

1 LA CYBERSÉCURITÉ ET LES ÉTABLISSEMENTS DE SANTÉ

DONNÉES 2022

- **730 déclarations d'incidents** de cybersécurité [1] (tentatives d'attaques : 70% phishing, comportement inhabituel de comptes...)
- **30% d'incidents de plus** qu'en 2021
- **27 attaques par rançongiciel** réussies [2]
- **39%** des établissements de santé ont dû faire fonctionner les **services en mode dégradé**
- **63%** disent avoir vu un **impact direct sur la donnée** du patient et l'organisation interne

Prise en charge des patients
Fuite des données, perte de sécurité et de continuité des soins

Changement des pratiques et réglementation
Responsabilité accrue des personnels des services informatique, biomédical et de soins dans la gestion des risques cyber

RGPD, "Dispositifs médicaux" (2017/745 et 2017/746)

SG/DSSIS/2016/309

5 ENJEUX MAJEURS

Certification HAS v2024
Gestion des risques numériques dans la prestation des soins

HAUTE AUTORITÉ DE SANTÉ

Impacts financiers
Perte de chiffre d'affaires, reconstruction du Système d'Information

Répartition des rôles
Entre service biomédical et service informatique

Exemple : définir parmi les logiciels et postes de travail ceux sous la responsabilité d'un service

2 AIDER LES INGÉNIEURS BIOMÉDICAUX À INTÉGRER LA CYBERSÉCURITÉ DANS LES DISPOSITIFS MÉDICAUX

Outil 1 : Sécurité numérique et achats

Objectif
Faciliter la prise en compte des risques cyber lors des achats

Environ 20 minutes de lecture
Logigramme des questions posées et aide à la saisie des réponses

Questions réparties en 4 blocs

Dispositif → Serveurs et architectures logicielles → Logiciels → Maintenance et sécurité

Le logiciel peut-il envoyer des données dans le dossier patient?

Publication, en 2021, d'un document concernant la **sécurité numérique des équipements biomédicaux** [3]
4 recommandations adaptées à la prévention des cyberattaques

Outil 2 : Collaboration entre service biomédical et informatique

Objectif
Encourager et faire des propositions pour favoriser la collaboration

Fiche de 2 pages

1 LA CYBERSÉCURITÉ ET LES DM

- Risques cyber
- Mauvaises pratiques
- Schéma d'une cyberattaque typique (erreurs et solutions)

2 LA CYBERSÉCURITÉ ET LA COLLABORATION

3 axes de collaboration de l'AFIB :

- Définir les modalités de la collaboration
- Identifier et suivre les logiciels
- Définir le périmètre des ingénieurs biomédicaux

Outil 4 : Analyse et gestion des risques cyber d'un DM

Objectif
Élaborer des plans d'actions adaptés aux risques cyber des DM

Environ 10 minutes

Exemple : **moniteurs multiparamétriques**

Analyser la criticité → Analyser la vulnérabilité → Remplir la matrice du risque → Élaborer des plans d'actions

Criticité : 22/36 Criticité modérée → Vulnérabilité : 5/10 Vulnérabilité modérée

Vulnérabilité numérique du dispositif médical	Niveau de criticité du DM		
	Forte	Modérée	Acceptable
Forte			
Modérée		X	
Acceptable			

9 niveaux de plans d'actions

NOTRE CONTRIBUTION

Élaboration de 4 outils en fonction des recommandations de l'AFIB

Vidéo globale d'explication

Outil 3 : Sensibilisation

Objectif
Vidéo de 4 minutes que le service biomédical peut transmettre aux personnels de santé pour comprendre les **risques cyber liés aux DM** (périphériques USB notamment)

3 RETOURS SUR LES OUTILS

28 téléchargements (25/01/2024)

9 retours d'expérience d'ingénieurs biomédicaux principalement de CHU ayant permis d'adapter les outils à la réalité du terrain

- Améliorations possibles :**
- Avoir des retours de services informatiques hospitaliers
 - Fonctionnalité de pré-saisie de l'outil 4
 - Intégrer les résultats de l'outil 4 dans la GMAO

4 BIBLIOGRAPHIE

[1] E. BOUSSIN et J. SCHREIBER, « Retour sur les grandes cyberattaques en France en 2022 : quelles résolutions pour 2023 ? », Portail de l'Intelligence Économique. Consulté le : 19 décembre 2023. [En ligne]. Disponible sur : <https://www.portail-ie.fr/univers/risques-et-gouvernance-cyber/2023/retour-sur-les-grandes-cyberattaques-en-france-en-2022-quelles-resolutions-pour-2023/>

[2] NDMN, « Cybersécurité en France, 10 statistiques clés à connaître en 2021 ! », 8 juin 2022. Consulté le : 20 septembre 2023. [En ligne]. Disponible sur : <https://www.ndmn.fr/statistiques-cybersecurite-2022>

[3] 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 », IRBM News, février 2021, vol. 42, n°1, p. 100298, doi: <https://doi.org/10.1016/j.irbmw.2021.100298>