX"

CONTEXTE

Au sein des établissements de santé, l'intégration de **technologies numériques dans les dispositifs médicaux (DM)** offre de nombreux avantages en améliorant la qualité des soins et la prise en charge des patients. Cependant, ces dispositifs ouverts et connectés peuvent présenter de **potentielles vulnérabilités** et créer des failles de sécurité exploitables par des acteurs malveillants.

LES RISQUES CYBER LIÉS AUX DM

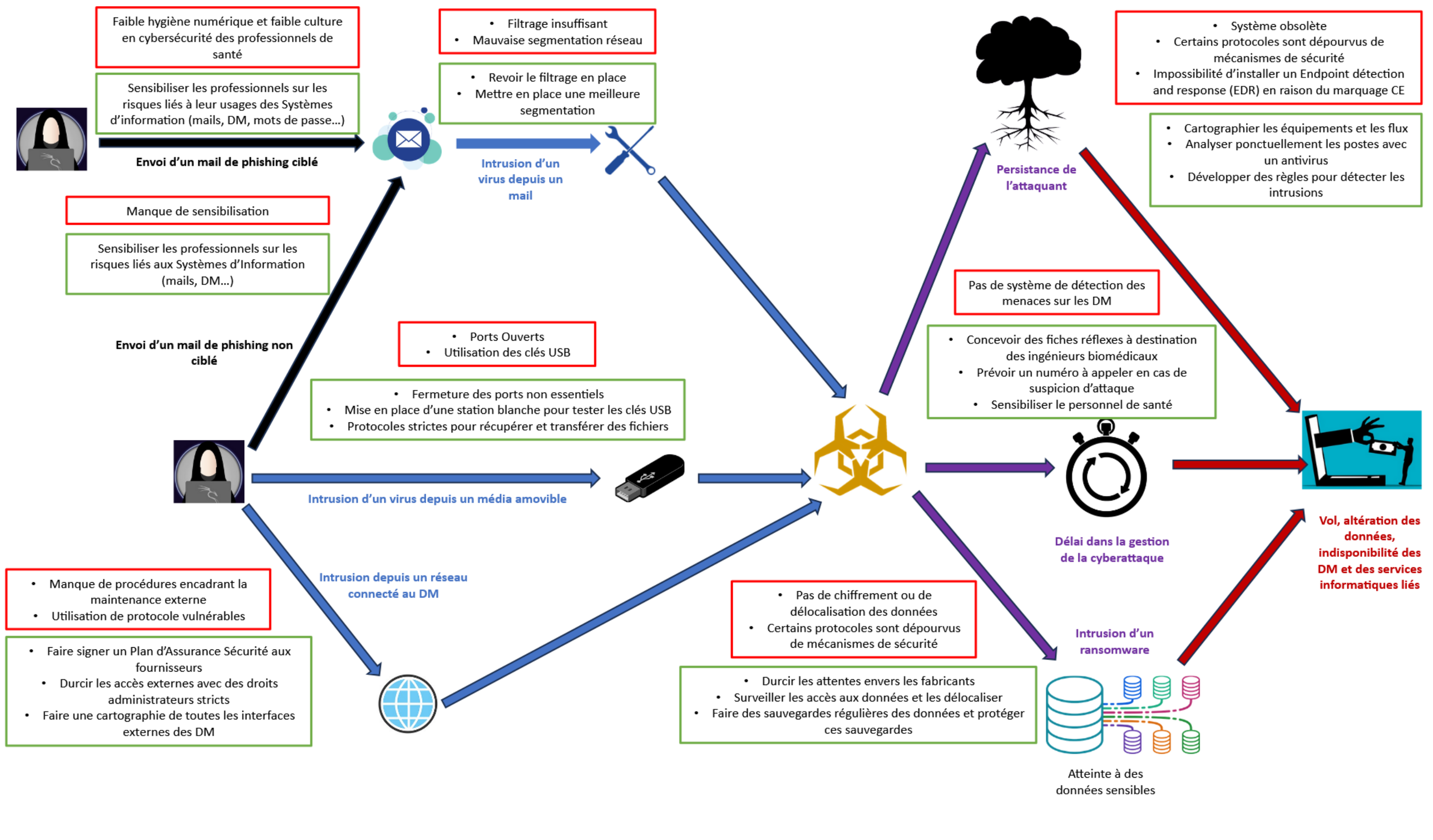
- **Dégradation de la prise en charge des patients**
- **Divulgation de données** de santé pouvant atteindre la vie privée des patients.
- **Désorganisation** des établissements.
- **Altération des paramétrages** des dispositifs médicaux (exemple : modification des unités de mesure).
- Altération des résultats et/ou des données d'**identification des patients.**
- **Arrêt ou prise en main à distance** des équipements (exemple : équipements de chirurgie).

LES MAUVAISES PRATIQUES

- **Manque de dialogue et de compréhension** entre le service informatique et le service biomédical (exemple : pas ou peu d'analyse de risque en commun).
- Manque de clarté sur **l'affectation des budgets** liés à la sécurisation du Système d'Information Technique Hospitalier.
- **Manque de cloisonnement** des systèmes d'information critiques pour l'hôpital.
- Mauvaise maîtrise des **accès de télémaintenance.**
- **La cartographie du parc des équipements** n'est pas disponible.
- **Manque de formation** du personnel qui n'a pas les compétences pour réagir à un incident de sécurité.
- **Manque de moyens de détection et de protection des attaques,** rendant difficile la gestion des incidents de sécurité.
- Manque de prise en compte des **exigences de cybersécurité par les fournisseurs.**

UNE CYBERATTAQUE TYPIQUE

Les **rectangles rouges** indiquent les mauvaises pratiques entraînant une cyberattaque potentielle.
Les **rectangles verts** indiquent des solutions éventuelles pour pallier au développement d'une cyberattaque.



Master Ingénierie de la Santé - Technologies Biomédicales et Territoires de Santé - 2023/2024 - IDS 213
Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/
DOI : https://doi.org/10.34746/ids213

LA CYBERSÉCURITÉ ET LA COLLABORATION

CONTEXTE

L'AFIB a proposé 4 recommandations en lien avec la prévention des cyberattaques dans le document : **Définir la collaboration dans les établissements de santé.** [1]
Cette recommandation a pour objectif de proposer un **fonctionnement et une ligne de partage entre le service biomédical et et le service informatique** grâce aux retours d'expérience de différents établissements de santé.

DEFINIR LES MODALITÉS DE LA COLLABORATION

Service Biomédical

- Vérification du **bon fonctionnement** après une intervention, une mise à jour ou la modification d'une interface.
- Le **référent biomédical** doit être informé de toute modification.
- Définir le besoin de **sauvegardes**, leur récupération et leur fin de vie.
- Responsable pendant toute la **durée de vie** de l'équipement.

Service Informatique

- Mettre en place les **réseaux** LAN (Local Area Network) propriétaire spécifique pour les équipements médicaux (éviter le Wifi si possible).
- **Achats** sur les recommandations du service biomédical.
- Un **référent informatique** est nommé pour les diagnostics, dépannages et modification sur les équipements médicaux.
- Effectuer les **sauvegardes** sur un serveur sécurisé.

IDENTIFIER ET SUIVRE LES LOGICIELS

Nouvelle application = fiche d'identification de l'application

- Nom du logiciel
- Version
- Fournisseur
- Poste informatique
- Interfaces
- Serveurs
- Type de connexion au réseau
- Sauvegardes et modalités
- Modalités de protection
- Modalités de restauration en cas de pannes

La gestion et la conservation des fiches **dépendent du poste informatique** sur lequel est installé l'application

Postes propriétés de l'**établissement** → **Service informatique**

Postes propriété du **fournisseur** → **Service biomédical**

Cette fiche permet de gérer l'obsolescence des systèmes d'exploitation et de mieux répartir le suivi et les actions entre le service biomédical et l'informatique.

DEFINIR LE PERIMETRE

Revient à définir clairement parmi les logiciels et poste de travail ceux qui sont de la responsabilité du service biomédical. Cette définition du périmètre doit être revue chaque année

Sous la responsabilité du service biomédical :

- Les logiciels et applications marqués CE et relevant du statut de DM ou de DM de diagnostic In vitro
- Les systèmes d'information embarqués dans les DM
- Les serveurs internes ou externes captifs des fournisseurs d'équipements
- L'architecture réseau en VLAN et/ou WIFI des DM
- Les postes informatiques de pilotage ou supervision des équipements biomédicaux nécessitant des performances ou cartes d'acquisition spécifiques ou pour lesquels le fournisseur déconseille fortement l'utilisation d'un poste informatique autre que celui fourni avec l'équipement.

[1] V. BOISSART, D. LAURENT, L. MONNIN, M.-J. ORY, F. RAJI, et S. ROUSSEL, « GROUPE DE TRAVAIL AFIB 2019-2020 : Sécurité Numérique des équipements biomédicaux », no 42, p. 18, févr. 2021, doi: https://doi.org/10.1016/j.irbmnw.2021.100298