Numéro 14
Juin 2010

Octet

La lettre d'information du SIIH

Édito

Sécurité : la gestion des risques intégre le SIH !

Nous sommes entrés de plein fouet dans l'ère de la sécurité des données médicales. Les enjeux sont nombreux et correspondent à une amélioration constante de la prise en charge des patients.

Les lois de 2002, 2004 et 2009 ont défini un cadre pour l'exercice de cette sécurité des systèmes d'information (SI) de santé. Ces textes nous indiquent que la prise en charge par les directions d'établissements de la gestion des risques liés aux SI doit être une préoccupation de premier ordre.

Un moyen simple consiste à intégrer la gouvernance de la sécurité des systèmes d'informations hospitaliers (SIH) dans celle de la gestion des risques, combinée à un processus d'amélioration permanente du niveau de sécurité. Certaines orientations sont encore attendues des services de l'Etat pour préciser les modalités de mise en oeuvre. Mais dès à présent, une méthodologie adaptée aux risques SIH permet aux établissements de déterminer les menaces et les vulnérabilités auxquelles ils doivent faire face. Il sera alors plus facile de mettre en place des plans d'actions. Le RSSI (Responsable de la Sécurité du Système d'Informations), avec son positionnement stratégique, anime cette réflexion et assure le suivi du plan d'actions.

C'est dans ce contexte qu'en 2008, 27 établissements de la région Nord-Pas-de-Calais se sont regroupés dans un projet mutualisé pour se mettre en conformité avec le décret "confidentialité". L'assistance à maitrise d'ouvrage a été confiée au SIIH. Deux projets, financés par le plan hôpital 2012, ont été lancés : le premier sur la définition et la mise en oeuvre d'une politique de sécurité du SI dans l'établissement ; le deuxième sur la mise en oeuvre d'un système de contrôle des accès avec une authentification forte.

Pour aider les établissements de santé, le SIIH étudie actuellement un ensemble de services dans la mise en oeuvre et le suivi de leur politique de sécurité. Par ailleurs, le syndicat accueille le club sécurité régional, dont la première réunion a eu lieu le 22 avril. Nous apporterons notre contribution à son animation. La sécurité sera un des thèmes majeurs de cette année 2010. Soyez assurés que le SIIH et ses équipes seront à vos côtés pour répondre au mieux à vos besoins.

Luc Vaurette
Directeur opérationnel RSSI et prospective

Le point de vue « sécurité » de ...

Guillaume DERAEDT

Responsable de la Sécurité du Système d'Information (RSSI), Correspondant Informatique et Liberté au CHRU de Lille, et Trophée Jeune RSSI 2010 du magazine 01 Informatique Business et Technologies.

Présent lors de la journée sécurité organisée par le SIIH, Guillaume Deraedt, témoigne sur deux des projets sécurités menés au CHRU de Lille : la sécurité des équipements biomédicaux et les cartes d'authentification et de contrôle des accès.

Octet : Vous avez travaillé sur la sécurité des équipements biomédicaux, pourquoi s'être intéressé à ce sujet au CHRU de Lille ?

G. Deraedt : *« De nombreux établissement ont rencontré, au niveau de ces équipements, des problèmes de virus informatiques. La Fédération Hospitalière de France, à travers Le Conseil National des DSI des CHU, m'a mandaté pour animer un groupe de travail afin de mettre au point un document de politique de sécurité pour les équipements biomédicaux...*

Lire la suite page 2

Dossier

Le 22 avril dernier, le SIIH organisait une rencontre autour de la sécurité des systèmes d'informations hospitaliers. Une thématique d'actualité qui fait écho à l'application du décret confidentialité. Étaient présents 25 établissements de la région, qui participent à trois projets phares pilotés par le SIIH : la mise en place des politiques de sécurité ; les moyens d'authentification et de contrôle d'accès ; la création d'un « club sécurité ». Octet revient sur les avancées réalisées dans ces domaines.

Le point de vue « sécurité » de ...

Guillaume DERAEDT

G. Deraedt : *...Après une analyse des risques, nous nous sommes rendu compte qu'il y avait deux sources d'infections principales : l'une depuis les dispositifs médicaux eux-mêmes (scanner, échographe...), l'autre via les mémoires de masse amovibles type def USB. Il devenait primordial de sécuriser les failles de sécurité utilisées par ces vecteurs. Voilà pourquoi des spécialistes de la sécurité ont travaillé à l'élaboration d'un outil simple, en l'occurrence un guide d'une vingtaine de pages, mis à la disposition des Etablissements de Santé. Ce document fait le point sur l'analyse des risques autour de ces équipements et propose une grille d'évaluation des fournisseurs en une centaine de points. »*

Octet : Dans cette démarche, quel rôle joue le SIIH ?

G. Deraedt : *« Le SIIH est un intermédiaire essentiel à la diffusion régionale de ce guide. Il est capital de sensibiliser et de légitimer les personnes en charge de la sécurité dans les établissements en leur donnant les outils adéquats. Le syndicat est une structure bénéfique pour la région, parce qu'il est capable de faire le lien entre les spécialistes de la sécurité et les DSI locaux. »*

Octet : Vous avez été récompensé au Trophée du jeune RSSI, notamment grâce au projet d'authentification et de contrôle des accès mené au CHRU de Lille, votre réaction ?

G. Deraedt : *« Le projet sécurité lié à l'authentification des personnes et au contrôle des accès a été mené efficacement. Nous avons distribué 13 000 cartes d'accès multi-usages (parking, cantine, poste de travail...) lié à un compte informatique nominatif à valeur probante sur un an. Le SIIH, qui avait en charge la mise en oeuvre de ce projet, a fait preuve d'une bonne compréhension de nos besoins. Ses compétences techniques et son expertise ont facilité le bon déploiement des opérations. Je tiens donc à associer l'équipe projet du SIIH à ma victoire au Trophée du jeune RSSI. Je remercie également Luc Vaurette, pour les préceptes qu'il m'a aimablement transmis lors de ma prise de fonction. »*

Journée Régionale sur les projets sécurité au SIIH

Sécurité, qua nous tiens !

Projet 1

Mise en place des politiques de sécurité

Motivation optimum des établissements

Après un an d'analyse des politiques de sécurité, menée en collaboration avec le SIIH par les centres hospitaliers participant au projet, les résultats apparaissent plutôt encourageants. Les établissements ont participé activement à l'état des lieux. Ce dernier a révélé un niveau de maturité de sécurité globalement faible, mais tout a fait logique puisque la démarche ne fait que commencer. Par ailleurs certains domaines, comme par exemple l'exploitation informatique ou le contrôle d'accès aux applications, sont particulièrement bien sécurisés. Les établissements se donnent deux ans pour couvrir l'ensemble des points de vigilance et dérouler leur plan d'actions. Pour répondre aux nombreuses attentes apparues suite à cette analyse, le SIIH continue l'accompagnement des établissements qui le souhaitent dans la mise en place de leur politique de sécurité (formation, mutualisation des projets, maîtrise d'ouvrage...).

Contact : Luc Vaurette / luc.vaurette@siih5962.fr

Objectifs du projet

- Définir un plan d'actions concret et adapté à chaque établissement.
- Intégrer la gestion des risques des systèmes d'informations dans la gestion globale des risques.
- Atteindre un niveau de maturité de la sécurité des systèmes d'informations en partant du niveau de sécurité existant.
- Placer chaque établissement dans une démarche d'amélioration continue du niveau de sécurité.

and tu

84%

des établissements participants au projet ont intégré la gestion des risques des systèmes d'informations à leur démarche globale de gestion des risques.

57%

des établissements participants au projet ont signé leur PGSSI (Politique Générale de Sécurité des Systèmes d'Informations).

Projet 2

Authentification et contrôle des accès

Bientôt tous identifiés !

Le projet d'authenfication et de contrôle des accès des personnes accédant aux données médicales est aujourd'hui une question centrale dans les politiques de sécurité. Ce projet se décompose en cinq chantiers : la gestion des identités (annuaire des personnes), des habilitations, des accès, des moyens d'authentifcation et enfin la gestion de la traçabilité. Un dialogue compétitif a été lancé par le SIIH pour répondre à l'ensemble de ces problématiques. Trois candidats ont été retenus. Le gagnant sera connu à l'automne, pour un déploiement en 2011/2012. À n'en pas douter, ce projet d'envergure entraînera une véritable évolution des processus d'organisation dans les centres hospitaliers.

Contact : Luc Vaurette / luc.vaurette@siih5962.fr

Projet 3

Club sécurité régional

Devenez membre !

Dans la continuité du projet sur les politiques de sécurité, les établissements ont fait part de leur envie de concevoir une structure spécifique pour échanger sur les problématiques sécurité. L'idée du « club » était né ! Le SIIH, en tant que structure de mutualisation, pourra si les membres le souhaitent, gérer l'animation du club et apporter son expertise. Une première réunion a d'ores et déjà eu lieu. Tous les établissements de la région sont d'ailleurs invités à le rejoindre. N'hésitez plus. Prenez votre carte de membre !

Contact : Luc Vaurette
luc.vaurette@siih5962.fr

« Un club voulu par les établissements pour les établissements.»

Zoom sur

« 25 établissements accompagnés par le SIIH élaborent leur politique de gestion des risques SI »

En visite au SIIH pour la journée de rencontres sur la sécurité des systèmes d'informations, Claire Lenain, chargée de mission au Pôle territoires à l'ASIP Santé (Agence des Systèmes d'Information Partagées de Santé), nous a accordé une interview. Retour avec elle sur les projets sécurité menés par le SIIH et les 25 établissements régionaux.

Octet : Que pensez-vous de la mutualisation sur la région de projets liés à la sécurité des systèmes d'informations ?

Claire Lenain : *« L'ASIP Santé a pour mission de favoriser le développement des usages en e-santé dans le respect d'un cadre de confiance établi entre tous les acteurs du monde de la santé, patients et professionnels. La démarche entreprise par les 25 établissements de la région Nord-Pas-de-Calais et le SIIH est intéressante parce qu'elle contribue à la mise en oeuvre de cet espace de confiance, pour lequel nous sommes tous mobilisés. Faire en sorte que, dans les hôpitaux et les cliniques, se mettent en place une gouvernance de la sécurité des systèmes d'informations, une politique de sécurité et un plan d'actions continu… c'est favoriser un terreau indispensable pour le développement des systèmes d'information partagés (DMP, télémédecine…). »*

Octet : En quoi les démarches entreprises par l'ASIP Santé au niveau national, notamment la création d'une PGSSI (Politique Générale de Sécurité des Systèmes d'Informations), et celle menée par le SIIH et les 25 établissements sont-elles en adéquation ?

Claire Lenain : *« L'ASIP Santé est chargée de définir et de publier les référentiels d'interopérabilité et de sécurité sur le secteur santé et médico-social. A ce titre, l'ASIP Santé publiera prochainement une PGSSI qui devra s'appliquer à l'ensemble des projets de e-santé. Les 25 établissements fédérés par SIIH ont déjà évalué leurs risques, rédigé leur politique de sécurité ; ils sont en train de mettre en oeuvre les actions correctives et inscrivent la sécurité dans tous leurs projets de SI. C'est un vrai acquis, et une expérience qui peut intéresser les établissements d'autres régions. Il conviendra ultérieurement de s'assurer que leur politique de sécurité interne est en adéquation avec la PGSSI, notamment pour ce qui concerne les échanges et le partage d'informations avec l'extérieur. »*

Octet : L'ASIP Santé dans ces discours parle d'une certaine souplesse sur les moyens d'authentification, qu'en est-il ?

Claire Lenain : *« Dans le cadre des travaux menés en concertation sur la PGSSI, l'ASIP Santé établira des préconisations sur les niveaux de sécurité à atteindre pour les systèmes d'informations partagés et des consignes plus précises en matière d'authentification (cible et trajectoire). En attendant, les établissements ne doivent pas hésiter à continuer leur démarche visant à inscrire la sécurité dans leur gestion des risques, identifier de manière nominative toute personne qui accède au système d'information, améliorer la gestion des droits et tracer les accès. Par ailleurs, l'ASIP Santé prévoit de diffuser à partir de cet automne une nouvelle version de la carte de professionnel de santé (CPS3) qui permet un usage en « sans contact » pour les établissements qui en font la demande. »*

***Directeur de la publication** : Jean-Louis Fruit - **Rédaction et réalisation** : 3e AILE*
SIIH 59/62 : 255 rue Nelson Mandela - 59120 Loos
www.siih5962.fr - Email : siih@siih5962.fr - Tél. : 03 28 55 67 00