Agence nationale de sécurité du médicament et des produits de santé

Compte-rendu de séance

Date du document : 13/02/2019

Direction des dispositifs médicaux, des cosmétiques et des dispositifs de diagnostic in vitro
Equipe produits diagnostic, des systèmes radiogènes et des systèmes d'information
Sophie Nogaret

Comité Scientifique Spécialisé Temporaire

« Cyber sécurité des logiciels dispositifs médicaux »

Séance du Mercredi 21 novembre 2018 de 10h00 à 13h00 en salle 3

Programme de séance		
1.	**Introduction**	
1.1	Présentation rapide des intervenants	
1.2	Adoption de l'ordre du jour	
2.	**Point Etape**	
2.1	Bilan des précédentes réunions → état des lieux de l'avancement du projet	
2.2	Objectifs - Echéancier	
3.	**Projet de recommandations à l'attention des fabricants de Dispositifs Médicaux**	
3.1	Discussion et travail de fond sur le document	
4.	**Questions diverses - Conclusion**	

Agence nationale de sécurité du médicament et des produits de santé

Compte-rendu de séance

Noms des participants	Membres/ secrétaire	Présent	Absent/ excusé
Vincent ARCHER	Membre	Présent	
Bruno BLANCHET	Membre	Présent (Téléconférence)	
Luc CHAUSSON	Membre	Présent	
Régis GUILLEMAUD	Membre	Présent	Excusé
Alain MERLE	Membre	Présent	
Cédric CARTAU	Membre	Présent (Téléconférence)	
Stéphane PASQUIER	Membre	Présent (Téléconférence)	
Vincent LOUIS	Membre		Excusé
Philippe LOUDENOT	Membre		Excusé
Bernard CASSOU MOUNAT	Membre		Excusé
Thierry SIRDEY	ANSM	Présent	
Gwennaelle EVEN	ANSM		Excusée
Virginie GAIFFE	ANSM	Présent	
Sophie NOGARET	ANSM	Présent	
Caroline CHIUMA	ANSM	Présent	
Thomas LECARDEZ	ANSM	Présent	
Philippe DURR	ANSM	Présent	
Valérie SOUMET	ANSM	Présent	

1. Introduction

1.1.Présentation des intervenants

Il est rappelé aux intervenants que la séance est enregistrée puis un tour de table est effectué : les différents membres du CSST et les personnes internes à l'Agence se sont présentés. La présente séance est composée de 7 experts (dont 3 par téléconférence) et de 7 personnes de l'ANSM.

Aucune situation de conflit d'intérêt majeur n'a été déclarée, ni retenue au cours de la séance du 13 avril 2018.

Le document a été transmis aux experts en amont de la réunion. L'ANSM remercie les experts pour leurs nombreuses remarques qui vont alimenter la discussion en séance.

3 documents ont été fournis aux experts en séance :

-Une présentation PowerPoint d'introduction.
-Un tableau Excel récapitulant l'ensemble des remarques des experts.
-Une version du document en mode suivi des corrections dans lequel l'ensemble des commentaires des experts ont été combinés.

1.2.Adoption de l'ordre du jour

L'ordre du jour est adopté à l'unanimité.

2. Point Etape

2.1. Bilan des réunions précédentes

L'ANSM rappelle brièvement les éléments discutés lors des 3 CSST précédents :
-CSST du 26/06/2017 : Présentation des objectifs du groupe et discussion sur les définitions
-CSST du 11/10/2017 : Travail sur le plan du document et premières discussions sur les recommandations
Il a été décidé de structurer les recommandations autour du cycle de vie du logiciel.
-CSST du 13/04/2018 : Travail sur la partie gestion du risque et discussion autour de la liste des recommandations. Premiers échanges sur les aspects techniques des recommandations.

L'ANSM a participé à une conférence organisée par l'ENISA le 14/11/2018 à Rotterdam. L'approche française et les travaux du groupe ont été présentés.

L'ANSM rappelle que le document rédigé au niveau national a pour vocation à être traduit dès que possible. En effet, un groupe dédié la problématique de la cybersécurité des DM a été créé en 2018 au sein de la commission. Des travaux équivalents sont également réalisés au sein d'autres pays de l'Union (UK, Allemagne et Irlande).

Remarque : suite à des problèmes de réseau téléphonique, les personnes par téléphone ont été déconnectées en cours de séance.

2.2. Objectifs

Avant d'entamer la discussion sur le fond du document, l'ANSM fait un bilan général des commentaires transmis par les experts.

Au total, environ 90 commentaires ont été rédigés par les experts suite à la revue du document.

Certains commentaires, qui ne posaient pas matière à discussion ont directement été pris en compte et intégrés dans le texte.
Les commentaires restants ont été abordés en séance.

3. Discussion sur le fond du document

3.1. Points généraux

L'utilisation de la dénomination DMIL est validée par les experts en début de séance.

Les experts valident la structure générale du document. Ils indiquent que seuls certains paragraphes à la marge seront à déplacer.

Il avait été question lors de la dernière séance d'utiliser un DM en exemple comme fil conducteur. Cette proposition s'avère finalement difficilement applicable et n'a pas été retenue.

Suite à la remarque d'un expert concernant le directive sur la sécurité des réseaux et des systèmes d'information, la question se pose de l'intégrer aux recommandations. Suite aux discussions, cette directive n'étant pas spécifique aux DM, il est proposé de la citer en tant que référence. L'objectif est de faire un lien entre le dossier de gestion des risques DM et celui des hôpitaux. Il faudra mentionner que les établissements de santé devront gérer certains risques liés à la présence de DM connectés. Il doit y avoir une continuité entre le dossier de gestion des DM et ceux des hôpitaux.

3.2. Produits concernés

La mention des DMDIV dans la définition des produits concernés doit être conservée. Il s'agit de 2 règlements disjoints. Même si les exigences essentielles sont similaires, les experts sont d'avis de conservés les deux en parallèle.

3.3. Les bases réglementaires

L'ANSM s'interroge sur l'ajout d'une annexe concernant la classification des DM. Après discussion, il est décidé de renvoyer au texte via l'ajout d'une référence.

3.4.Distinction en sécurité et sureté

Plusieurs remarques sur la notion de probabilité d'exploitation d'une faille ont été faites. Les experts proposent d'enlever toute référence à la notion de probabilité car elle est difficilement compréhensible hors contexte et nécessiterait de se justifier sur des éléments probabiliste. Il n'est pas possible de quantifier de manière fiable la probabilité d'apparition d'un défaut logiciel, d'une vulnérabilité. Il faut partir du postulat qu'une vulnérabilité existe ou qu'elle n'existe pas. C'est l'analyse de risque qui va permettre de vérifier si une vulnérabilité est exploitable ou non.
De plus, il faut considérer que lorsqu'une vulnérabilité existe, dès qu'elle a été identifiée, elle est considérée comme connue de l'ensemble de la communauté.

3.5. Gestion des risques appliquée aux dispositifs médicaux

Les experts sont gênés par la mention suivante dans le texte « blessure acceptable sous condition ». L'ANSM indique que ces deux notions peuvent être associées dans le monde du DM. En effet, le risque peut être acceptable dans certains cas. Le risque de décès peut être acceptable en fonction de l'occurrence par exemple (occurrence très faible) et si le rapport bénéfice/risque est favorable. Suite aux discussions il est décidé de reformuler ce point en reprenant la formulation de la norme.

Les experts indiquent qu'il manque la notion d'intégration du DM dans un SI. En effet, le DM peut présenter une vulnérabilité et être un vecteur de propagation d'une menace. Il faut considérer le SI comme une cible potentielle. De même, pour un équipement, il faut penser à la structure dans laquelle il va être déployé. Par contre, les experts soulignent qu'il ne faut pas faire une analyse de risque du système complet. Il faut faire une analyse de risque de l'effet que peut avoir une malversation sur le DM. D'un point de vue pratique, il faut vérifier que le logiciel n'est pas modifié : vérifier l'intégrité du logiciel et en cas d'attaque, avoir mis en place des mesures pour éviter la propagation à l'ensemble du système.
Il est rappelé que selon les exigences essentielles, le fabricant doit s'assurer de la bonne compatibilité de l'équipement avec l'environnement. Le fabricant ne se pose pas forcément la question dans ce sens.
Après discussion, il est décidé d'évoquer ce point au niveau de la partie analyse de risques et d'indiquer au niveau de la partie technique des recommandations que le fabricant doit implémenter des mesures afin d'empêcher la propagation d'une menace.

3.6. Partie III – Recommandations

Plusieurs propositions d'identification des recommandations ont été présentées aux experts : numérotation, identification du type de DM, pictogrammes. Après discussion, il est décidé de numéroter les recommandations sans préciser le domaine d'application et d'ajouter la mention sous réserve d'applicabilité. L'objectif est de laisser le développeur trancher et justifier le caractère non applicable d'une recommandation pour un dispositif donné.

Concernant les dispositifs médicaux implantables actifs intégrant du logiciel, il est décidé de rédiger une annexe précisant les particularités applicables à ce type de dispositifs.

Il est également proposé d'illustrer, dans la mesure du possible les recommandations avec des exemples afin d'aider les fabricants.

Les experts demandent d'indiquer plus lisiblement que la première recommandation est bien l'analyse de risque ce qui n'était pas très lisible dans le projet de document.

3.7. Activité de conception

Le groupe s'interroge sur la notion de minimisation de la complexité des données. Suite aux discussions, il apparait difficile de généraliser. Si l'élément de base en sécurité est de limiter la complexité, ceci est difficilement applicable à certains types de dispositifs.
Le groupe propose donc de préciser ce point : il est recommandé au fabricant de minimiser la complexité de la partie sécuritaire du DM. Le fabricant pourra réaliser une segmentation entre zone critique et non critique. Seules les zones identifiées comme critiques devront répondre à des exigences de minimisation des données.

3.8. Contrôle des accès

Les experts rappellent que la notion de mot de passe est très critiquée. Cette solution ne peut pas être préconisée en première intention. Les experts proposent de changer la hiérarchisation des items (solutions matérielles, badges, puces…). Enfin, si l'utilisation d'un mot de passe est la seule alternative possible, des précautions devront être prises.

3.9. Environnement d'utilisation

Les experts ont identifié une confusion au niveau de la partie environnement d'utilisation dans laquelle il est fait mention qu'on ne peut pas imposer un wifi sécurisé. Ils indiquent qu'il est possible de demander un niveau minimum de sécurité, même au domicile du patient (système de configuration de la box par exemple) Les experts demandent de supprimer ce point.

Les experts indiquent également que certaines des règles proposées dans cette partie font partie de la démarche classique du système de management de la qualité. Par exemple, la norme 13485 est bien en place dans l'industrie et dans les stratégies de développement. Par exemple, définir les exigences de compatibilité entre logiciels et matériel est une démarche qualité bien établie. La question se pose donc de l'intérêt de rappeler ces éléments.
Suite aux discussions, il est décidé de rappeler brièvement ces points sans rentrer dans les détails et d'ajouter une référence.

3.10.Activité de développement du logiciel

Concernant le langage de programmation, les experts rappellent qu'il n'est pas possible de recommander un langage spécifique. Le choix du langage est à l'initiative du fabricant. Par contre, le choix doit être justifié et les règles de codage doivent être définies dans le système qualité du développeur. Les règles de codages doivent correspondre aux bonnes pratiques en termes de sécurité. Il faut insister sur la partie qualité et notamment sur l'importance d'un système de validation et sur la réalisation de tests de régression.

3.11. Données importées sur le DM

Les données importées sur le DM doivent être contrôlées. Ceci doit être pris en compte dans l'analyse de risques. Par exemple, une clé usb peut être utilisée dans la mesure où son utilisation est maitrisée : données chiffrées par exemple. Par contre, il ne faut pas pouvoir modifier le logiciel embarqué.

Il faut également prendre en compte les risques liés aux supports physiques comme la clé usb qui détruit physiquement le système (« USB killer »).

Les experts développent la notion d'acceptance check ou contrôle de conformité. Dans le cas de l'intégration de n'importe quel élément, il faut avoir mis en place un système de contrôle d'acceptation de l'importation.
Ceci doit s'appliquer pour les sous-traitants, dans le cas de l'incorporation d'un SOUP et pour tous les achats. Il s'agit de mettre en place un système de maitrise des prestations externalisées. Pour cela, les spécifications doivent avoir été définies en amont. L'intégration d'un élément ne pourra être validée qu'après vérification qu'il répond bien aux spécifications. Il s'agit de ne pas intégrer des éléments externes à l'aveugle.
Par exemple : librairies SSH : identification de failles dans certaines versions
Cas de SOUP : Utilisation de librairies éprouvés – acceptance check à rappeler.

3.12.Mise en service – 1ère utilisation

Les experts demandent que les points suivants soient ajoutés : règles de mises à jour le plus souvent possible – installation/initialisation est un moment ou c'est possible

3.13.Gestion des incidents

L'ANSM interroge sur l'expert sur la gestion des incidents relèverait plutôt de l'utilisateur. L'ANSM demande aux experts si ceci rentre dans le scope des recommandations.

Suite aux discussions, il est décidé que la question de la notification des incidents doit être mentionnée car beaucoup d'interlocuteurs différents sont présents en France (CNIL, ASIP ANSSI et ANSM…)

Il est proposé de faire un rappel des différents moyens de déclaration via un tableau synthétique.

3.14. Mise à jour et maintenance

Les paragraphes relatifs à la mise à jour, la maintenance, la durée d'indisponibilité, des conditions de mis à jour relèvent plutôt de la responsabilité de l'utilisateur. Afin de ne pas perdre l'objectif des recommandations, il est décidé de supprimer ces points.

3.15. Point concernant les annexes

Suite à une demande de l'ANSM, les experts souhaitent conserver l'annexe récapitulant la liste des institutions et l'ensemble des normes.

L'annexe concernant la classification des DM n'apparait pas utile. Une référence aux règlements sera ajoutée dans le texte.

Concernant le tableau récapitulatif des recommandations, les experts proposent de conserver la colonne des biens à protéger. La colonne des objectifs doit être nuancée : ajouter la mention par exemple ou a minima. Il est décidé de supprimer les colonnes : cycle de vie et DM concernés.

L'annexe relative aux formulaires de déclaration sera supprimée.

Concernant la proposition de réaliser une l'annexe relative à la partie cryptographie, il s'avère quelle sera soit trop réductrice soit incompréhensible. Il existe des documents très complets concernant ce point. Il est donc décidé de renvoyer au RGS concernant cette partie et de supprimer l'annexe.

3.16. Eléments à ajouter

Les experts évoquent la possibilité de mettre en évidence les recommandations minimales. L'objectif serait d'avoir une liste rapide et compréhensible.

Concernant la partie vérification et validation, les experts proposent de faire mention d'un processus renforcé de vérification de la sécurité : test de pénétration, scan de vulnérabilité

Ces points devront être développés.

Discussion concernant les notices en ligne : quel serait l'impact en terme d'intégrité de l'information

Il est décidé de rappeler que les mesures de maitrise du risque doivent être évaluées dans le cadre du processus d'aptitude à l'utilisation. Il est proposé de citer la norme harmonisée 62366 dans laquelle on retrouve tous les éléments d'aptitude à l'utilisation pour réduire les risques cyber : aspects notice, aspects formation, sécurité dans les formations etc…

4. Conclusion

L'ANSM va intégrer les éléments discutés dans le projet de document. Une relecture de cette version sera proposée aux experts.

L'objectif est d'obtenir une première version consolidée des recommandations pour le premier trimestre 2019. Le document sera ensuite traduit.

Une consultation publique devrait être lancée en parallèle.

L'ANSM rappelle que le CSST est nommé jusqu'en juin 2019.

L'ANSM tient à remercier tous les experts pour leur participation active aux discussions.

Levée de séance.