Analyse des risques de cybersécurité pour les dispositifs médicaux

Analyse des risques associant le questionnaire de vulnérabilité et la méthode M.A.C.E |
Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | 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

Définitions

Nous aborderons dans cet outil de présentation deux grandes notions :

- **La criticité** : Selon la norme ISO 60812 la criticité est définie comme “la combinaison de la sévérité d’un effet et de la fréquence de son apparition , ou d’autres attributs d’une défaillance comme une mesure de la nécessité d’un traitement ou d’une atténuation.”

Nous avons fait choix de la méthode M.A.C.E (**Méthode d’Analyse de la Criticité des dispositifs médicaux en Exploitation**)

- **La vulnérabilité** : Selon L’ANSSI (Agence nationale de la sécurité des systèmes d’informations) [6], la vulnérabilité d’un réseau ou d’un système d’information est “une faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l’installation ou la configuration d’un système, ou dans la façon de l’utiliser.

Remarque : Une vulnérabilité peut être utilisée par un code d’exploitation et conduire à une intrusion dans le système”.

Nous avons choisi de prendre un tableau réalisé par le **groupe de travail de l’AFIB 2019-2020** car l’échelle de cotation permet de pointer les caractéristiques liés au système informatique des dispositifs médicaux

Contexte

A lire

L'AFIB a proposé **4 recommandations** en lien avec la prévention des cyberattaques dans le document: *Définir le niveau de risque associé aux équipements biomédicaux* [1]

Cet outil se concentre sur la dernière recommandation : **Définit le niveau de risque associé aux équipements biomédicaux**

Introduire la sécurité numérique dans les procédures d'acquisition

Définir la collaboration dans les établissements de santé

Assurer la sécurité autour des équipements biomédicaux

Définir le niveau de risque associé aux équipements biomédicaux

Fonctionnement de l'outil

Icônes cliquables	Description
	Cette icône permet de revenir à la page "Contexte"
	Ces flèches (peu importe leur couleur), situées aux sommaires, permettent d'amener à la partie associée
	L'icône permet de ramener à la page "Sommaire"
	Permet de renvoyer vers les informations utiles pour la compréhension des différentes questions des questionnaires
	Ces flèches (peu importe leur couleur) permettent de ramener à la matrice de risque final lorsque l'on se situe dans les actions à mettre en place
	Cette icône permet de passer à la diapositive suivante
	Cette icône permet de passer à la diapositive précédente

 Cette icône indique des informations complémentaires

 Cette icône indique des pistes d'actions

Utilisation de l'outil

Remplir les différentes questions de criticité, calculer le score sur 36 points et positionner l' équipement dans les différentes catégories

Remplir les différentes questions de vulnérabilité, calculer le score sur 36 points et positionner l'équipement dans les différentes catégories

Combiner les résultats des analyses précédentes pour obtenir une catégories de risques.

A partir de chaque catégorie de risque vous aurez accès à des idées de plans d'actions à mettre en place (Source : [3])

Vous pouvez utiliser cet outil de plusieurs façons :

- Réaliser cette analyse à l'achat de **chaque dispositif médical**
- Réaliser cette analyse par code **CNEH** (Centre National de l'Expertise Hospitalière)
- Réaliser cette analyse par code **EMDN** (Nomenclature européenne des dispositifs médicaux)

Cet outil vous permet de faire l'étude de l'état actuel des risques des dispositifs médicaux (cartographie) et de les classer par ordre de priorité en ce qui concerne les actions de cybersécurité à mettre en place. Cet ordre de priorité vous aidera à mettre en place des actions pour renforcer la protection des dispositifs médicaux.

TEMPS DE REMPLISSAGE TOTAL ESTIMÉ : 5 À 10 MINUTES

Sommaire

Analyse de la criticité d'un Dispositif Médical

Analyse de la vulnérabilité d'un Dispositif Médical

Matrice du risque selon la vulnérabilité numérique

Vous pouvez cliquer pour accéder aux questionnaires

Analyse de la criticité d'un Dispositif Médical

Réponse (Nombre de points) Critère	1	2	3	4	Numéro de réponse
SERVICE BIOMÉDICAL (Estimation de l'impact du critère sur la criticité)					
Classe CE du Dispositif Médical (DM)	I : Faible degré de risque	IIa : Degré moyen de risque	IIb : Degré de risque élevé	III : Degré de risque très sérieux	
Vétusté du DM (fréquence d'usage, âge, conditions d'emploi)	Équipement neuf	Équipement mature	Équipement vétuste	Équipement à renouveler/réformer	
Fréquence d'apparition d'une défaillance du DM, ou de son environnement technique	Défaillance exceptionnelle	Défaillance rare	Défaillance occasionnelle	Défaillance fréquente	
Détectabilité de la panne du DM, ou de son environnement technique	Facilement détectable	Détectable	Difficilement détectable	Indétectable/Aucun signe avant-coureur	
Délai de la maintenance du DM, ou de son environnement technique	Délai court/dispositif de remplacement disponible	Service après vente rapidement disponible	Délai plus ou moins tolérable	Délai très long et absence de dispositif de remplacement	
SERVICE UTILISATEUR (Estimation de l'impact du critère sur la criticité)					
Usage fait du DM (compétences du personnel, dangerosité de l'acte médical, ergonomie d'utilisation)	Usage en service de soins ou HAD à risque faible	Usage en service de soins ou HAD à risque peu important	Usage en service de soins ou HAD à risque important	Usage en service de soins ou HAD à risque élevé	
Valeur technique (plus value, vétusté fonctionnelle) du DM	Dernière génération	Génération actuelle	Génération vieillissante	Totalement obsolète	
Dépendance du DM à un défaut de l'environnement technique	Compatible avec un fonctionnement continu	Plusieurs alternatives techniques envisageables	Une alternative technique envisageable	Inopérant en cas de défaut de l'environnement technique	
Gravité des pannes en cas d'arrêt du DM	Aucune répercussion	Répercussions légères sur la qualité des soins	Répercussions sur la sécurité des soins	Répercussions graves sur la continuité des soins	

Score final	/36

Niveau 1 (de 0 à 12 points)	Criticité acceptable	Niveau 2 (de 13 à 24 points)	Criticité modérée	Niveau 3 (de 25 à 36 points)	Criticité forte

Analyse de la vulnérabilité d'un Dispositif Médical

CRITÈRES	RÉPONSE	OUI	NON
L'équipement est sur un réseau segmenté		0	1
Le système d'exploitation est supporté et les mises à jour de sécurité sont réalisées		0	1
Le code d'accès est sécurisé		0	1
Le dispositif médical ne communique pas en Wifi ou la communication se fait sur un réseau Wifi sécurisé		0	1
Les données sont stockées et sauvegardées de manière délocalisée		0	1
Les ports d'entrée non utilisés sont bloqués et les autres sont sécurisés		0	1
Les interfaces entre des applications externes au DM sont connues, sécurisées et limitées au strict nécessaire		0	1
La fiche d'identification du système d'information est conservée par la personne compétente et les mises à jour et changement de protocoles sont suivies		0	1
Le patch de sécurité est installé et mis à jour		0	1
Des audits de sécurité et des tests d'intrusions sont réalisés avec une fréquence acceptable		0	1

Score final	/10

Niveau 1 (score entre 0 et 2)	Vulnérabilité acceptable	Niveau 2 (score entre 3 et 5)	Vulnérabilité modérée	Niveau 3 (score entre 6 et 10)	Vulnérabilité forte

Matrice du risque selon la vulnérabilité numérique en fonction de la criticité d'un Dispositif Médical

Matrice du risque selon la vulnérabilité numérique en fonction de la criticité d'un Dispositif Médical

		Niveau de criticité du Dispositif Médical		
		Forte	Modérée	Acceptable
Vulnérabilité numérique du Dispositif Médical	Forte			
	Modérée			
	Acceptable			

Plans d'actions possibles selon chaque niveau de risque (***Cliquez sur le texte ci-dessous pour voir les informations correspondantes***) :

Risque acceptable (Simple surveillance nécessaire)	**Risque modéré** (Niveau d'action conseillé)	**Risque fort** (Niveau d'action prioritaire)

Classe CE des Dispositifs Médicaux selon le règlement 2017/745

Le règlement 2017/745 [8] relatif aux dispositifs médicaux classe ces derniers sous 4 grandes catégories :

- **Classe I** : Dispositif à faible degré de risque
- **Classe IIa** : Dispositif à degré de risque moyen
- **Classe IIb** : Dispositif à degré de risque élevé
- **Classe III** : Dispositif à degré de risque très sérieux

La catégorisation en classe se fait selon deux grands critères :

- Le **temps d'utilisation/d'implantation** du dispositif à destiné du patient
- Le **type d'usage** du dispositif

Il existe une classe I spéciale que l'on ne prendra pas en compte de manière distincte ici

Vétusté du DM (fréquence d'usage, âge, conditions d'emploi)

Un DM est jugé comme obsolète lorsqu'il répond à 1 de ces 3 catégories [4], [5] :

- Lorsqu'il **perd ses performances initiales**
- Lorsque ses **performances sont insuffisantes** donnant recours au besoin de l'utilisation de nouvelles technologies médicales,
- Lorsque d'autres dispositifs médicaux, ayant une meilleure sécurité d'utilisation et/ou pour le patient, sont **disponibles sur la marché**

En règle générale, un DM est jugé obsolète, **en moyenne**, au bout de **7 ans d'utilisation**.

7 ans est une moyenne car certains DM (pousse-seringue, moniteurs multiparamétriques…) sont obsolètes au bout de 10 ans d'utilisation et certains DM (gros appareils d'imagerie comme scanners, échographes) le sont au bout de 5 ans d'utilisation

Pour déterminer la vétusté de votre dispositif il est donc nécessaire de se tenir au courant de ce qui se fait sur le marché et de tenir compte des maintenances préventives et curatives

Fréquence d'apparition d'un défaillance du DM, ou de son environnement technique

Il faut déterminer le nombre de fois qu'une **panne est présente sur un DM en l'espace d'un an**.

A titre d'information :

- Un dispositif ayant une **défaillance exceptionnelle** est un DM qui tombe en panne 1 ou 2 fois par an
- A l'inverse un dispositif ayant une **défaillance fréquente** est un DM qui tombe en panne 6 fois par an ou plus

Les données chiffrées ne font pas foi. Elles sont le reflet de différentes expériences que nous avons vécues au cours de notre formation.

Détectabilité de la panne du DM, ou de son environnement technique

Dans cette partie, il faut déterminer toute technologie ou composant présent dans un Dispositif Médical permettant de faciliter la détection d'une panne :

- Le DM possède un **système d'alarme** en cas de problème,
- La capacité du DM à faire un **auto-test**
- L'ergonomie du DM permet la **visualisation d'une panne**
- L'ergonomie du DM permet d'indiquer la **localisation de la panne**
- Toute autre information qui vous paraît pertinente

Les données ci-contre ne font pas foi. Elles sont le reflet de différentes expériences que nous avons vécues au cours de notre formation.

Délai de la maintenance du DM, ou de son environnement technique

Dans cette partie, il faut déterminer des facteurs externes qui permettent d'effectuer la maintenance sur un DM tombé en panne [2]:

- **Rapidité de réponse du service biomédical** (Délai entre le moment ou le DM n'est plus dans son service d'origine jusqu'au moment ou il revient)
- Prêt d'un DM
- **Rapidité de réponse du service après-vente** de l'entreprise qui a construit le DM
- Toute autre information qui vous paraît pertinente

Usage fait du DM (compétences du personnel, dangerosité de l'acte médical, ergonomie d'utilisation)

Cette partie se concentre sur l'usage du dispositif médical, les critères d'utilité, l'environnement d'utilisation et le personnel l'entourant.

Il faut ainsi prendre en compte [1] :

- **Qui l'utilise**, si les personnes sont formés (tout l'appareil, partie de l'appareil).
- **Quels types d'actes médicaux** sont permis par le matériel et la gravité de l'acte rapporté au patient
- **Les conditions d'utilisation de l'appareil** en lui-même (s'il doit se trouver en salle stérile, avoir un régime électrique particulier, …)
- Toutes autres informations qui vous paraissent pertinentes

Valeur technique (plus value, vétusté fonctionnelle) du DM

Il est simplement demandé ici de déterminer la valeur que porte les équipes soignantes à l'appareil à travers la mention de **plus value.**

Le critère de notation met également en évidence la **vétusté fonctionnelle** du DM et donc la "nouveauté" de l'appareil et/ou de la technologie aux sein du service.

La **vétusté fonctionnelle** du dispositif médical correspond à la dégradation naturelle des fonctions et éléments du dispositif dût à son utilisation.

Dépendance du DM à un défaut de l'environnement technique

Dans cette partie, c'est la **résilience** du DM en cas de problème dans les services qui est évaluée [1].

Il faut donc s'intéresser aux possibilités de **fonctionnement en condition dégradée** de l'appareil et des différentes options mise en place pour permettre le fonctionnement de l'appareil.

Il faut également prendre en compte **le nombre et le type d'option de fonctionnement dégradé** pour déterminer le niveau de criticité.

Gravité des pannes en cas d'arrêt du DM

Dans cette partie, il faut déterminer les **impacts des dysfonctionnements sur le ou les services utilisant** le DM. Une enquête terrain approfondie peut être nécessaire pour répondre de manière optimale à cette question

Il est nécessaire de prendre en compte la **gravité du dysfonctionnement sur les soins prodigués aux patients [1].**

L’équipement est sur un réseau segmenté

La notion de **segmentation du réseau** revient à découper celui-ci en différentes sous réseaux ou sous unités. Cette solution permet toujours l’échange entre les différents items du réseau. Cependant, dans son organisation, la segmentation permet de sécuriser les échanges entre les items. Cette sécurisation passe notamment par l’installation de routeurs, de filtres type V-Lan ou encore de pare-feu physique pour contrôler le flux des données [7].

Il est nécessaire de définir avec les utilisateurs et le service informatique le **niveau de segmentation approprié** en ce qui concerne les données et les impacts sur les services en cas de cyberattaque

Le système d'exploitation est supporté et les mises à jour de sécurité sont réalisées

Le **système d'exploitation**, plus communément appelé O.S par les informaticiens, est le programme permettant d'exploiter le dispositif de manière informatique. Il est donc crucial de savoir quel type d'O.S est supporté par la machine car cela va impacter la configuration matérielle, l'infrastructure réseau et d'exploitation du DM.

De part son rôle important, il est donc important de s'assurer de la **mise à jour de** celui-ci sur le DM pour éviter de laisser des failles de vulnérabilité qui pourraient être exploitées dans le cadre d'une cyberattaque

Il est nécessaire de définir avec les utilisateurs et le service informatique l'obsolescence et les ressources matérielles et humaines pour maintenir le DM en condition de sécurité.

Parmi les actions à mettre en place spécifiquement pour ce point, on retrouve la mise à jour du système d'exploitation ou encore le renouvellement partiel ou total de l'équipement.

Le code d’accès est sécurisé

L'accès aux différents dispositifs ou logiciels se doit d’être protégé par des **mots de passe**. Ces mots de passe peuvent être attribués selon les services, les praticiens, les dispositifs eux-même...

Les codes d'accès sécurisés jouent un rôle vital dans la **protection des informations sensibles** [7]. Ces codes permettent de restreindre l'accès aux dossiers médicaux et aux systèmes informatiques, garantissant ainsi la confidentialité des patients et la sécurité des données.Il est essentiel de mettre en place des mesures de cybersécurité robustes pour protéger ces codes et prévenir les intrusions indésirables..

Il est nécessaire de définir avec les utilisateurs et le service informatique un accès sécurisé en rapport avec la politique de l’établissement

Parmi les actions à mettre en place spécifiquement pour ce point, on retrouve la modification des codes d’accès pour les rendre plus robuste et l’instauration de règles communes à l’établissement de santé

Pas de communication Wifi du DM ou communication sur un réseau Wifi sécurisé

La communication sans fil des dispositifs médicaux sur un **réseau Wi-Fi** est devenue essentielle pour améliorer la qualité des soins. Cependant, cette dépendance à la connectivité sans fil expose les établissements de santé à des cyberattaques potentielles. Ne pas passer par un réseau Wifi pour communiquer ou utiliser un réseau Wifi sécurisé est une étape importante dans la prévention des cyberattaques.

Il est possible de **sécuriser une connexion au réseau via différente techniques** comme [7] :

- Limiter l'accès par l'utilisation de clé d'accès au réseau
- La mise en place d'un VLAN agissant comme un filtre réseau sur la base des adresses I.P et/ou M.A.C
- Mettre en place des accès temporaire
- Utilisé le réseau de l'hôpital associé spécifiquement aux dispositifs médicaux.

Il est nécessaire de définir avec les utilisateurs et le service informatique le degré de sécurité acceptable de la communication Wifi

Parmi les actions à mettre en place spécifiquement pour ce point, on retrouve la mise en place, en collaboration avec le service informatique de protocoles de communication sécurisés ou d'une communication Wifi sécurisé lorsqu'une communication Wifi est requise

Stockage et sauvegarde délocalisée des données

Les établissements de santé sont **responsables de la gestion de données médicales sensibles** ce qui en fait une cible intéressante pour les cyber attaquants. Le stockage et la sauvegarde délocalisés des données est donc une approche nécessaire pour garantir que les données médicales critiques sont sécurisées et disponibles en cas de besoins.
Il est cependant nécessaire que ces sauvegardes délocalisées soient sécurisées pour éviter tout accès non autorisé.

Il est nécessaire de définir avec les utilisateurs et le service informatique ce qui doit être conservé et le temps de leur conservation.

Les ports d'entrée non utilisés sont bloqués et les autres sont sécurisés

La prévention de la cybersécurité passe par la gestion rigoureuse des ports d'entrée sur les réseaux informatiques. Désactiver les ports inutilisés permet de réduire la surface d'attaque potentielle. Les ports actifs, quant à eux, sont sécurisés avec des pare-feu, des protocoles d'authentification robuste et des systèmes de surveillance en temps réel.

Il est nécessaire de définir avec les utilisateurs et le service informatique l'utilité ou non de garder des ports fonctionnels ainsi que de définir le niveau de sécurité acceptable.

Parmi les actions à mettre en place spécifiquement pour ce point, on retrouve le blocage des ports non utilisés ou encore l'utilisation de stations blanches.

Les interfaces entre des applications externes au DM sont connues, sécurisées et limitées au strict nécessaire

La gestion des interface est une notion cruciale pour permettre l'**interconnectivité** des dispositifs médicaux. Il est nécessaire de gérer minutieusement les interfaces entre les applications externes et les dispositifs médicaux. **Ces interfaces doivent être rigoureusement identifiées, sécurisées et réduites au strict nécessaire.**

Cette approche limite les points d'entrée potentiels pour les cyberattaques tout en garantissant que seules les connexions essentielles sont autorisées. La gestion des interfaces externes vise à préserver l'intégrité des données médicales et la continuité des opérations dans les établissements de santé.

Il est nécessaire de définir avec les utilisateurs et le service informatique les interfaces externes de manière exhaustives et de sécuriser ces interfaces.

Parmi les actions à mettre en place spécifiquement pour ce point, on retrouve l'arrêt des interfaces non nécessaires à la prise en charge médicale.

La fiche d'identification du système d'information est conservée par la personne compétente et les mises à jour et changement de protocoles sont suivies

Dans le contexte de la cybersécurité des établissements de santé, la fiche d'identification du système d'information a une grande importance. Cette fiche contient des informations essentielles sur l'infrastructure de l'établissement de santé et les protocoles en place. Les mises à jour et les changements de protocoles doivent être systématiquement suivis et enregistré pour gérer les risques. L'objectif est de maintenir une visibilité sur l'évolution du système d'information et de garantir que les mesures de sécurité restent adaptées aux menaces actuelles.

Il est nécessaire de définir avec les utilisateurs et le service informatique qui conserve la fiche d'identification et qui suit les mises à jours.

Parmi les actions à mettre en place spécifiquement pour ce point, on retrouve l'inventaire des logiciels et des postes informatiques, le suivi des maintenances et des mises à jour.

Le patch de sécurité est installé et mis à jour

L'**assurance de la mise à jour des éléments de sécurité** est déterminante pour assurer la protection des données. La mise à jour des éléments de sécurité est donc indispensable.

Il est nécessaire de définir avec les utilisateurs et le service informatique quel patch a été installé et si les mises à jours sont bien effectuées

Parmi les actions à mettre en place spécifiquement pour ce point, on retrouve l'inscription des mises à jour de sécurité dans les contrats de maintenance, et le fait de privilégier les postes informatiques de l'établissement gérés par le service informatique

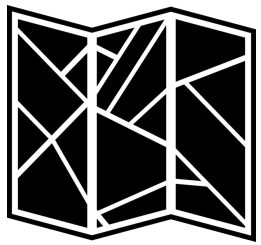
Des audits de sécurité et des tests d'intrusions sont réalisés avec une fréquence acceptable

Afin de s'assurer de la résilience du réseau et du système d'information, il est indispensable de pouvoir tester ces derniers. Leurs **révisions par des audits** et des tests en condition réel permettent une vision d'ensemble sur les potentiels failles du système. Définir une fréquence à ces tests permet d'avoir un suivi méthodique sur l'état de santé du réseau relié au dispositif médical.

Il est nécessaire de définir avec les utilisateurs et le service informatique la fréquence minimum des tests d'intrusion et leur modalité.

Parmi les actions à mettre en place spécifiquement pour ce point, on retrouve l'instauration de tests d'intrusion réguliers.

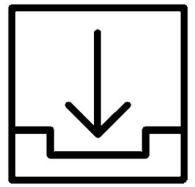
Propositions de plan d'action à mettre en place pour un Dispositif Médical ayant un risque acceptable (1/3)



Référencez-vous suffisamment votre DM au niveau informatique ?

- Inventorier les **équipements et services**
- Inventorier les **logiciels** (nom, fonctions principales, version, éditeur, présence sur le parc informatique, historique de mises à jour, utilisateurs…)
- Inventorier les **accès** (catégorie de l'utilisateur : administrateur, utilisateur, invité… / type d'accès : connexion locale ou à distance)

Effectuez vous des sauvegardes régulièrement ?



- **Identifier les données à sauvegarder** (données personnelles, financières, administratives…)
- Respecter le **cadre juridique** et la **stratégie** de l'établissement de santé (les données dites «personnelles », qu'elles soient relatives aux employés ou aux usagers, nécessitent des mesures de protection renforcées pour garantir le respect des exigences issues du Règlement Général sur la Protection des Données (RGPD))
- Choisir **le ou les supports à privilégier pour vos sauvegardes** (disque dur externe à accès limité, cloud sécurisé…)

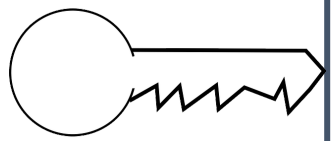
Appliquez-vous régulièrement les mises à jour ?

Propositions de plan d'action à mettre en place pour un Dispositif Médical ayant un risque acceptable (2/3)

Utilisez-vous des dispositifs informatiques afin de sécuriser vos données ?

- Activer son **pare-feu local**
- Installer un **pare-feu physique**

Avez-vous implémenté une politique d'usage de mots de passe robustes ?



- Choisir des **mots de passe robustes** (L'Agence Nationale de la Sécurité des Systèmes d'Information recommande un mot de passe d'au moins 14 caractères avec au moins : 2 majuscules, 2 minuscules, 2 chiffres et 2 caractères spéciaux. Aucun élément personnel ne doit être compris dans ce mot de passe tels qu'une date de naissance ou un prénom.)
- Définir une bonne **politique d'usage des mots de passe** (chaque service doit posséder 1 mot de passe différent)

Avez-vous une utilisation des outils numériques sûre ?

- **Connaître les risques** (usurpation d'identité, intrusion depuis internet, intrusion depuis une clé USB…)
- Adopter les **bons réflexes** (protection de messagerie, lien proposé cohérent avec le sujet évoqué, nom de l'expéditeur)

Propositions de plan d'action à mettre en place pour un Dispositif Médical ayant un risque acceptable (3/3)

Maîtrisez-vous le risque numérique lié au nomadisme des professionnels ?

- **Limiter** au maximum l'**utilisation de matériel hors de son lieu de travail**

Gérez-vous correctement les relations avec vos collaborateurs et tiers-personnes ?

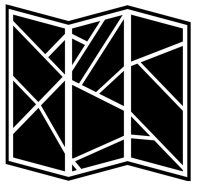
- **Connaître les acteurs** (ARS et GRADeS proposent régulièrement des conseil et accompagnements sur le sujet de la sécurité numérique)
- **Rédiger des contrats** qui incluent des exigences précisent pour lesquelles les tiers s'engagent

Quelles actions mettez-vous en place pour réagir en cas de cyberattaque ?

- Avoir des **options de premières action** en cas de cyberattaque (plan de déconnexion d'équipement avec des codes couleurs, déconnexion de réseau vulnérables, contact des instances qui peuvent venir en aide…)
- Utiliser des **solutions matérielles** en cas de besoin (version papier des documents)

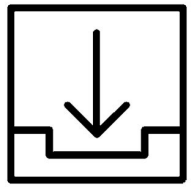
Propositions de plan d'action à mettre en place pour un Dispositif Médical ayant un risque modéré (1/3)

Référencez-vous suffisamment votre DM au niveau informatique ?



- Inventorier les **équipements et services**
- Inventorier les **logiciels** (nom, fonctions principales, version, éditeur, présence sur le parc informatique, historique de mises à jour, utilisateurs…)
- Inventorier les **accès** (catégorie de l'utilisateur : administrateur, utilisateur, invité… / type d'accès : connexion locale ou à distance)
- Inventorier les **données et traitements** (le but ici est de répondre aux questions suivantes : "Quelles sont les données et traitements susceptibles d'affecter la prise en charge des usagers ?" et "Quelles sont les données sensibles et celles soumises à des obligations légales ?
- Inventorier les **interconnexions avec l'extérieur**

Effectuez vous des sauvegardes régulièrement ?



- **Identifier les données à sauvegarder** (données personnelles, financières, administratives…)
- Respecter le **cadre juridique** et la **stratégie** de l'établissement de santé (Les données dites «personnelles », qu'elles soient relatives aux employés ou aux usagers, nécessitent des mesures de protection renforcées pour garantir le respect des exigences issues du Règlement Général sur la Protection des Données (RGPD))
- Choisir **le ou les supports à privilégier pour vos sauvegardes** (disque dur externe à accès limité, clou sécurisé…)
- **Identifier les données à sauvegarder** (après l'inventaire du matériel, il est nécessaire de déterminer quelles données sont essentielles à la poursuite de votre activité : données personnelles, financières…)

Appliquez-vous régulièrement les mises à jour ?

- Utiliser des **logiciels mis à jour**

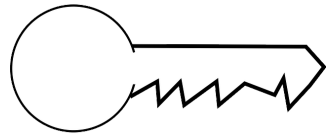
Analyse des risques associant le questionnaire de vulnérabilité et la méthode M.A.C.E |
Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/ - DOI : https://doi.org/10.34746/ids213

Propositions de plan d'action à mettre en place pour un Dispositif Médical ayant un risque modéré (2/3)

Utilisez-vous des dispositifs informatiques afin de sécuriser vos données ?

- Activer son **pare-feu local**
- Installer un **pare-feu physique**
- Utiliser un **antivirus**

Avez-vous implémenté une politique d'usage de mots de passe robustes ?



- Choisir des **mots de passe robustes** (L'Agence Nationale de la Sécurité des Systèmes d'Information recommande un mot de passe d'au moins 14 caractères avec au moins : 2 majuscules, 2 minuscules, 2 chiffres et 2 caractères spéciaux. Aucun élément personnel ne doit être compris dans ce mot de passe tels qu'une date de naissance ou un prénom.)
- Définir une bonne **politique d'usage des mots de passe** (chaque service doit posséder 1 mot de passe différent)

Avez-vous une utilisation des outils numériques sûre ?

→ **Connaître les risques** (usurpation d'identité, intrusion depuis internet, intrusion depuis une clé USB…)
→ Adopter les **bons réflexes** (protection de messagerie, lien proposé cohérent avec le sujet évoqué, nom de l'expéditeur)
→ **Créer et gérer des comptes utilisateurs** (création d'un compte par employé et sans privilège d'administration, seuls les comptes utilisateurs doivent être utilisés pour naviguer sur internet, les comptes administrateurs doivent être utilisés uniquement pour configurer des équipements ou installer des logiciels
→ **Configurer sa messagerie** (mettre en place des systèmes d'authentification, activer le chiffrement des échanges, ne pas exposer directement sur internet les serveurs de messagerie électronique)

Analyse des risques associant le questionnaire de vulnérabilité et la méthode M.A.C.E |
Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | 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

Propositions de plan d'action à mettre en place pour un Dispositif Médical ayant un risque modéré (3/3)

Maîtrisez-vous le risque numérique lié au nomadisme des professionnels ?

- **Limiter** au maximum l'**utilisation de matériel hors de son lieu de travail**
- **Sécuriser la mobilité** numérique (sauvegarde de données, mots de passes non pré-enregistrés…)

Gérez-vous correctement les relations avec vos collaborateurs et tiers-personnes ?

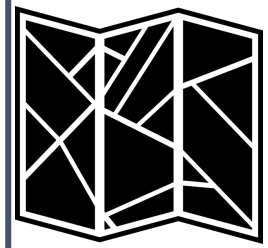
- **Connaître les acteurs** (ARS et GRADeS proposent régulièrement des conseil et accompagnements sur le sujet de la sécurité numérique)
- **Rédiger des contrats** qui incluent des exigences précisent pour lesquelles les tiers s'engagent
- Deux points de vigilance concernant les contrats (Il faut **faire attention aux contrats proposés par des tiers** car ces derniers peuvent fixer des modes de traitement des données ne respectant pas les législations / Il faut **accroître le niveau de vigilance et les exigences** en ce qui concerne la sécurité)
- **S'informer et sensibiliser régulièrement** (le CERT-SANTE, une cellule de l'Agence du Numérique en Santé propose ses services en terme de veille technique relative aux campagnes d'attaques et aux vulnérabilité des dispositifs médicaux)
- **Suivre et évaluer le respect des exigences de sécurité** par les tiers

Quelles actions mettez-vous en place pour réagir en cas de cyberattaque ?

- Avoir des **options de premières action** en cas de cyberattaque (déconnexion d'équipement, déconnexion de réseau…)
- Se **préparer à l'incident** d'une cyberattaque (Le CERT Santé peut apporter son aide en cas d'incident. Il assure une mission de prévention et d'alerte face aux menaces de cybersécurité et partage différentes recommandations pour réduire au maximum les effets en cas de cyberattaque)
- **Aspects juridiques** (Le décret n° 2022-715 du 27 avril 2022 relatif aux conditions et aux modalités de mise en œuvre du signalement des incidents de sécurité informatique. Ce décret permet aux autorités compétentes d'éviter la propagation des cyberattaques)
- Utiliser des **solutions matérielles** en cas de besoin (version papier de vos documents)

Analyse des risques associant le questionnaire de vulnérabilité et la méthode M.A.C.E |
Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | 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

Propositions de plan d'action à mettre en place pour un Dispositif Médical ayant un risque fort (1/4)

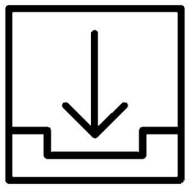


Référencez-vous suffisamment votre DM au niveau informatique ?

- Inventorier les **équipements et services**
- Inventorier les **logiciels** (nom, fonctions principales, version, éditeur, présence sur le parc informatique, historique de mises à jour, utilisateurs…)
- Inventorier les **accès** (catégorie de l'utilisateur : administrateur, utilisateur, invité… / type d'accès : connexion locale ou à distance)
- Inventorier les **données et traitements** (le but ici est de répondre aux questions suivantes : "Quelles sont les données et traitements susceptibles d'affecter la prise en charge des usagers ?" et "Quelles sont les données sensibles et celles soumises à des obligations légales ?"
- Inventorier les **interconnexions avec l'extérieur**
- **Mettre régulièrement à jour les différents inventaires** (Les cinq inventaires ci-dessus doivent être mis à jour au minimum 2 fois par an pour présenter une image relativement proche du réel et rester un outil de suivi et de contrôle)

Effectuez vous des sauvegardes régulièrement ?

- **Identifier les données à sauvegarder** (données personnelles, financières, administratives…)
- Respecter le **cadre juridique** et la **stratégie** de l'établissement de santé (Les données dites «personnelles », qu'elles soient relatives aux employés ou aux usagers, nécessitent des mesures de protection renforcées pour garantir le respect des exigences issues du Règlement Général sur la Protection des Données (RGPD))
- Choisir **le ou les supports à privilégier pour vos sauvegardes** (disque dur externe à accès limité, cloud sécurisé…)
- **Identifier les données à sauvegarder** (après l'inventaire du matériel, il est nécessaire de déterminer quelles données sont essentielles à la poursuite de votre activité : données personnelles, financières…)
- Déterminer une **procédure pour vos sauvegardes** (la fréquence des sauvegardes est à définir en lien avec le volume de données produites. Pour cela, nous conseillons l'utilisation de la règle "3-2-1" : 3 exemplaires de sauvegarde de données / 2 tests de restauration complets des données pour vérifier le bon état de fonctionnement des supports / 1 copie de sauvegarde protégée et déconnectée physiquement du système informatique



Analyse des risques associant le questionnaire de vulnérabilité et la méthode M.A.C.E |
Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | 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

Propositions de plan d'action à mettre en place pour un Dispositif Médical ayant un risque fort (2/4)

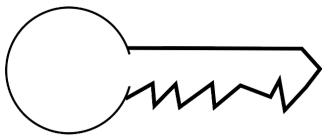
Appliquez-vous régulièrement les mises à jour ?

- Utiliser des **logiciels mis à jour**
- Activer la **mise à jour automatique** des logiciels et des matériels

Utilisez-vous des dispositifs informatiques afin de sécuriser vos données ?

- Activer son **pare-feu local**
- Installer un **pare-feu physique**
- Utiliser un **antivirus**
- **Centraliser** l'utilisation des **antivirus sur le réseau**

Avez-vous implémenté une politique d'usage de mots de passe robustes ?



- Choisir des **mots de passe robustes** (L'Agence Nationale de la Sécurité des Systèmes d'Information recommande un mot de passe d'au moins 14 caractères avec au moins : 2 majuscules, 2 minuscules, 2 chiffres et 2 caractères spéciaux. Aucun élément personnel ne doit être compris dans ce mot de passe tels qu'une date de naissance ou un prénom.)
- Définir une bonne **politique d'usage des mots de passe** (chaque service doit posséder 1 mot de passe différent)
- Utiliser un **système d'authentification unifié** (type Single Sign-on permettant de simplifier et renforcer les mécanismes d'authentification)

Propositions de plan d'action à mettre en place pour un Dispositif Médical ayant un risque fort (3/4)

Avez-vous une utilisation des outils numériques sûre ?

- **Connaître les risques** (usurpation d'identité, intrusion depuis internet, intrusion depuis une clé USB…)
- Adopter les **bons réflexes** (protection de messagerie, lien proposé cohérent avec le sujet évoqué, nom de l'expéditeur)
- **Créer et gérer des comptes utilisateurs** (création d'un compte par employé et sans privilège d'administration, seuls les comptes utilisateurs doivent être utilisés pour naviguer sur internet, les comptes administrateurs doivent être utilisés uniquement pour configurer des équipements ou installer des logiciels)
- **Configurer sa messagerie** (mettre en place des systèmes d'authentification, activer le chiffrement des échanges, ne pas exposer directement sur internet les serveurs de messagerie électronique)
- **Administrer son SI**

Maîtrisez-vous le risque numérique lié au nomadisme des professionnels ?

- **Limiter** au maximum l'**utilisation de matériel hors de son lieu de travail**
- **Sécuriser la mobilité** numérique (sauvegarde de données, mots de passes non pré-enregistrés…)
- Adopter de **bons réflexes durant les déplacements** (refus de connexion d'équipement appartenant à une tiers-personne, garder les appareils les supports et les fichiers que vous transportez sur vous…)

Propositions de plan d'action à mettre en place pour un Dispositif Médical ayant un risque fort (4/4)

Gérez-vous correctement les relations avec vos collaborateurs et tiers-personnes ?

- **Connaître les acteurs** (ARS et GRADeS proposent régulièrement des conseil et accompagnements sur le sujet de la sécurité numérique)
- **Rédiger des contrats** qui incluent des exigences précisent pour lesquelles les tiers s'engagent
- Deux points de vigilance concernant les contrats (Il faut **faire attention aux contrats proposés par des tiers** car ces derniers peuvent fixer des modes de traitement des données ne respectant pas les législations / Il faut **accroître le niveau de vigilance et les exigences** en ce qui concerne la sécurité)
- **S'informer et sensibiliser régulièrement** (le CERT-SANTE, une cellule de l'Agence du Numérique en Santé propose ses services en terme de veille technique relative aux campagnes d'attaques et aux vulnérabilité des dispositifs médicaux)
- **Suivre et évaluer le respect des exigences de sécurité** par les tiers

Quelles actions mettez-vous en place pour réagir en cas de cyberattaque ?

- Avoir des **options de premières action** en cas de cyberattaque (déconnexion d'équipement, déconnexion de réseau…)
- Se **préparer à l'incident** d'une cyberattaque (Le CERT Santé peut apporter son aide en cas d'incident. Il assure une mission de prévention et d'alerte face aux menaces de cybersécurité et partage différentes recommandations pour réduire au maximum les effets en cas de cyberattaque)
- **Aspects juridiques** (Le décret n° 2022-715 du 27 avril 2022 relatif aux conditions et aux modalités de mise en œuvre du signalement des incidents de sécurité informatique. Ce décret permet aux autorités compétentes d'éviter la propagation des cyberattaques)
- **Connaître et faire évoluer son contrat d'assurance** au risque cyber selon son profil d'établissement
- Utiliser des **solutions matérielles** en cas de besoin (version papier de vos documents)

RÉFÉRENCES

[1] J. LHOMME, J. HUMBERT, et G. FARGES, « La criticité des dispositifs médicaux : état de l'art et calcul », IRBM News, vol. 34, nº 5-6, p. 150-154, octobre 2013, doi: https://doi.org/10.34746/q1wm-2917.

[2] 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, vol. 42, nº 1, p. 18, février 2021, doi: https://doi.org/10.1016/j.irbmnw.2021.100298.

[3] Agence Numérique de la Santé, « Présentation sur "La cybersécurité pour le social et le médico-social en 13 questions" », octobre 2022. Consulté le: 3 novembre 2023. [En ligne]. Disponible sur: https://esante.gouv.fr/actualites/un-nouveau-guide-cybersecurite-destination-du-medico-social

[4] M. LÉCART, « Efficience de la gestion de l'obsolescence », Université de Technologie de Compiègne, Compiègne, Rapport de Stage, 2020. Consulté le: 3 novembre 2023. [En ligne]. Disponible sur: https://www.utc.fr/tsibh/public/3abih/20/stage/lecart/index_fichiers/projet.pdf

[5] J. ANCELLIN, « Maintenance et obsolescence des dispositifs médicaux », *Annales Françaises d'Anesthésie et de Réanimation*, vol. 18, nº 2, p. 258-260, févr. 1999, doi: 10.1016/S0750-7658(99)90403-3.

[6] Agence nationale de la sécurité des systèmes d'information, «Glossaire », 2020. Consulté le: 3 novembre 2023. Consulté le: 3 novembre 2023. [En ligne]. Disponible sur : https://www.ssi.gouv.fr/entreprise/glossaire/

[7] J. DORDOIGNE, « Principes de sécurisation d'un réseau », in *Réseaux Informatiques - Notions fondamentales*, 8e édition., in ENI. , Editions ENI, 2019, p. 621-679.

[8] MDCG, Éd., « MDCG 2021-24 Guidance on classification of medical devices ». octobre 2021. Consulté le: 3 novembre 2023. [En ligne]. Disponible sur: https://health.ec.europa.eu/system/files/2021-10/mdcg_2021-24_en_0.pdf