HealthManagement
Promoting Management and Leadership

Volume 5 - Numéro 1, 2012 - Dossier : La Gestion Des Risques

La Sécurité Des Systèmes d'Information De Santé

Auteur

Mylène Jarossay

Directrice adjointe des systems d'information et RSSI

Institut Curie

Paris, France

mylene.jarossay@curie.net

Les risques sur les systèmes d'information (SI) de santé sont identifiés depuis quelques années, c'est-à-dire depuis que les établissements ont largement informatisé leur processus de soins et que se sont développés des dispositifs biomédicaux embarquant des systèmes informatiques complexes.

Les Enjeux

La protection de l'information médicale et des systèmes et réseaux informatiques qui l'hébergent et la transportent répond à plusieurs exigences. Il s'agit tout d'abord de garantir une continuité et une sécurité des soins. La dépendance visà- vis de l'informatique est telle qu'un incident informatique peut avoir des conséquences lourdes, depuis la désorganisation ou la perte d'activité jusqu'à des risques vitaux pour les patients. La sécurité de l'information répond également à un besoin de confidentialité et de respect du secret. Il en va de la protection de la vie privée des patients et de la confiance qu'ils placent dans la structure de santé qui les prend en charge. Ces deux grands domaines, la disponibilité et la confidentialité, font l'objet d'un réglementaire complexe, en pleine évolution, et qui place très haut le niveau d'exigence sur la sécurité des systèmes d'information de santé.

Si l'information de santé est critique dans les processus de prise en charge des patients, elle possède aussi une valeur dans le cadre d'activités de recherche. La production de dossiers médicaux électroniques consolide des textes, images ou données structurées des résultats issus d'appareils biomédicaux pour constituer un véritable patrimoine immatériel. Contrairement aux dossiers papiers ou films, ces ensembles d'information sont facilement exploitables et interrogeables. Ce patrimoine doit être protégé contre l'intrusion, le vol, la destruction ou la fuite d'information.

La Démarche Sécurité

Pour répondre à ces différents enjeux, une organisation doit être mise en place, dont l'objectif est de définir et de mettre en oeuvre une politique de sécurité des systèmes d'information. La démarche sécurité s'appuie sur des analyses de risqué qui identifient les vulnérabilités des SI, les évènements redoutés (ou menaces), leur impact potentiel sur les métiers et leur probabilité d'occurrence, pour en déduire une liste de risques évalués selon une échelle de criticité. Pour chaque risque une stratégie de traitement doit être déterminée. L'ensemble des risques et leurs traitements consolidés constitue un « plan de traitement des risques ».

La mise en oeuvre du plan, son contrôle et son adaptation éventuelle s'inscrivent naturellement dans une logique d'amélioration continue de la sécurité. Comme dans les approaches qualité, la sécurité des systèmes d'information se construit à travers un « Système de Management de la Sécurité de l'Information » (SMSI) et suit un modèle PDCA (Plan Do Check Act)*, conformément aux recommandations de la norme ISO 27001. Le RSSI (Responsable de la Sécurité du Système d'Information) est un expert de risques. Il assure une veille active dans son domaine d'expertise qui est extrêmement évolutif. Sa mission est de définir et coordonner les diverses actions sécurité, qu'elles soient techniques ou concernent l'éducation, la communication, les évolutions organisationnelles ou encore les actions juridiques et contractuelles. Ces mesures doivent être auditées, évaluées et améliorées.

Les Mesures Techniques Et Organisationnelles

Les mesures techniques sont généralement mises en oeuvre par les DSI (Directions des Systèmes d'Information). Elles portent par exemple sur la sécurisation des réseaux, via l'authentification des terminaux qui s'y connectent ou encore le découpage des réseaux en différents sous-réseaux logiques cloisonnés qui permet d'éviter les contaminations ou attaques massives et de protéger les serveurs. Ce cloisonnement est important, notamment pour pallier une sécurité souvent faible des dispositifs biomédicaux, vecteurs connus de contaminations des réseaux dans les hôpitaux. La protection des systems informatiques suppose également la sécurisation des systèmes d'exploitation des postes de travail, le deployment régulier de correctifs de sécurité, l'installation de logiciels antimalwares, des développements applicatifs sécurisés, la separation des environnements de tests des plates-formes de production, le chiffrement des terminaux mobiles, des messageries, des flux, des fichiers et bases de données sensibles.

La mise en oeuvre d'un système de gestion des identités est également essentielle pour sécuriser l'accès logique à l'information. Il s'agit de spécifier, avec l'aide des DRH, qui peut se connecter, avec quel compte informatique, quel est son rôle dans l'organisation et qui a le droit de faire quoi sur tel système ou telle application. Il faut une gestion des entrées et sorties de personnels qui déclenche des ouvertures et fermetures de comptes, une gestion des habilitations appuyée sur les métiers et services des personnes mais aussi une politique d'authentification qui s'appuie soit sur l'usage de mots de passe robustes, soit sur des dispositifs d'authentification forte par une carte professionnelle ou un autre dispositif. Toutes ces mesures techniques doivent être régulièrement éprouvées grâce à des audits et tests d'intrusion qui permettent de vérifier leur solidité.

En matière de disponibilité du SI, il faut élaborer des Plans de Continuité d'Activité (PCA) et des Plans de Reprise d'Activité (PRA) pour garantir un fonctionnement continu et être en capacité de réagir en cas de crise. Cela implique une redondance des salles et serveurs informatiques, et des mécanismes de basculement des systèmes nominaux sur les systems de secours. Dans des modes de secours qui peuvent être « dégradés », il faut définir avec les professionnels de santé la façon de maintenir une activité quand les systems informatiques ne sont que partiellement opérationnels. Ces plans doivent être définis a priori, car il n'est pas toujours facile ni même faisable d'élaborer une stratégie de secours lorsque le sinistre survient.

L'Approche Juridique

L'aspect juridique et contractuel concerne d'abord les usagers habituels du SI pour lesquels il faut, par exemple, élaborer des chartes sécurité ou prévoir des clauses sécurité dans les contrats de travail. Il concerne aussi les tiers, et principalement les fournisseurs des progiciels métiers et des équipements biomédicaux. Des exigences sécurité doivent être intégrées dans les cahiers des charges. Elles se retrouvent dans les contrats d'acquisition, puis dans les contrats de maintenance. Il est important de bien fixer les responsabilités du fournisseur, ce qu'il a le droit de faire sur le système qu'il maintient, la traçabilité de ses accès et l'engagement sur les délais de remise en condition opérationnelle en cas d'incident. La prise en compte des tiers sur le plan juridique concerne enfin les clauses de confidentialité et de propriété pour les stagiaires, thésards et autres étudiants qui interviennent sur le SI, ainsi que des contrats avec des prestataires usagers réguliers du SI.

Le Facteur Humain

La sécurité des SI repose très largement sur les comportements humains, qui constituent souvent le maillon faible de la chaîne de sécurisation. Les mesures techniques et juridiques sont des prérequis mais il est également essentiel que chaque professionnel comprenne les risques, et connaisse ses obligations et les bonnes pratiques à observer pour preserver le SI. Rappelons que l'essentiel des fuites et pertes d'information ne passe pas par des piratages mais par des accès légitimes au SI. Une sensibilisation à la sécurité est donc nécessaire pour l'ensemble des professionnels qui y ont accès. Elle peut s'intégrer dans une démarche coordonnée de formation sur les différents domaines de risques et vigilances réglementaires et notamment sur l'identito-vigilance, l'un des thèmes adressés par la sécurité des SI. Il ne s'agit pas de proposer un enseignement technique sur la sécurité, complexe à mettre en place et vite obsolète, l'évolution technologique étant très rapide. L'objectif est plutôt de faire comprendre quelques principes de base.

D'abord, les utilisateurs doivent réaliser que les incidents de sécurité peuvent profondément affecter leur métier. Qu'il s'agisse d'accidents (panne, sinistre), d'erreurs humaines (fausse manipulation, bug) ou de malveillances, le nombre d'incidents de sécurité est en très forte augmentation. Ce n'est pas un mythe, la quantité d'attaques véhiculées par Internet explose ! Les attaques sont désormais orchestrées par des mafias organisées, et les hôpitaux ne sont pas épargnés par le phishing, les spams, vers, botnets, et autres fraudes.

Les utilisateurs doivent aussi être sensibilisés à la notion de secret. Ils doivent être vigilants sur toute communication d'information, vers les patients ou d'autres professionnels de santé, en face-à-face, par téléphone ou par email. Ils doivent se soucier d'authentifier leur interlocuteur et de vérifier la légitimité des demandes. L'incitation à la discrétion concerne le temps passé au travail mais aussi la vie personnelle. La frontier est de plus en plus floue entre les deux mondes. Les réseaux sociaux contiennent de nombreuses informations qui témoignent de ce mélange entre vie privée et vie professionnelle. La notion de secret médical est ancienne et bien connue des professionnels, mais elle doit être aujourd'hui decline dans un monde numérique hyper-communiquant afin d'éviter les disséminations et fuites d'information.

Sur un plan plus pratique, il faut que les utilisateurs aient le réflexe de ne jamais cliquer sur des liens contenus dans des emails reçus, ni envoyer de données médicales sur des messageries en clair sur Internet, ni stocker des données médicales sur des postes personnels et de toujours privilégier le stockage sur des serveurs de fichiers professionnels sécurisés et sauvegardés. Ils doivent utiliser des comptes personnels ; leurs actions dans les applications sont traces et leur sont imputables à travers le compte utilisé. Les mots de passe doivent être complexes, jamais communiqués et changés régulièrement. La session sur un poste de travail doit être fermée ou, a minima, verrouillée quand on quitte son

poste. Les médias amovibles, exposés aux malwares, doivent être utilisés uniquement sur des postes sécurisés. Il faut également rappeler à chaque professionnel les exigencies de la loi « Informatique & Libertés » et veiller à declarer tout traitement de données directement ou indirectement nominatives. Ces quelques grandes règles sont à compléter dans chaque contexte, en fonction des équipements et applications en place, mais aussi de l'organisation.

Les Spécificités Des Systèmes d' Information De Santé

En milieu hospitalier, les systèmes informatiques sont particulièrement exposés : les établissements de santé sont des milieu physiquement ouverts au public, les professionnels de santé sont itinérants dans et hors des structures, les equips de soins se partagent des SI avec des responsabilités parfois mal définies sur l'information dématérialisée et manipulent des volumes considérables d'information, notamment dans le domaine de l'imagerie et les SI des hôpitaux sont de plus en plus ouverts vers des partenaires extérieurs. De plus, le niveau d'exigence sécurité sur le plan réglementaire est très élevé. Dans un tel contexte, la sécurité des SI de santé est complexe à définir et à mettre en oeuvre et nécessite l'implication forte de tous les métiers de l'établissement.

Published on : Sat, 30 Apr 2005