Agence nationale de sécurité du médicament et des produits de santé

Compte rendu de séance

Date du document : 18/8/2017
Direction des dispositifs médicaux de diagnostic et des plateaux techniques
Pôle Dispositifs Médicaux médicaux radiogènes, injection, aide patient, logiciels
Myriam DAHANI

Comité Scientifique Spécialisé Temporaire

« Cyber sécurité des logiciels dispositifs médicaux »

Séance du jeudi 29 juin 2017 de 13h30 à 16h30 en salle A015

Programme de séance		
1.	**Introduction**	
1.1	Rappel du principe du CSST	
1.2	Présentation des experts	
2.	**Contexte et problématiques concernant la Cyber sécurité des logiciels dispositifs Médicaux**	
2.1	Présentation de l'ANSM	
3.	**Discussion**	
3.1	Tour de table	
4.	**Conclusion**	

Noms des participants	Membres/ secrétaire	Présent	Absent/ excusé
Vincent ARCHER	Membre	Présent	
Bruno BLANCHET	Membre	Présent	
Luc CHAUSSON	Membre	Présent	
Alain ESPINOUX	Membre	Présent	
Régis GUILLEMAUD	Membre	Présent	
Alain MERLE	Membre	Présent	
Benjamin MORIN	Membre	Présent	
Stéphane PASQUIER	Membre	Présent	
Philippe LOUDENOT	Membre		Excusé
Bernard CASSOU MOUNAT	Membre		Excusé
David GIORGIS	ANSM	Présent	
Thierry SIRDEY	Secrétaire de séance	Présent	
Hélène BRUYERE	ANSM	Présent	
Myriam DAHANI	ANSM	Présent	
Joelle LOCARDEL	ANSM	Présent	
Noelle THEBAUT	ANSM	Présent	
Marion VANCASSEL	ANSM	Présent	

1. Introduction

Une présentation de l'agence et de Direction des Dispositifs Médicaux de Diagnostic et des Plateaux techniques (DMDPT) est effectuée par l'ANSM, détaillant les dispositifs médicaux dont la DMDPT a la charge, dont les logiciels dispositifs médicaux ainsi que les logiciels d'aide à la prescription.

La cyber-sécurité est une problématique connue depuis longtemps, en forte croissance néanmoins. L'ANSM a souhaité prendre en charge le sujet pour avoir une action au niveau institutionnel sur cette thématique.

1.1. Déclarations publiques d'intérêts – présentation du règlement intérieur des CSST

Aucune situation de conflit d'intérêt majeur n'a été déclarée ni retenue au cours de la séance du 29 Juin 2017.

Les modalités pratiques telles que la composition du comité, les durées des mandats des experts, le rappel des règles de déontologie (DPI) est effectué par l'ANSM. Il est précisé que les comptes rendus des réunions seront publiés sur le site de l'ANSM après commentaires des experts.

Une question d'ordre pratique est posée : si un membre n'est pas en capacité de continuer son mandat, peut-on désigner un remplaçant ?

Réponse : oui, des changements sont possibles du moment que l'expert remplaçant remplit les conditions en termes de déontologie.

1.2. Présentation des experts

Il est précisé que la séance est enregistrée, puis un tour de table est effectué, au cours duquel les différents membres du CSST se sont présentés, ainsi que les personnes internes à l'Agence conviées à assister à ce comité (3 évaluateurs).

2. Contexte et problématique concernant la cyber sécurité des logiciels dispositifs médicaux : présentation de l'ANSM

2.1 Constats : exemples d'attaques malveillantes

L'ANSM rappelle le contexte situant la raison de la tenue de ce CSST, ainsi que des exemples d'attaques malveillantes survenues récemment dans les domaines de santé et de dispositifs médicaux (DM).

2 cas de figure sont à distinguer :

- Le cas où le DM lui-même est la cible du piratage
- Le cas où le DM est un vecteur ou un relais de l'attaque, exemple des DM connectés au réseau des établissements de santé (scanner, IRM, laveur-désinfecteur)

2.2 Tour d'horizon de la réglementation sur la cyber sécurité des logiciels dispositifs médicaux

L'ANSM fait un bref rappel de la réglementation DM actuelle, précisant notamment l'arrivée du nouveau règlement entré en vigueur en Mai 2017. Une brève analyse de l'évolution de la notion de logiciel dans cette réglementation est effectuée.

L'ANSM rappelle également quels sont les différents acteurs impliqués dans le domaine du dispositif médical, ainsi que leurs rôles respectifs dans le paysage institutionnel et non institutionnel (Parlement Européen, Conseil de l'Europe, Organismes notifiés, Commission Européenne, ANSM, Organismes de normalisation, Fabricant etc.).

Le Règlement Européen actuel définit des exigences en termes de sécurité pour les logiciels dispositifs médicaux. Néanmoins, l'intégralité de la problématique cyber-sécurité n'est pas couverte par cette réglementation. C'est pour cela qu'il serait utile d'avoir un guide, certes non opposable, mais émanant d'une autorité compétente qui a une certaine écoute auprès des fabricants de DM, et qui pourra servir de base de travail pour faire évoluer les approches sur ce thème.

2.3 Bibliographie

En amont de la séance, l'ANSM a effectué un travail bibliographique sur le sujet de la cyber-sécurité des dispositifs médicaux. Les principaux textes traitant de la sécurité des systèmes d'information, en séparant les textes spécifiques des dispositifs médicaux de ceux traitant de la sécurité d'information en général, et en séparant également les textes français des textes européen et internationaux, sont brièvement cités.

A la lumière de ce travail bibliographique, il apparaît qu'il y a :

- beaucoup d'initiatives internationales sur la sécurisation des systèmes d'information (SI) de manière globale, non spécifique aux DM, moins d'initiatives Européennes ou Françaises.

- une insuffisance normative relative à la protection contre les attaques malveillantes dirigées contre des DM (NF EN 62304)

=> En conclusion, on peut dire qu'il y a une insuffisance de prise en compte de ces questions dans la réglementation ou à travers des recommandations nationales ou européennes.

Il a été spécifiquement mentionné le document rédigé par l'ASIP Santé intitulé « **Guide sur les dispositifs connectés d'un SI de Santé »** axé sur la sécurité des dispositifs médicaux connectés. Ce document de la PGSSIS est un premier document émanant d'une institution française sur le sujet de la sécurité de l'information des DM. Il est à préciser que ce document exclut les implantables de son champ, et exclut également les DM utilisés en ambulatoire.

Il est souligné qu'une clarification sur le positionnement des documents nationaux les uns par rapport aux autres sera nécessaire, à terme.

2.4 Objectif du travail proposé

L'objectif est de fournir des recommandations aux fabricants de logiciels DM de manière à ce qu'ils puissent prendre toutes les dispositions nécessaires pour prévenir toute attaque malveillante à l'encontre de leurs dispositifs médicaux et ainsi prévenir la compromission des données et l'utilisation détournée du dispositif médical.

A ce jour, dans le domaine du DM, les aspects sécurité sont pris en compte de matière hétérogène par les fabricants. Certains fabricants sont bien conscients de ce risque et le prennent en compte dès la conception du produit, d'autres fabricants ne prennent pas encore en compte cet aspect.

Ce document n'a pas pour objectif de donner des recommandations de pratique aux utilisateurs de logiciels DM, mais de donner aux fabricants de ces logiciels des recommandations allant de la conception jusqu'à la fin de vie du logiciel DM.

2.5 Champ du travail proposé

Tous les logiciels répondant à la définition du DM dans le règlement européen relatif aux dispositifs médicaux entrent dans le champ de ce travail.

Ainsi, ce travail couvrira tous les logiciels DM ainsi que les DM connectés, qu'ils soient embarqués ou autonomes, et ce quelle que soit leur classe de risque, sur l'ensemble de leur cycle de vie.

Les logiciels SaaS (Software As a Service) font partie du champ également.

Il est précisé que l'environnement d'utilisation du logiciel (interfaces de communication avec les SI en place, hardware lié au software, postes de travail sur lesquels peuvent être utilisés les logiciels etc.) fait partie du champ du travail proposé.

Pour rappel, le point 14.2 de l'annexe 1 du Règlement DM précise que : « Les dispositifs sont conçus […] de manière à éliminer […] tout risque associé à une éventuelle interaction négative entre les logiciels et **l'environnement informatique** dans lequel ceux-ci fonctionnement et avec lequel ils interagissent ».

2.6 Niveau de précision du livrable

En terme rédactionnel, l'objectif est de rédiger un document de « bonnes pratiques ». Il est souhaitable que le document ne rentre pas dans des détails techniques trop précis. Ces éléments, surtout en termes de technologie, risquent d'être rapidement obsolètes.

Exemples de livrables de granularité similaire à atteindre : guides de bonnes pratiques de l'ANSSI, PGSSIS etc.

Le document final pourra en revanche renvoyer vers des documents plus précis et plus techniques qui seraient amenés à évoluer dans le temps.

2.7 Définition de la cyber sécurité

Plusieurs organismes ont proposé des définitions différentes du terme « cybersécurité ».

On peut constater que certaines notions reviennent fréquemment en fonction des sources : protection, défense, confidentialité, intégrité, disponibilité, risque, résilience.

La proposition suivante de définition de la cyber-sécurité telle qu'on l'entend dans le champ de ce document est proposée au groupe :

« Protection de la **confidentialité**, de **l'intégrité** et de la **disponibilité** des informations contenues ou issues d'un dispositif médical connecté ou d'un logiciel dispositif médical contre le **risque** d'attaques et les attaques **intentionnellement malveillantes** dont il peut faire l'objet, et ce à toutes les étapes de son cycle de vie. »

2.8 Discussion autour de cette définition

Cette définition présente plusieurs points de faiblesse :

- On ne cherche pas uniquement à protéger les informations du DM mais également son fonctionnement

- La notion de traçabilité et de résilience n'apparaissent pas dans cette définition

Un travail sur la définition de la cyber sécurité, au cours de la rédaction du document, sera donc à effectuer.

L'expression « intentionnellement malveillante » est discutée. L'objectif de ce travail étant de rédiger des recommandations de manière à se prémunir d'attaques intentionnelles, par opposition à non-intentionnelles, dans le cadre d'un mésusage ou d'une erreur d'utilisation avec une volonté de nuire, cette précision mérite d'apparaître dans la définition.

Par ailleurs, le règlement UE relatif aux DM et la norme ISO 14971 ne contiennent pas de dispositions relatives à un usage malveillant du dispositif médical, quel que soit la nature du dispositif médical. Les virus informatiques ainsi que les utilisations visant à nuire sont des notions qui ont été peu prises en compte dans les réglementations et les normes relatives aux dispositifs médicaux.

Une question supplémentaire est soulevée : veut-on se protéger contre les mésusages ? Un mésusage peut être à l'origine d'une perte d'intégrité et de disponibilité des données, néanmoins il n'est pas prévu de traiter les mésusages de logiciels dans le cadre ce de groupe de travail.

Les notions clé à retenir pour la définition de la cyber sécurité sont donc : intégrité, disponibilité, résilience, aspect malveillant.

2.9 Plan du livrable

Pour le plan du document, 2 approches sont possibles :

- Aborder le sujet via la chronologie cycle de vie du logiciel DM (conception, développement, mise en service, surveillance, fin de vie du DM)

- Aborder le sujet par type d'activité (Identifier les vulnérabilités, Protéger, détecter les attaques etc.)

Les orientations générales pour établir le plan sont les suivantes :

- Conserver la distinction pré-market et post-market, tout en insistant sur la conception et le pré-market

- Porter les efforts du comité sur les notions d'intégrité et de disponibilité des données

3. Discussion

3.1 Protection des données personnelles

La question du traitement de la protection des données personnelles a été posée à plusieurs reprises par différents experts, en amont de cette première réunion.
Dans le champ du travail proposé, il est difficile de s'affranchir de cette question, mais les efforts pourraient être portés sur l'intégrité et la disponibilité des données, qui sont les « parents pauvres » du domaine.

Ce sont en effet ces 2 notions qui mettent directement en danger la santé et la sécurité du patient. La confidentialité est un point important, mais un vol de données personnelles est moins à même de constituer un risque vital en comparaison à une indisponibilité de données et/ou des systèmes ou à une compromission de l'intégrité des données et/ou des systèmes.
Par ailleurs, le sujet de la protection des données personnelles fait l'objet d'un règlement européen, le Règlement (UE) 2016/679, règlement général sur la protection des données (RGPD). Un renvoi vers ce document de référence sera effectué.
De plus, les mécanismes de protection qui seraient mis en place au sein d'un DM pour assurer l'intégrité et la disponibilité des données sont en partie capables de couvrir l'aspect confidentialité des données.

3.2 Fin de vie du logiciel

La question de la fin de vie du logiciel sera également à traiter. Plusieurs questions se posent :

- comment gérer la fin de vie des systèmes d'exploitation qui constituent l'environnement d'utilisation des logiciels ?

- comment gérer la fin de vie des aspects de chiffrement et des clés cryptographiques ? (clés cryptographiques qui expirent, quid de la récupération des données à ce moment là par ex, etc.)

- si une partie du DM (partie logiciel) est obsolète, considère-t-on que l'ensemble du DM est obsolète ?

3.3 Analyse de risques et catégories de DM

Dans le secteur médical, il peut y avoir un risque d'opposition entre la satisfaction d'exigences de sécurité et la satisfaction d'exigences fonctionnelles, notamment dans des contextes d'utilisation en urgence. Le challenge à relever pour ces questions de sécurité est de pouvoir combiner les exigences réglementaires et les possibilités terrain. Une catégorisation des DM en fonction de l'usage revendiqué est proposée (thérapeutique, monitoring/surveillance, diagnostic par exemple)

Même si l'analyse de risques est laissée à l'appréciation du fabricant, en fonction du contexte d'utilisation auquel il destine son dispositif médical, il est précisé que les problématiques de sécurité doivent être abordées différemment en fonction du DM, de sa destination, du risque de conséquences patient en cas de défaut de disponibilité ou d'intégrité du DM.

Une méthodologie est proposée par le groupe pour la définition du plan :

- définir des catégories de DM,
- puis raisonner en termes de vulnérabilités pour définir les protections à apporter

3.4 Le DM vecteur ou relais de l'attaque

Le DM doit être protégé pour éviter qu'il soit lui-même un vecteur d'attaque du SI dans lequel il est potentiellement intégré (exemple : accès aux données patient d'un établissement de santé en « entrant par » un IRM ou un scanner intégré au SIH)

En effet, si un DM est protégé contre une attaque, a priori, il est non-détournable pour attaquer un système, mais cela n'est pas systématique.

Exemple : un DM qui présente un faible risque de conséquences patient aura une classe de risque faible selon la réglementation DM et sa vulnérabilité vis-à-vis du système d'information hospitalier sera potentiellement négligée.

4. Conclusion

La prochaine étape consiste à établir le plan du document, avant répartition des différentes parties à rédiger entre les membres du CSST.

L'ANSM proposera un plan en même temps que le compte rendu de cette séance, pour commentaires et ajustements d'ici la 2è séance du CSST, dont la date sera définie ultérieurement.