SÉCURISATION DES DISPOSITIFS MÉDICAUX INTÉGRÉS AUX SYSTÈMES INFORMATIQUES

Jérôme LORANT
Ingénieur informatique Réseaux et Sécurité
Centre Hospitalier Yves le Foll
10, rue Marcel Proust
22000 SAINT-BRIEUC

Les obligations d'interconnexions des systèmes médicaux informatisés

La première décennie de notre siècle est marquée, dans le cadre du traitement de l'information de santé, par des besoins et des obligations d'échanges entre des systèmes qui s'ignoraient alors. Pourtant, dans certains établissements de santé les systèmes informatiques locaux n'intègrent toujours pas dans les projets ou le matériel informatique les dispositifs médicaux. Au siècle dernier, tant que les échanges d'information entre les dits systèmes n'étaient pas nécessaires, les réseaux s'ignoraient. Les Dispositifs Médicaux étaient installés isolément du système informatique local. Chaque secteur, dans son domaine remplissait les tâches qui lui incombaient. Dans un établissement de santé actuel, non seulement en local les systèmes sont appelés à communiquer, pour des logiques de fonctionnement et de sécurité mais chaque établissement doit maintenant échanger avec son voisin territorial, régional ou national, public ou privé. La Télémédecine de territoire a ouvert la voie bien avant les exigences de la loi HPST. Les Unités de Dialyses médicalisées du territoire des Côtes d'Armor, par exemple, peuvent récupérer ou envoyer des informations des Dispositifs Médicaux distants, par le biais d'un réseau opérateur dédié et sécurisé (BIPS : Breizh IP Santé). Il en sera très certainement de même pour l'imagerie, alors comment peut-on, dans ce dernier cas encore envisager, en fonction de la taille de l'établissement, qu'un PACS local ne soit pas appelé un jour ou l'autre à devenir un PACS territorial lui-même maillon d'un PACS national ?

Cette évidente évolution technique pour ceux qui y travaillent et sont à même de la prévoir, entraîne des changements de pratiques et d'approches conséquents, des bouleversements culturels qui peuvent paraître insurmontables pour certains établissements de santé. Toutefois, tout n'est pas technique et force est à la loi car les orientations politiques et juridiques telles que la loi HPST obligent à des changements techniques et organisationnels. D'autres secteurs d'activité ont réussi à surmonter ces impératifs d'échange d'informations professionnelles. La sécurité de l'information de santé doit dorénavant faire partie intégrante des projets touchant au systèmes d'information des établissements de santé mais aussi pourvoir à l'amélioration de l'existant.

Pour le domaine biomédical, les services informatiques des établissements n'intègrent pas, ou encore trop peu, les Dispositifs Médicaux qui sont de plus en plus informatisés et en réseau. Dans le pire des cas ils laissent libre action à la mise en place des réseaux isolés, qui semblent être "protégés" mais qui par cet isolement forcené ne sont pas surveillés : les mises à jour de sécurité ne peuvent se faire, et les antivirus n'existent pas, ou ne sont pas mis à jour… Il faut aussi reconnaître que dans la plupart des cas il n'existe aucune Politique de Sécurité d'établissement alors que politiques nationales, régionales voire territoriales sont en voie de finalisation sous l'impulsion de la PMSSIS (Politique Ministérielle de Sécurité des Systèmes d'Information de Santé).

La multiplication des supports mobiles tels que les clés USB, faisant la navette d'un réseau à l'autre est un vecteur de contamination important. A vouloir ne pas interconnecter les réseaux et de fait, mieux les surveiller, on accroît le risque de contournement des utilisateurs qui transfèrent eux même les informations d'un système à l'autre par le biais de supports infectés. L'expérience du ver Conficker en 2009 a mis en exergue le fait que pour la plupart des cas, dans les hôpitaux, les origines de propagation venaient de matériels informatiques de laboratoires, d'imagerie ou biomédicaux. Cette douloureuse expérience à ouvert les esprits vers des échanges professionnels plus appuyés entre les informaticiens et les techniciens biomédicaux. Force est tout de même de constater que la majeure partie des personnels biomédicaux actuellement en activité et jusqu'à une certaine génération n'ont pas eu de formation informatique de base. Cela a pour effet de « crisper les échanges techniques » entre les secteurs biomédicaux et informatiques dans le cadre d'intégration des Dispositifs médicaux informatisés. Dans le pire des cas, le secteur informatique considère les équipements biomédicaux comme différents des outils informatiques classiques et le secteur biomédical considère qu'il n'a pas à gérer le volet informatique. Ce dernier est souvent parfois amener à accepter des solutions informatisées« clé en main »d'intégrateurs ou industriels sans avoir pensé à leur intégration dans le système d'information local et avoir sollicité la DSI locale.

Par la force des choses et le cadre législatif de plus en plus prégnant ; les habitudes sont entrain de changer avec la prise de conscience de l'importance de l'information médicale dans sa disponibilité, sa confidentialité et son intégrité... et finalement, pour survivre et vivre ne vaut-il pas mieux se regrouper que se diviser ?.

Il s'agit aussi de rappeler que dans la majeure partie des cas : « La DSI doit mener un travail de fond concernant ses relations avec les services effectuant de fait des acquisitions informatiques (biomédical, laboratoires, services techniques, imagerie, pharmacie). Cela passe par des sensibilisations ou des formations régulières (éléments présents dans l'ISO 27002) et la mise à disposition de ressources ingénieur pour instruire les demandes les plus en amont possible. C'est à ces seules conditions que la sécurité de ces équipements pourra être assurée[1] ».

[1] *La Sécurité des Systèmes d'Information des établissements de santé, Cédric CARTAU, Presses de l'EHESP, 2012, p 180.*

Biomédical et informatique en général

Comme nous l'avons vu précédemment et de manière introductive, quelle que soit la taille d'un établissement de santé, il est actuellement inconcevable de penser qu'il n'existe aucun rapprochement technique et organisationnel entre le service informatique et le service biomédical.

Les deux secteurs, semblent indubitablement différents à la fois dans leur technicité originelle mais aussi dans le service rendu. Pourtant depuis maintenant quelques années le secteur biomédical installe ou fait installer des dispositifs médicaux qui sont équipés d'interfaces physiques et logiques (réseaux et applications) et le fonctionnement de ces derniers rejoint de fait les postes informatiques installés pour d'autres secteurs ou métiers de l'hôpital. Le métier de technicien biomédical a aussi évolué du « purement mécanique » vers les couches physiques électroniques ou logiques (dans le sens de logicielle) que l'informatique impose. La nouvelle génération de techniciens sortant des écoles biomédicales doit être familiarisée avec les techniques de base de l'informatique surtout et principalement en ce qui concerne les échanges clients/serveurs et la mise en réseau spécifiques et sécurisés (Vlan dédiés, Firewall et antivirus). Il n'est en aucun cas demandé aux services biomédicaux d'avoir en charge la totalité de l'informatique de leur secteur mais plutôt d'avoir des connaissances sur le sujet qui permettront à la fois des échanges simplifiés avec les services informatiques locaux mais aussi et de manière devenue naturelle d'intégrer dans les cahiers des charges et les CCTP la partie informatique et sécurité de l'information.

Lorsqu'il s'agit de sécurité, le volet qui induit à la fois la disponibilité, l'intégrité et la confidentialité de l'information a souvent fait l'objet soit d'un total oubli ou d'un rabotage sévère des moyens financiers. Pourtant, les recommandations et politiques nationales ministérielles s'enchaînent maintenant depuis presque 10 ans (Décret de Confidentialité, Certification de la HAS, Loi HPST 2009, la Politique Ministérielle de Sécurité des Systèmes d'Information de Santé de 2011 et enfin le programme Hôpital Numérique de 2012-2013…)

Pendant trop longtemps les expressions de besoins dans le secteur biomédical ce sont, et cela se comprend historiquement, cantonnés à la finalité du produit de soin, en l'absence durant des années d'une obligation de communiquer avec les autres systèmes des établissements pour fonctionner ou récupérer des informations d'ordre médical ou identitaire. De plus, le marquage CE et ses obligations ont semé pendant un temps le trouble quant à la modification, l'utilisation et l'interconnexion des Dispositifs médicaux. Combien de DMP informatisés ont été installés sans Antivirus par excès de prudence quant à ce marquage CE.

Comment doit-on procéder de manière systématique pour que le secteur biomédical qui constitue en lui-même un système d'information puisse intégrer le système d'information global d'un établissement ? Aucun secret à cela, tout simplement des échanges continuels entre les services informatiques et biomédicaux afin que l'expérience d'un secteur serve à l'autre et inversement. A la fois en ce qui concerne la partie technique mais aussi organisationnelle, le risque informatique et par extension la sécurité de l'information doivent faire l'objet d'une gestion des risques à l'instar de la sécurité incendie ou des personnes, par exemple. Pour ce faire une méthodologie normalisée, complétée d'une approche systémique, adaptée peuvent conduire au succès attendu.

Comment intègre-t-on les dispositifs médicaux dans le système d'information ?

Méthodologie et approche systémique (du système informatique au système d'information)

La sécurité des Dispositif médicaux et des systèmes de santé qui en découle ne se cantonne pas uniquement à la partie intégration physique du matériel et des moyens techniques sécuritaires que l'on va mettre en place, Vlan, Firewall, IPS. Toutefois, les principaux échanges entre le service informatique et biomédical devront porter sur les critères techniques suivants :

- Sureté des infrastructures avec la résilience des liens physiques, électriques et réseaux informatiques. La redondance des éléments actifs (Switchs, Serveurs). Sans être exhaustive, cette première partie répond en majeure partie aux critères de Disponibilité de l'information.

- Mise en réseau et système avec des switchs et Vlan dédiés, de la commutation et du routage optimaux pour l'imagerie, Backbone à 10 Gigabits si possible, intégrations des serveurs biomédicaux dans l'infrastructure système de l'établissement dans les salles serveurs climatisées sécurisées avec contrôle des accès. Prévoir une télémaintenance, via des VPN, clairement identifiée avec le contrôle des outils de prise à distance des prestataires, le contrôle des accès avec traçabilité des connexions et des modifications apportées au système. Il s'agit de répondre aux critères de disponibilité, de confidentialité, d'intégrité et de traçabilité.

- Intégration et identification précises des DM (logiques et géographiques) avec une protection antivirale obligatoire… Intégrité et Confidentialité.

Pour répondre efficacement aux exigences de sécurité précédemment évoquées il faudra irrévocablement en passer par une analyse des risques. Il va s'agir de savoir précisément ce qu'il faut protéger et à quel degré. L'environnement humain et les pratiques professionnelles doivent être pris en compte avant d'entamer toute démarche de sécurité.

Sans une approche méthodique, voire systémique, la sécurisation efficace est vouée à l'échec : Soit par oubli de l'essentiel ou par une sécurisation à outrance. Il faut pour cela garder à l'esprit que le risque 0 n'existe pas, il s'agira donc de sécuriser ce qui est nécessaire dans un système et non la totalité de celui-ci. Une acceptation du risque fait aussi partie de la démarche sécuritaire. Pour mieux appréhender une démarche d'analyse et engager le processus le plus simplement possible, il est possible de commencer par une

méthode de questionnement du type QQOQCP (Qui, Quoi, Où, Quand, Comment, Combien, Pourquoi ?)[2] :
Cette première méthode permet de préparer le terrain pour une analyse des risques plus en profondeur.
De plus, quelle meilleure passerelle culturelle et sémantique, pourrions-nous trouver que celle de l'approche systémique dont le nom en lui-même sonnera aux oreilles des médecins et chercheurs comme un terme connu :

Lettre	Question	Sous-questions	Exemples
Q	Qui ?	De qui, Avec qui, Pour qui…	Responsable, acteur, sujet, cible…
Q	Quoi ?	Quoi, Avec quoi, en relation avec quoi…	Outil, objet, résultat, objectif…
O	Où ?	Où, par où, vers où…	Lieu, service…
Q	Quand ?	tous les quand, à partir de quand, jusqu'à quand…	Dates, périodicité, durée…
C	Comment ?	de quelle façon, dans quelles conditions, par quel procédé…	Procédure, technique, action, moyens matériel…
C	Combien ?	Dans quelle mesure, valeurs en cause, à quelle dose…	Quantités, budget…
P	Pourquoi ?	Cause, facteur déclenchant	Justification par les causes qui ont amenés à ... (la "raison" d'être, la croyance)
	Pour quoi ?	Motif, finalité, objectif	Justification par le souhait, l'ambition, la prévision...

L'approche systémique parfois nommée analyse systémique est un champ interdisciplinaire relatif à l'étude d'objets dans leur complexité. Pour tenter d'appréhender cet objet d'étude dans son environnement, dans son fonctionnement, dans ses mécanismes, dans ce qui n'apparait pas en faisant la somme de ses parties, cette démarche vise par exemple à identifier :

- la « finalité » du système (téléologie),
- les niveaux d'organisation,
- les états stables possibles,
- les échanges entre les parties,
- les facteurs d'équilibre et de déséquilibre
- les boucles logiques et leur dynamique, etc.

Née aux Etats Unis au début des années 50, connue et pratiquée en France depuis les années 70, l'approche systémique ouvre une voie originale et prometteuse à la recherche et à l'action. La démarche a déjà donné lieu à de nombreuses applications, aussi bien en biologie, en écologie, en économie, dans les thérapies familiales, le management des entreprises, l'urbanisme, l'aménagement du territoire, etc. Elle repose sur l'appréhension concrète d'un certain nombre de concepts tels que: système, interaction, rétroaction, régulation, organisation, finalité, vision globale, évolution, etc. Elle prend forme dans le processus de ***modélisation***, lequel utilise largement le langage graphique et va de l'élaboration de modèles qualitatifs, en forme de "cartes", à la construction de modèles dynamiques et quantifiés, opérables sur ordinateur et débouchant sur la simulation. C'est pourquoi la mise en oeuvre de cette démarche passe par un effort d'apprentissage conceptuel et pratique auquel doivent consentir tous ceux (chercheurs, décideurs professionnels et politiques, hommes d'action mais aussi simples citoyens désireux de comprendre leur époque) qui ambitionnent de réaliser une plongée heureuse dans la complexité, afin d'être capable dans un premier temps de s'y orienter, puis dans un second temps d'agir sur elle. Combinant en permanence connaissance et action, la systémique se présente comme l'alliance indissoluble d'un savoir et d'une pratique.[3]

Je suis personnellement convaincu que cette approche scientifique est parfaitement transposable à la sécurité de l'information et une fois les deux parties présentes, méthode de questionnement et approche systémique, dans le processus d'intégration et de sécurisation des dispositifs médicaux, il est plus facile de rendre familière et systématique une analyse des risques. Pour ce dernier volet, nous pouvons nous appuyer sur des méthodes telles qu'EBIOS ou MEHARI[4] pour ne citer qu'elles. L'ANSSI, référence ministérielle et nationale pour les institutions publiques, propose EBIOS dans une version 2010 beaucoup plus digeste qu'auparavant et compatible ISO 27005.

Il faut bien avoir à l'esprit qu'il ne s'agit pas de réinventer la roue de Deming, mais de comprendre que le risque informatique rejoint de fait le risque de l'information. Il ne faut donc plus réfléchir et agir uniquement en tant que technicien et dans la sémantique intégrer le fait, une fois pour toute, qu'il s'agira définitivement de se placer dans un système d'information et non un système informatique. Chronologiquement, Les chefs de Centres informatiques sont devenus des RSI (Responsables des systèmes Informatiques) pour être chapeautés par des DSI (Direction des Systèmes d'Information) et certain RSI ou RSIO sont eux même devenus des Directeur des Systèmes d'Information. Cette « révolution sémantique » permet aussi d'intégrer le risque de l'information dans le processus général de gestion des risques d'un établissement de Santé ce qui laisse aussi sous-entendre que le sujet dans sa globalité n'est plus l'apanage de la seule DSI. Les Direction des Ressources Humaines, les Direction de la Qualité pourront elles aussi s'approprier la sécurité de l'information.

[2] Toute démarche d'analyse implique en effet une phase préalable de « questionnement systématique et exhaustif » dont la qualité conditionne celle de l'analyse proprement dite, ceci en vue de collecter les données nécessaires et suffisantes pour dresser l'état des lieux et rendre compte d'une situation, d'un problème, d'un processus ».Source : http://fr.wikipedia.org/wiki/QQOQCCP

[3] Sources : http://fr.wikipedia.org/wiki/Approche_syst%C3%A9mique, et http://www.afscet.asso.fr/SystemicApproach.pdf

[4] EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité, ANSSI 2010, MEHARI : MEthode Harmonisée d'Analyse des Risques, Clusif 2010

Gestion des risques et intégration du risque informationnel

En ce qui concerne la sécurité de l'information et à partir du moment où nous nous mettons à penser que la santé n'est plus un secteur différent des autres -du fait de sa confrontation aux technologies de communication et au partage d'informations sensibles - il s'agira de prendre exemple sur des secteurs dont la sécurité de l'information est une culture intégrée depuis des décennies (Banque, Assurances, Défense). Quels est le premier critère évident qui nous rapproche de ces secteurs ? Tout simplement le classement que la CNIL fait de nos informations : elles sont classées sensibles, juste en dessous des Confidentialité et Secret Défense. De plus, il faut savoir que les informations de santé font l'objet, de plus en plus, de trafics maffieux de revente ou d'usurpation d'identité médicale.

Qu'ont donc fait les autres secteurs professionnels avant nous et qu'est-ce qui peut expliquer leur avance ? Tout d'abord la participation aux travaux et l'utilisation de normes spécifiques à la sécurité de l'information, plus précisément les normes ISO de la Famille 27000 :

Les normes de la famille ISO 27000 permettent d'organiser et structurer la démarche de la gestion de la sécurité des systèmes d'information.

- *ISO 27001 décrit les processus permettant le management de la sécurité de l'information (SMSI)*
- *ISO 27002 présente un catalogue de bonnes pratiques de sécurité*
- *ISO 27003 décrit les différentes phases initiales à accomplir afin d'aboutir à un système de Management tel que décrit dans la norme ISO 27001*
- *ISO 27004 permet de définir les contrôles de fonctionnement du SMSI*
- *ISO 27005 décrit les processus de la gestion des risques*
- *ISO 27006 décrit les exigences relatives aux organismes qui auditent et certifient les SMSI des sociétés.*

Il faut donc que ces normes soient connues et utilisées par les service qualité et gestion des risques des établissements de santé à l'instar de l'utilisation des normes ISO 9000. Ces normes, 9000 et 27000 il faut le savoir, sont étroitement liées structurellement et culturellement.

L'information de santé et le cadre juridique

Point besoin pour cette dernière partie, de développer les contraintes et obligations légales et réglementaires auxquelles les établissements de santé sont confrontés et familiarisés… sauf en ce qui concerne la sécurité de l'information, pour laquelle depuis une dizaine d'années Décrets et loi se succèdent et font corps maintenant avec les projets numériques. Voici donc une présentation non exhaustive du cadre juridique de base.

Le Décret de confidentialité

L'objet du décret de confidentialité publié au JO le 17 mai 2007 est de déterminer *les exigences de confidentialité et de sécurité* à respecter par les professionnels de santé, les établissements de santé, les réseaux de santé, et tout organisme participant au système de santé, qui *conservent sur support informatique et échangent par voie électronique* des données de santé à caractère personnel.
Le décret rend obligatoire le respect de référentiels définis par arrêté du Ministre chargé de la santé, qui décrivent les règles de sécurité et de confidentialité destinées à garantir en toutes circonstances le secret médical.
Son champ d'application concerne notamment la mise en œuvre dans les établissements :

D'une *politique de sécurité et de confidentialité*.
Des *référentiels de sécurité* relatifs à la confidentialité des données médicales.
De la *sécurisation des accès* avec la CPS et de l'organisation de sa gestion.
D'un *annuaire unique d'établissement* (référentiel des personnes) et de l'organisation de la gestion des mouvements de personnel.

D'une conduite du changement :

- *Sensibilisation à la confidentialité* (Politique de sécurité, charte, RSSI, responsabilité pénale, protocole de confidentialité…).
- *Repenser l'organisation* : Modélisation des processus cibles & guide d'élaboration de document et de cahier des charges.[5]

La PMSSI de Santé

Existait-il il y a encore quelques années et dans très peu d'établissements de santé, des politiques de sécurité autres que techniques ? Très souvent un Antivirus, un Firewall et quelques contrôles d'accès confortaient, à tort, la plupart des directions d'établissements alors que la majorité des incidents et accidents en sécurité de l'information était ou est encore due à des comportements humains non adaptés, du personnel non formé donc non sensibilisé.

En 2011, le Ministère de la Santé a fait part de la directive gouvernementale de doter la Santé d'une PMSSI, alors que d'autres institutions toutes aussi sensibles en bénéficiaient déjà depuis quelques années. Il s'agit là d'une avancée considérable dans le domaine de la santé et de la sécurité de l'information qui a l'avantage de devenir, de fait, déclinable jusqu'au niveau local des établissements. Cette PMSSI est ni plus ni moins empreinte des normes ISO 27000 et ses directives se basent sur la norme ISO 27002, document indispensable a une approche sécuritaire structurée et méthodique.

« La PMSSI peut être définie comme étant l'ensemble formalisé des éléments stratégiques et des principes de sécurité, ayant comme objectif la protection de système d'information »[6]

[5] *https://www.esante-poitou-charentes.fr/portail/tout-savoir-sur/politique-de-securite-du-sis/securite-des-systemes-d-informations/decret-de-confidentialite,197,188.html*

[6] *Extrait du document de politique générale PMSSI diffusé le 21/01/2011 par le ministère du travail de l'emploi et de la santé, source Frédéric CABON, RSSI du CHRU de Brest*

Conclusion

Les exigences légales et réglementaires ont mis en avant la sécurité de l'information dans le domaine de la santé. Ce sujet, la sécurité de l'information, est déjà traité et intégré dans des secteurs comme la banque, les assurances, la défense et ce depuis déjà de nombreuses années. Il n'y a aucun secret dans la recette, il s'agit de mettre en application les conseils et directives des normes de la famille ISO 27000. Encore faudra-t-il conserver à l'esprit qu'il s'agira avant tout de mettre la technique au service de l'humain mais que l'erreur elle est bien et sera toujours humaine. Il est donc encore temps de changer les points de vue par le biais de présentations, de formations et de sensibilisation sur le sujet... et enfin aborder le sujet de la sécurité de l'information autrement que par la contrainte systématique et la coercition. Pour se faire, les discours doivent être adaptés et ne plus être l'apanage que des seuls techniciens. La Sécurité de l'Information doit impérativement faire partie de la gestion des risques d'un hôpital au même niveau que le sanitaire et la technique. Sans cette approche, les établissements de santé échoueront irrémédiablement ou d'autres secteurs ont ou réussissent déjà.

Dans tous les cas et au regard des expériences vécues au sein d'établissement de diverses tailles, aussi bien ceux qui ont courageusement anticipé le processus de sécurisation que d'autres qui faute de moyens ou tout simplement de maturité ont toujours procédé par petites touches ou rustines rassurantes. Je peux leur proposer de méditer une citation de Francis Blanche : « Il vaut mieux penser le changement que changer le pansement »

Biblio et Webographie

Ouvrages :

La Sécurité des Systèmes d'Information des établissements de santé, Cédric CARTAU, Presses de l'EHESP, 2012.

Supports :

Exigences de sécurité des Systèmes d'Information pour les équipements biomédicaux des établissements de santé, Guillaume DERAEDT (RSSI, CHRU de Lille), François FAURE (IBMH, CHU d'Angers). Présentation HIT 2010.

Liens WEB :

http://www.sante.gouv.fr/IMG/pdf/DGOS_Guide_d_indicateurs_Programme_Hopital_Numerique_-_avril_2012-2.pdf

https://www.esante-poitou-charentes.fr/portail/tout-savoir-sur/politique-de-securite-du-sis/securite-des-systemes-d-informations/decret-de-confidentialite,197,188.html

http://www.i-med.fr/spip.php?article335

http://www.sante.gouv.fr/IMG/pdf/_CP_DGOS_Programme_Hopital_numerique_-_Politique_nationale_relative_aux_SIH_-_mai_2012.pdf

http://fr.wikipedia.org/wiki/Approche_syst%C3%A9mique

http://www.sante.gouv.fr/IMG/pdf/DGOS_Guide_d_indicateurs_Programme_Hopital_Numerique_-_avril_2012-2.pdf

http://www.ssi.gouv.fr/IMG/pdf/EBIOS-1-GuideMethodologique-2010-01-25.pdf

ANALYSE DES RISQUES LIÉES À LA MISE SUR LE RÉSEAU DE SYSTÈMES INFORMATIQUES ASSOCIÉS À DES DISPOSITIFS MÉDICAUX, ET DES AUTOMATISMES

Philippe TOURRON
Responsable de la Sécurité du Système d'Information
Chef du service Sécurité-Qualité de la DSIO
APHM
Direction des Systèmes d'Information
et de l'Organisation
125 bd Baille
13005 MARSEILLE

Gilles FRENKIAN
Ingénieur Biomédical en Chef
AP-HM
Direction Médicaux Technique & des Equipements Biomédicaux
80 Rue Brochier
13354 MARSEILLE Cedex 05

Compte tenu de l'évolution des technologies embarquées dans les dispositifs médicaux, il est devenu impératif de concilier une intégration croissante des moyens des domaines biomédical et technique aux architectures gérées par les DSI d'établissements de santé (ETBS). Encore indépendants et autonomes il y a peu de temps, ces systèmes convergent vers des environnements standards (serveurs et stockages). Ainsi les techniques de virtualisation comme les échanges via le réseau local s'invitent dans les paysages technique et biomédical.

Cette intégration conduit à gérer la sécurité de ces architectures hybrides en conformité avec les politiques de sécurité des ETBS. Une phase d'adaptation et de transition est souvent nécessaire face à des éditeurs et fabricants pas toujours prêts à respecter ces nouvelles exigences, et à des équipes qui n'avaient pas l'habitude de gérer ces « zones » d'interface.

La problématique se pose en ces termes : « Comment aborder la sécurité du SI dans ce contexte et quels outils vont être nécessaires pour progresser dans cette voie ? ».
L'approche par les risques semble une méthodologie qui permettra : de baliser des étapes de progression et d'identifier des mesures de sécurité pour gérer ce changement majeur des SI hospitaliers.

1. Les évolutions

Les technologies « réseaux » implémentées dans la plupart des Dispositifs Médicaux ainsi que dans les équipements techniques de gestion centralisée, sont maintenant supportées par l'infrastructure du réseau hospitalier. Cette évolution induit des risques émergents qui doivent être pris en compte par les différents services gestionnaires ou support. Les risques deviennent partagés : D'où l'importance de la visibilité et de la compréhension des besoins de sécurité de chaque composant(e) de la chaîne de traitement.

Exemple : un serveur hébergé à la DSI, s'il est virtualisé, doit hériter des mesures de sécurité en cohérence avec les besoins de sécurité des données ou processus à protéger qu'il héberge tout comme une console ou un poste d'acquisition.

2. Les composants d'un risque SI

La réduction des risques inhérents aux systèmes informatiques, passe impérativement par la connaissance de l'inventaire des produits et processus qui le compose et communiquent au sein du système d'information. Cette approche permet d'apprécier la vulnérabilité, d'exprimer les besoins et d'identifier les objectifs de sécurité afin de traiter au mieux les risques relatifs à la sécurité des systèmes d'information (SSI).

Pour atteindre cet objectif : la méthode de gestion des risques EBIOS[1] (***E***xpression des ***B***esoins et ***I***dentification des ***O***bjectifs de ***S***écurité) permet d'apprécier et de traiter les risques relatifs à la Sécurité des Systèmes d'Information (SSI).

Elle permet aussi de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires afin de contribuer au processus commun de gestion des risques SSI. En fournissant les justifications nécessaires à la prise de décision (descriptions précises, enjeux stratégiques, risques détaillés avec leur impact sur l'organisme, objectifs et exigences de sécurité explicites), EBIOS est un véritable outil de négociation et d'arbitrage.

L'ISO 27005 définit un cadre, EBIOS est la méthode pour le mettre en œuvre [2]

La norme internationale ISO 27005 définit un cadre commun pour gérer les risques de sécurité de l'information. Elle présente ainsi les principes qui ont fait l'objet d'un consensus international. De ce fait, il ne s'agit évidemment pas d'une méthode directement applicable. Pour appliquer ces principes, l'emploi d'une méthode est indispensable, et chacun peut créer sa propre démarche. L'évolution d'EBIOS en EBIOS 2010 permet aujourd'hui de gérer les risques conformément à l'ISO 27005 en utilisant la terminologie des normes internationales :

- ***le risque*** est un scénario, avec un niveau donné, combinant un événement redouté et un ou plusieurs scénarii de menaces ; son niveau correspond à l'estimation de sa vraisemblance et de sa gravité ;

- *l'événement redouté* est un scénario générique représentant une situation crainte par l'organisme ; il s'exprime par la combinaison des sources de menaces susceptibles d'en être à l'origine, d'un bien essentiel, d'un critère de sécurité, du besoin de sécurité concerné et des impacts potentiels ;

- *le scénario de menace* est un scénario, avec un niveau donné, décrivant des modes opératoires ; il combine les sources de menaces susceptibles d'en être à l'origine, un bien support, un critère de sécurité, des menaces et les vulnérabilités exploitables pour qu'elles se réalisent ;

- *la gravité* est l'estimation de la hauteur des effets d'un événement redouté ou d'un risque ; elle représente ses conséquences ;

- *la vraisemblance* est l'estimation de la possibilité qu'un événement redouté, un scénario de menace ou un risque, se produise ; elle représente sa force d'occurrence ;

- *l'objectif de sécurité* est l'expression de la décision de traiter un risque selon des modalités prescrites ; on distingue notamment la réduction, le transfert (partage des pertes), le refus (changements structurels pour éviter une situation à risque) et la prise de risque ;

- *la mesure de sécurité* est le moyen de traiter un risque de sécurité de l'information ; la nature et le niveau de détail de la description d'une mesure de sécurité peuvent être très variables.

3. EBIOS : méthode de gestion des risques

La démarche est dite itérative. En effet, il sera fait plusieurs fois appel à chaque module afin d'en améliorer progressivement le contenu, et la démarche globale sera également affinée et tenue à jour de manière continue.

Module 1 - Étude du contexte

À l'issue du premier module, qui s'inscrit dans l'établissement du contexte, le cadre de la gestion des risques, les métriques et le sujet de l'étude sont parfaitement connus ; les biens essentiels, les biens supports sur lesquels ils reposent et les paramètres à prendre en compte dans le traitement des risques sont identifiés.

Module 2 - Étude des événements redoutés

Le second module contribue à l'appréciation des risques. Il permet d'identifier et d'estimer les besoins de sécurité des biens essentiels (en termes de disponibilité, d'intégrité, de confidentialité…), ainsi que tous les impacts (sur les missions, sur la sécurité des personnes, financiers, juridiques, sur l'image, sur l'environnement, sur les tiers et autres…) en cas de non-respect de ces besoins et les sources de menaces (humaines, environnementales, internes, externes, accidentelles, délibérées…) susceptibles d'en être à l'origine, ce qui permet de formuler les événements redoutés.

Module 3 - Étude des scénarii de menaces

Le troisième module s'inscrit aussi dans le cadre de l'appréciation des risques. Il consiste à identifier et estimer les scénarii qui peuvent engendrer les événements redoutés, et ainsi composer des risques. Pour ce faire, sont étudiées les menaces que les sources de menaces peuvent générer et les vulnérabilités exploitables.

Module 4 - Étude des risques

Le quatrième module met en évidence les risques pesant sur l'organisme en confrontant les événements redoutés aux scénarii de menaces. Il décrit également comment estimer et évaluer ces risques, et enfin comment identifier les objectifs de sécurité qu'il faudra atteindre pour les traiter (notions de réduction, transfert, refus, prise de risques).

Module 5 - Étude des mesures de sécurité

Le cinquième et dernier module s'inscrit dans le cadre du traitement des risques. Il explique comment spécifier les mesures de sécurité à mettre en œuvre, comment planifier la mise en œuvre de ces mesures et comment valider le traitement des risques et les risques résiduels.

Cette dernière étape met aussi les mesures en perspective d'application avec les notions de défense en profondeur, de déclaration d'applicabilité, de plan d'action et de validation.

4. Macro-analyse de risque (non exhaustive) en 5 étapes

Module 1 - Étude du contexte

Le périmètre des risques analysés couvre tous les systèmes autres que les applications « natives » de la DSI. Nous utiliserons la Terminologie : Système d'Information Hospitalier (que nous ne décrirons pas), Système Biomédical et Gestion Technique. Il s'agit souvent de 3 SI distincts dans leur architectures et leurs gestions. Il devient donc essentiel d'en gérer les interfaces et les recouvrements.

Le Système Biomédical :

Il concerne des Systèmes informatiques actifs connectés ou implémentés sur le dispositif médical (DM) : capteur, unité informatique spécifique, process…), par exemple, les boites têtières EEG de captation et de transfert des signaux physiologiques peuvent être un composant connecté voire mutualisé. Le traitement spécifique des données sur un ordinateur spécifique, ainsi que le « stockage dédié » ou non au biomédical font partie intégrante du périmètre à prendre en compte dans le cadre de cette gestion des risques.

La Gestion Technique :

Sont concernés tous les équipements de pilotages, surveillances ou gestions nécessaires au fonctionnement des infrastructures hospitalières.

Les enjeux : Fiabiliser les fonctionnements et garantir un accès contrôlé aux informations et aux process.
Les évolutions du cadre réglementaire, du marché et des technologies conduisent à de nouveaux enjeux de maîtrise :

- De *la prise en compte de la confidentialité* des données patient;
- De *l'Interpénétration* des SI (composites) ;
- Du *Passage d'un mode isolé à un mode communiquant et mutualisé.* En effet, depuis environ 5 ans on constate une forte connexion des outils/composants autres que « natifs » des DSI, sur le réseau hospitalier ainsi que l'hébergement des serveurs et applications sur des parcs standards des DSI.

Les Processus médicaux "inter-pénétrants" sont de tous types et toutes origines :

- Exploration fonctionnelle (épreuve d'effort, ecg, holter, …)
- Traitement des patients (radiothérapie, hémodialyse, …)
- Analyse (laboratoire)
- Supervision d'équipement (caisson hyperbare, traitement d'eau de dialyse, …)

Et les informations issues de ces dispositifs sont très diverses :

- Données patients : avec comme objectif de sécurité une confidentialité importante ;
- Données techniques : avec comme objectif de sécurité une disponibilité importante des éléments relatifs aux configurations, résultats …

Les Sources de menaces sont multiples et peuvent être classées en deux types de sources :

- *d'Origines Humaines :*
  - Via les Techniciens de maintenance : internes et externes (erreurs de configuration, transfert de virus lors de mise à jour par clef usb, …)
  - Par des Démonstrateurs (mise en place de fonctionnalité ou logiciels non validés/sécurisés : marquage CE, non-conformité aux politiques de sécurité internes), exemple : un logiciel de pousse seringue récupéré sur internet peut présenter des défaillances d'intégrité de fonctionnement
  - Par les Utilisateurs eux-mêmes lors de l'installation de logiciels qui perturbent le fonctionnement (jeux, films, applications d'origines douteuses, …) ou d'erreurs d'utilisation
  - Hacker, …
- *d'Origines Non Humaines :*
  - Code malveillant ;
  - Coupure électrique/climatisation;
  - Foudre, surtension ;
  - Phénomène naturel ou canalisations : inondation ; …

Les Critères qui permettent d'évaluer la prise en charge de la protection des données par rapport au niveau de risque acceptable sont :

- la disponibilité : moyens ou données accessibles dans un délai convenu
- l'intégrité : données et calculs à un degré de précision attendu
- la confidentialité : l'évolution de la prise en compte de ce critère fait notamment suite à une nouvelle prise de conscience imposée par les recommandations et exigences de la CNIL (Commission Nationale Informatique et Libertés);
- la preuve : comme dans toutes approche 'certifiante' il est de plus en plus important de pouvoir apporter des éléments de preuves relatifs aux engagements pris ainsi qu'aux exigences légales et réglementaires.

Certaines *Mesures de sécurité sont déjà existantes* (sauvegarde, contrôle des réglages, antivirus,…), toutefois elles sont variables selon les éditeurs/fournisseurs et les ETBS. L'analyse de ces mesures ne fait pas l'objet de cette présentation.

Module 2 - Étude des événements redoutés (ER)

- Une Mauvaise Configuration ou un étalonnage erroné (réglage de conformité) ;
- La Perte de configuration des différents systèmes ;
- L'Obsolescence technologique des dispositifs malgré des fonctionnalités 'parfaites' du DM ;
- Vieillissement non contrôlé du parc (maintien 'pirate' d'un matériel après remplacement) ;
- Incompatibilité des équipements périphériques avec les dispositifs biomédicaux toujours opérationnels et répondant aux besoins suite à des renouvèlements partiels (exemple : disparition des interfaces RS232, IEEE 485, interfaces parallèle type centronics, …) ;
- Plus largement, des Erreurs conduisant à un impact sur les patients ;
- L'Impossibilité de délivrer les résultats ;

Module 3 - Étude des scénarii de menaces (SM)

- Virus apporté par un technicien de maintenance
- Introduction de systèmes non contrôlée
- Gestion des changements non contrôlée (ou contrôlée mais sans analyse des impacts) du système hébergeant les fonctionnalités informatiques de traitement
- Accès pirate aux dispositifs et aux systèmes de traitement (et au systèmes techniques dont dépendent les SI biomédical et SIH)
- Collecte d'information vers le fournisseur à l'insu de l'ETBS
- Fin de vie ou maintenance avec récupération des supports numériques
- Non déclaration de données nominatives

Ces SM peuvent tout aussi bien provenir ou s'attaquer à des *Biens Supports* tels que :

- Capteurs ;
- Dispositifs actifs
- Réseau d'échange
- Poste /console

- Postes/serveurs de traitement
- Locaux dédiés (salles serveurs,... qui peuvent être communs avec le SIH)

Module 4 - Étude des risques

Le Risque est la composition/combinaison : ER x SM qui permet la rédaction d'un scénario de risque comme décrit dans les 3 exemples suivants.

Scénario 1 : Des données issues du fonctionnement d'un Dispositif Médical (données de patients non anonymisées), sont utilisées par un fournisseur (sans l'accord de l'ETBS ni des patients) pour mettre au point des techniques ou produits sans aucuns liens avec l'objet du contrat portant sur le DM en place et liant l'ETBS avec le Fournisseur. Ceci peut provoquer un préjudice d'image ou financier et juridique.

Scénario 2 : Lors d'une visite de maintenance sur des postes non SIH connectés au réseau, un employé du prestataire utilise sa clef USB pour effectuer une mise à jour et 'infecte' par un virus les machines maintenues puis celles du réseau qui ne sont pas protégées soit par omission, soit pour des raisons techniques. Les machines infectées ne permettent plus de produire les résultats nécessaires aux soins des patients. Les chances de soins aux patients peuvent être diminuées.

Scénario 3 : Des informations de traitement médical de patients issues de dispositifs sont publiées sur internet, des plaintes sont déposées. Ces données ont été collectées via le système de maintenance à distance.

A l'issu d'un *choix de traitement* (réduire, éviter, transférer ou prendre les risques), des Mesures seront sélectionnées pour les risques à réduire à un niveau acceptable. Elles auront pour objectif la limitation des risques et s'appliquent principalement aux biens supports.

Module 5 - Étude des mesures de sécurité

Exemple de mesures:

- Engagement de confidentialité formalisé et signé par les acteurs du SI
- Sensibilisation pour prendre conscience des risques (consignes, formation, chartes, e-learning …)
- Marchés d'achat : règles d'intégration au(x) SI ou de qualification des composants
- Contrats de maintenance : sortie d'information /collecte automatique vers le mainteneur à décrire et identifier la présence de données patient
- Contrats de recherche : clause de diffusion et contrôle des données de santé
- Anonymiser les données (lors des envois, récupération pour maintenance)
- Procédure et moyen de destruction des données (patients) sur les supports en fin de vie ou maintenance (intégration dans les marchés)
- Garantir l'auditabilité : avoir des comptes permettant de consulter les paramètrage des dispositifs
- Engagement de mise à jour des composants (correctifs de sécurité)
- Exigence d'antivirus (niveaux à identifier : compatibilité avec celui validé par l'ETBS, antivirus fourni et mis à jour par le mainteneur, …)
- Organisation (clause contractuelle, tests) de la réversibilité : Récupération d'un appareil en maintenance, de données en mode hébergé.

Conclusion

La résistance d'une chaîne est liée à son plus faible maillon, ainsi tous les composants des SI interconnectés doivent être intégrés dans une gestion des risques. Pour arriver à gérer les risques de manière globale dans un environnement hospitalier il convient donc de favoriser et d'organiser les échanges entre les acteurs gestionnaires des composants à protéger. Utiliser une méthode, un langage et des outils communs comme EBIOS facilite la compréhension commune des scénarios de risques, des risques en cascades ou combinés et des mesures à appliquer. S'entrainer à gérer des situations de crise ensemble est aussi un moyen de comprendre et prévoir les mesures de prévention, de protection et de récupération. Dans le cadre de la mise en place d'un système de management de la sécurité, la revue des risques et des incidents, le plan de traitement des risques et le plan d'audit communs sont des perspectives d'amélioration continue pour garantir un niveau de risque maîtrisé. Cette démarche permettant ainsi d'amener à une politique de sécurité du système d'information transversale.

Références bibliographiques

[1] Guides de la méthode EBIOS : ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), www.ssi.gouv.fr

[2] JRES 2009 (Journées réseaux des Universités) : TOURRON P., GRALL M., Article publié dans les actes du congrès : Utilisation de la méthode EBIOS : de l'organisation projet aux composants du SMSI (Système de Management de la Sécurité de l'Information), JRES, 2009