Le Mans, 4 au 6 décembre 2012

24 heures de débats, d'échanges et de convivialité

© Ville du Gilles Mousse

2e congrès national

Sécurité des Systèmes d'Information de Santé

Agir pour bâtir une sécurité durable des SI de santé

LIVRET SCIENTIFIQUE DU CONGRÈS

Le Mans Une Marque

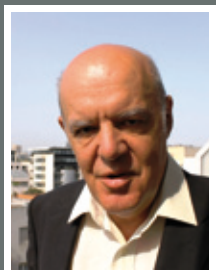
Le Mans Métropole Communauté urbaine

LE MANS DEVELOPPEMENT

LE MAGAZINE DES SYSTÈMES D'INFORMATION HOSPITALIERS DSiH

Congrès national de la Sécurité des Systèmes d'Information de Santé

SOMMAIRE



Monsieur Gérard PELIKS
EADS CASSIDIAN
Président de l'Atelier Sécurité – Forum ATENA

Panorama international de la cybercriminalité et du cyber terrorisme

Gérard Peliks est expert sécurité dans le Cassidian Cybersecurity (groupe EADS). Il travaille depuis plus de 15 ans dans le domaine de la sécurité de l'information et depuis plus de 30 ans dans l'informatique. Il préside l'atelier sécurité de l'association Forum Atena, dans lequel il organise de grands évènements autour de sujets techniques sur le futur de l'Internet et coordonne l'écriture de livres collectifs sur la sécurité de l'information. Il est membre du conseil d'administration de l'association des réservistes du chiffre et de la sécurité de l'information et participe au groupe sécurité de l'AFNOR.
Gérard Peliks est chargé de cours sur différentes facettes de la sécurité, dans le cadre de l'Institut Télécom.

Résumé de l'intervention
Vous, moi, le monde de la santé, baignons dans le cyberespace. De l'information sur les posologies aux blocs opératoires, du dossier médical à la clé USB, du stimulateur cardiaque à l'alimentation en énergie des hôpitaux, le cyberespace recouvre tout. Ne pas être connecté à l'Internet n'est pas un moyen suffisant pour lui échapper.
Le cyberespace est-il sûr ? Pouvez-vous lui accorder une confiance sans limites indispensable dans le monde de la santé ? La réponse est hélas : Non. Il est donc nécessaire de prendre des précautions suffisantes pour sécuriser non seulement les données personnelles des patients mais aussi le fonctionnement des appareils médicaux. La sécurité et la sûreté sont encore trop souvent absentes aujourd'hui du monde de la santé qui fait pourtant si étroitement partie du cyberespace rempli de menaces et d'attaques avérées.
Nous définirons ce qui constitue le cyberespace, modèle en trois couches (couche physique, couche logique, couche sémantique) pour mieux appréhender sa réalité qui est loin d'être celle d'un nuage, d'un espace virtuel et du seul Web. Nous dresserons ensuite un panorama de quelques attaques lancées sur le cyberespace, entre autres :

- L'attaque en déni de service distribué, par des cyberhackers, appuyée par des Botnets, qui a causé une perturbation massive en Estonie en 2007.
- La propagation du ver Confiker en 2008, toujours présent en 2012, qui a fortement inquiété le monde de la défense, de la finance... et celui de la santé.
- L'attaque sur les centrifugeuses d'enrichissement d'uranium de l'usine de Natanz, en Iran en 2010, par des cyberguerriers, qui illustre comment une attaque sur les infrastructures vitales d'un pays peut menacer sa souveraineté.
- L'attaque contre le Ministère de l'Industrie et des Finances, par des cyberespions, en 2011, pour subtiliser l'information intéressant le G20, par des APT (Advanced Persistant Threats).
- Le vol des informations personnelles non chiffrées de 100 millions de clients de Sony, en 2011, par des cybercriminels, grâce à des certificats subtilisés qui remettent en cause les bases de l'économie numérique.
- Des assauts des Anonymous au virus Gauss en 2012, nous verrons aussi les attaques les plus modernes qui dérobent des informations sensibles afin de les monnayer et faire fructifier ses gains dans les marchés noirs de la cybercriminalité et de la monnaie virtuelle.
- Et bien sûr si une nouvelle attaque se révèle avant le congrès, il en sera aussi question.

Si les infrastructures et les informations sensibles du monde de la santé ont été pour l'instant « relativement » épargnées, le type des attaques évoquées peut se retourner contre lui dans les mois qui viennent à des fins de chantage ou pour créer une panique généralisée à l'échelle du pays. Des contre-mesures existent pour diminuer les risques jusqu'à un niveau accepté, les interventions suivantes les évoqueront.

Monsieur Philippe LOUDENOT
FSSI auprès du Premier Ministre

Je suis connecté. C'est grave Docteur ?

Philippe Loudenot est le fonctionnaire de sécurité des systèmes d'information (FSSI) rattaché au haut fonctionnaire de défense et de sécurité auprès du Premier ministre. Ancien responsable national de la sécurité des systèmes d'information du service de santé des armées, puis FSSI adjoint pour les ministères chargés des affaires sociales, il dispose d'une connaissance approfondie du monde de la santé. Ancien auditeur de l'institut des hautes études de la défense nationale, Philippe est également certifié ISO 27001 Lead Auditor.
Il est chargé de cours SSI au profit de différentes universités et écoles d'Ingénieurs.
Il est membre du conseil d'administration de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information.

Résumé de l'intervention
830 volts ! ... houlà ça pique ! est-ce grave docteur ?
C'est pourtant ce qui a été envoyé à un pacemaker en octobre 2012 lors d'une démonstration au cours d'un congrès à Melbourne, ce qui, s'il avait été porté par un être humain aurait provoqué une crise cardiaque. Systèmes d'information de santé, appareils biomédicaux, ils sont de plus en plus communiquant mais leur sécurité est-elle prise suffisamment au sérieux ?

Monsieur Yves NORMAND

RSSI et CIL du SIB

Monsieur Olivier CAZALS

Responsable département Services et Sécurité du MIPIH

De la valorisation de la sécurité dans les processus métiers des Etablissements de Santé

Yves Normand est Responsable de la Sécurité des Systèmes d'Information (RSSI) et Correspondant Informatique & Libertés (CIL) au sein du Syndicat Interhospitalier de Bretagne (S.I.B).
Il intervient, depuis le début de sa carrière professionnelle, dans le domaine de la sécurité de l'information. Il a été Directeur Technique et Directeur Général d'une structure éditrice de solutions de sécurité (SSO, chiffrement de données,...), pour le compte de banques, d'assurances et d'industriels.
Puis, il a été consultant en SSI et chargé d'affaires, sur l'aspect organisationnel de la SSI (audit, analyse des risques, PSSI,...), pour le bénéfice de banques, ministères, DCSSI, collectivités territoriales. Fort de la diversité de ses expériences, de son expertise méthodologique (EBIOS, normes ISO27000,...), de son écoute, Yves Normand intervient aujourd'hui pour les établissements de santé adhérents du SIB.
Yves Normand, ingénieur UTC, est certifié « Lead Auditor ISO/IEC 27001:2005 » et « Risk Manager ISO/CEI 27005:2008 ». Il est membre de l'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personnel) - groupe de travail « Données de santé », et membre fondateur du groupe de travail « sécurité » de l'Asinhpa (association des structures d'informatique hospitalière publique autonomes).

Olivier Cazals est responsable du département « Services et Sécurité » au Mipih (Midi Picardie Informatique Hospitalière), depuis 2011. Ce département a notamment pour mission la mise en œuvre de produits de sécurité (SSO, IAM,...) dans les établissements de santé.
Des missions d'audit et de sensibilisation à la sécurité sont également réalisées.

Olivier a été pendant 10 ans ingénieur d'affaires chez Ilex, éditeur de logiciel spécialisé sur les problématiques de sécurité et de gestion des identités.
Actuellement, plusieurs dizaines d'établissements de santé, adhérents du Mipih, ont bénéficié des produits et conseils du département « Services et sécurité ».
Olivier est membre du groupe de travail « sécurité » de l'Asinhpa.

Résumé de l'intervention

Sécuriser l'information de l'hôpital pour mieux soigner les patients est une des ambitions du programme Hôpital Numérique. Il s'agit de :

- Pouvoir à tout moment disposer de l'information,
- Garantir aux personnels soignants et administratifs une information fiable
- Protéger la confidentialité des informations confiées par le patient à l'établissement de soin

L'identification et la prise en compte des risques liés à la sécurité de cette information doivent s'intégrer dans une démarche globale de management et de réduction des risques.

L'Asinhpa (Association des structures d'informatique hospitalière publique autonomes), au travers de son groupe sécurité (regroupant CPage, MIPIH, SIB, SIIH, SIL) illustrera dans le cadre d'un processus métier une démarche de sécurité de l'information dans un établissement de santé. L'EPSM du Morbihan (Saint Avé) et le Centre hospitalier d'Argenteuil apporteront leur témoignage.

Monsieur Ben KOKX
Healthcare Product Security Director - PHILIPS

Security and privacy for medical devices

Traduction simultanée

The security and privacy landscapes are continuously changing, requiring an increasing and joined effort from both Healthcare providers and manufacturers across the globe.
Ben Kokx, joined Philips in 2001 as member of the software development team for x-ray equipment where he became responsible for the product security features of the system. He was a member of the Philips Healthcare global product security team from the start of the program. In the following years his role as Product Security Officer was extended with the role of Privacy Officer, responsible for the processes within the Interventional X-Ray business unit. In 2010 Ben moved to the Global Sales and Service International organization where he has regional responsibilities which also allowed him to work closer with customers. In 2012 Ben became the acting Director of Product Security with the responsibility of the overarching product security program within Philips Healthcare.

Résumé de l'intervention
Almost ten years ago Philips started a program to ensure that security and privacy requirements are embedded in the design of our products and services. In this presentation I will provide a brief overview of how Philips established a security governance model.
We have come a long way, and with the rapid, ever changing threat landscape the maintenance of this governance model will be an ongoing effort.
It also has become clear that we need a change in the relation between the health care providers and the equipment manufacturers. Security is not a battle between them, security is about together fighting the bad guys engaged in criminal activities who can impact the safe, effective and secure operation of medical devices. Risk management, that requires the joint effort of all parties, is the way forward. The new ISO/IEC 80001 standard, "Application of risk management for IT-networks incorporating medical devices", can be the method that supports this.

Maître Omar YAHIA

Avocat au Barreau de Paris

Diplômé du CAPA en 2005, responsable des affaires juridiques en hôpital public puis en polyclinique, Maître Omar YAHIA a intégré le Barreau de Paris en qualité d'avocat off counsel au sein du Cabinet DRAI ASSOCIES, puis en tant qu'associé au sein du cabinet SAINT-MARC Avocats.

Auteur (DSIH, Santé RH, Finances Hospitalières, DH Magazine, Thema Radiologie) formateur (COMUNDI, Entreprises Médicales), créateur d'un blog (HOSPIDROIT), Maître Omar YAHIA accompagne, conseille et défend les professionnels de santé, les établissements de santé et les industriels dans de nombreux domaines du droit de la santé (ressources humaines, contrôles T2A, télémédecine, coopérations hospitalières, etc.).

Résumé de l'intervention

Application technique de l'e-santé (ou télésanté), la télémédecine, sous l'égide de la DGOS, de l'ASIP Santé et des ARS, est en cours de déploiement sur tout le territoire national. Le schéma opérationnel retenu dans les régions correspond :

• sur le plan organisationnel, à la création d'un GCS régional e-santé, et, le cas échéant, à l'élaboration, pour chaque discipline, d'un outil de coopération, soit conventionnel, soit organique ;

• sur le plan matériel, à l'établissement d'une convention exposant les modalités d'organisation et de fonctionnement de la télémédecine, et d'un contrat particulier entre l'ARS et soit la personne physique, soit la personne morale concourant à l'activité.

A un rappel des outils de coopération conventionnels et organiques existants succèderont les questions relatives à l'impact de la télémédecine sur les droits des patients et sur la responsabilité des tiers technologiques.

Maître Jean-François FORGERON

Avocat au Barreau de Paris

Avocat à la Cour, Maître Jean-François Forgeron a débuté sa carrière en 1986 en pratiquant immédiatement le droit de l'informatique et des nouvelles technologies. Il a rejoint Alain Bensoussan Avocats en 1990.

Il y a assuré notamment le développement des activités relatives au droit de la santé électronique. Aujourd'hui Directeur du Pôle Informatique & Droit du cabinet, il encadre également le Département Santé électronique du Cabinet Alain Bensoussan dirigé par Maître Marguerite Brac de La Perrière.

Il intervient en conseil et en contentieux, auprès de clients publics et privés, en droit de l'informatique et en droit de la santé en particulier dans les domaines suivants :

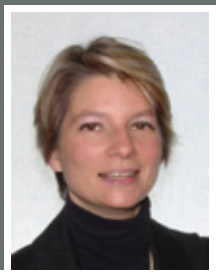
- Systèmes d'information hospitaliers (SIH)
- traitements et hébergement de données de santé à caractère personnel
- recherches dans le domaine de la santé
- télémédecine (contrats, responsabilité des acteurs)
- qualification, distribution de logiciels / dispositifs médicaux
- communications / publicités en ligne de produits de santé
- sites web santé

Résumé de l'intervention

Le partage de données de santé entre acteurs du système de soins, reconnu par tous comme contribuant à l'amélioration de la qualité des soins et à la maîtrise des dépenses, est un prérequis indispensable au développement de l'e-santé.

Dans ce contexte, la sécurité des données personnelles de santé est une priorité, largement encadrée, et plus récemment renforcée par la procédure d'agrément des hébergeurs de données de santé à caractère personnel qui vise à garantir la sécurité des données personnelles de santé hébergées par un organisme distinct du professionnel ou de l'établissement de santé ayant la charge médicale du patient.

Après une présentation du cadre légal des traitements de données de santé à caractère personnel, les textes, les référentiels et les pratiques applicables à ce traitement particulier qu'est l'hébergement de données seront donc détaillés.



Maître Emmanuelle PELETINGEAS

Avocat au Barreau de Paris

Diplômée de l'Université Paris X Nanterre en Droit Public de l'Entreprise et de l'Université de Paris V en Droit des Sciences Médicales, avocat au Barreau de Paris depuis 1998, Maître Emmanuelle PELETINGEAS est également Correspondante Informatique et Libertés.

Elle accompagne, depuis quinze ans, les créateurs d'entreprises et les dirigeants de sociétés, tant en droit des sociétés qu'en droit du travail. Elle assiste également les sociétés dans l'élaboration de documents tels que la charte informatique (utilisation des messageries, géolocalisation, vidéosurveillance, etc.), les contrats de sous-traitance et de maintenance des systèmes d'information (sécurité et confidentialité des données, responsabilité des parties).

Résumé de l'intervention

Les entreprises et les administrations recourent de manière croissante aux nouvelles technologies de l'information et de la communication pour gérer leurs ressources humaines. Si les possibilités techniques sont quasi-illimitées, le Droit encadre strictement leur usage aux fins de faire respecter l'intimité de la vie privée des salariés de l'entreprise et des agents de l'administration concernée.

Après un bref rappel des principes généraux gouvernant la mise en œuvre des traitements des données à caractère personnel, il y aura lieu d'évoquer les obligations mises à la charge de l'employeur par le code du travail, avant de dresser le panorama actuel des différents dispositifs de contrôle de l'activité des salariés (messagerie électronique, internet, vidéosurveillance, géolocalisation, etc.) à la lumière de la jurisprudence 2012.

Monsieur Philippe MAURY
Directeur régional - IMPRIVATA

Monsieur Dries SCHELFAUT
Expert SSI - IMPRIVATA

Les nouvelles technologies au service de la SSI

Philippe Maury est en charge du développement des activités d'Imprivata pour le territoire Europe du Sud.
M. Maury occupait auparavant le poste de responsable des activités SaaS de l'éditeur Websense pour les régions Europe du Sud et Moyen Orient. Avant cela, Mr Maury a occupé des postes à responsabilités pour différents éditeurs tels que Clearswift, Content Technologies, Hummingbird Communications.
M. Maury a commencé sa carrière en tant que développeur puis ensuite formateur sur les environnements C & C++ avant d'orienter son parcours vers des postes commerciaux & marketing. Mr Maury a plus de 15 ans d'expérience dans le secteur des nouvelles technologies.

Dries Schelfaut a commencé sa carrière professionnelle en l'an 2000 chez Skillteam – un filial d'IBM Belgique - en tant que développeur. Durant les années, il a pris des rôles de développeur junior, développeur senior, analyste technique et analyste fonctionnelle et chef de projet.
En 2010 il a quitté le monde de la consultance et il a rejoint l'équipe des ingénieurs avant-vente d'Imprivata en EMEA, le leader dans le domaine de la gestion d'authentification dans le secteur des soins de santé. Dans ce rôle Il supporte les partenaires dans la vente des technologies Imprivata, réalise des maquettes, donne des formations, répond aux appels d'offres, ... Il réalise également des implémentations Imprivata OneSign dans la région et il supporte les clients existants avec des questions sur leur installation existante.

Résumé de l'intervention
Imprivata est un éditeur de solutions de gestion d'authentification adressant principalement le secteur santé.
L'objectif de la présentation sera de parcourir un éventail de nouveaux concepts technologiques permettant d'améliorer le travail au quotidien des cliniciens.
La professionnalisation des équipements informatiques, leur déploiement chaque jour plus important dans la vie de l'hôpital doivent représenter une avancée pour les personnels de santé et non pas des contraintes supplémentaires ou une surcharge d'activité.
La présentation, axée sur plusieurs démonstrations, s'attachera à montrer comment faciliter et simplifier la relation entre les cliniciens et leur SIH.
En conclusion, Monsieur Sylvain Francois, DSI du CHU de Reims, viendra évoquer son retour d'expérience concernant la mise en œuvre d'une solution intégrant la gestion des identités et la gestion de l'authentification unique au sein du CHU de Reims.

Monsieur Vincent REGNAULT
Responsable du système d'information,
Correspondant Informatique et Libertés

Monsieur Philippe STOPPA
Vice-président FAIRWARNING

Protection de la vie privée des patients : témoignage du CH de Fécamp

Vincent Regnault est responsable du système d'information et correspondant Informatique et Libertés (CIL) du Centre Hospitalier Intercommunal du Pays des Hautes Falaises à Fécamp. Vincent est major de sa promotion de Master spécialisé 'Informatique et Libertés' à l'Institut Supérieur d'Electronique de Paris. Combinant une expérience de plus de 10 ans acquise en milieu hospitalier Vincent s'attache à protéger les données de santé à caractère personnel. Vincent a consacré plusieurs écrits et présentation en particulier au rôle du CIL au sein des établissements de santé.

Philippe Stoppa représente en Europe la société FairWarning, basée aux USA, qui apporte des solutions innovantes dédiées aux établissements de soins pour protéger la vie privée des patients en collectant les traces des accès aux applications cliniques et médicales. Précédemment Philippe Stoppa a développé les marchés de la santé pour un leader de la sécurité des systèmes d'information.

Résumé de l'intervention
Protection de la vie privée des patients - Témoignage du CH de Fécamp
Après avoir rappelé les aspects juridiques des données de santé à caractère personnel, les spécificités de la fonction du Correspondant Informatique et Libertés en établissement de santé seront abordées. Pour faire face aux contraintes sur les ressources liées à cette nouvelle fonction, la mutualisation de la fonction CIL au sein d'une Communauté Hospitalière de Territoire est une solution dont la mise en œuvre pratique sera discutée. Mais pour remplir sa fonction le CIL doit recourrir à des outils. Un de ceux-ci est la traçabilité des accès et des actions sur les applications métiers qui créent, enrichissent et manipulent les données sensibles

Monsieur Gilles TROUESSIN
Expert SSI – SCASSI Conseil

Des spécificités de la SSI en Santé

Après une thèse au CNRS (au LAAS – Laboratoire d'Analyse et d'Architecture des Systèmes) dans le domaine de la sûreté de fonctionnement et soutenue en 1991 sur le sujet du « traitement fiable de données confidentielles (par fragmentation-redondance-dissémination) », Gilles Trouessin a ensuite effectué un post-doc en 1992 à l'ONERA (au CERT – Centre d'Études et de Recherches de Toulouse) sur le sujet des « évaluations des propriétés de sécurité (par les théories de l'incertain) ».

Ensuite, jusqu'en 2001, il a travaillé comme ingénieur d'études-sécurité à la CNAMTS au CESSI – Centre d'Études des Sécurités du Système d'Information, l'équipe qui avait conçu et développé la méthode d'anonymisation et la fonction FOIN – Fonction d'Occultation d'Informations Nominatives ; période durant laquelle il a été membre et animateur de groupes d'experts en « sécurité des SIS » pour la normalisation en « informatique de santé » (« health informatics »), à l'AFNOR, au CEN, à l'ISO.

Puis, de 2001 à 2005, il a rejoint le cabinet d'audit ERNST&YOUNG comme auditeur / consultant en Sécurité des Systèmes d'Information de Santé (SIS) et des Systèmes d'Information Hospitaliers (SIH), période durant laquelle il a conduit le projet de recherche : « Modèles et Politiques de Sécurité des Systèmes d'Information et de Communication pour la sphère Santé/Social (MPSSICSS – MP6) ».

De 2005 à 2010, il a travaillé pour la Sté OPPIDA sud, comme consultant en sécurité des systèmes d'information de santé ; et s'est intéressé, à nouveau, à l'anonymisation et à la cohabitation entre les exigences de sécurité classiques incluant la confidentialité (ou confidentialité-discrétion) et les obligations de sécurité spécifiques incluant le respect de la vie privée (ou confidentialité-séclusion).

Depuis 2010, Gilles Trouessin a rejoint la Sté SCASSI Conseil, cabinet d'audit d'expertise et de conseil en sécurité de l'information où il est « responsable du département « sécurité des SIS / SIH » » ; il est toujours très impliqué dans la protection des données sensibles (de santé et/ou données à caractère personnel) ; en tant que adhérent et membre actif de l'AFCDP – Association Française des Correspondants à la protection des Données à caractère Personnel, il contribue au Groupe de Travail Thématique « données de santé » et anime le Groupe de Travail Régional – Sud-Ouest Pyrénéen.

Résumé de l'intervention
Voir page 12

Des spécificités de la SSI en Santé

Résumé de l'intervention

Après vingt-cinq années d'activités dans différents domaines de la « sûreté de fonctionnement » (ou « dependability » en anglais), l'intervention de Gilles Trouessin consistera à informer / sensibiliser et à débattre / controverser en préambule autour des différentes facettes de la sûreté de fonctionnement qui concernent aussi bien les Systèmes d'Information de Santé (en général) que (en particulier) les Systèmes d'Information Hospitaliers.

Toutes ces facettes, dites « attributs perceptifs », de la sûreté de fonctionnement sont fortement concernées par la confiance justifiée et/ou justifiable que l'on serait en droit de placer dans les services rendus par les SIS en général, les SIH en particulier et leurs fonctions-métiers primaires :

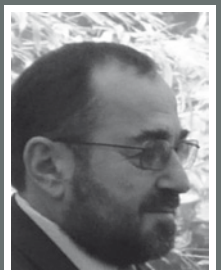
- sécurité-immunité ou « security » :
via disponibilité / intégrité / confidentialité / auditabilité du S.I.
- sécurité-innocuité ou « safety » :
éviter ainsi toute dérive vers une « informatique nosocomiale »
- liberté-intimité ou « privacy » :
respecter la vie privée et l'intimité (des données) de l'individu
- fiabilité ou « reliability » :
permettre aux systèmes de fonctionner sans risque de discontinuité
- maintenabilité ou « maintainability » :
rendre aisée les maintenances évolutives/correctives.

En particulier, une problématique centrale assez spécifique pour tous ces systèmes d'information contribuant à la prise en charge de la personne accueillie (malade, patient, convalescent, etc.) consiste à aborder de manière générale / généraliste mais aussi de façon plus spéciale / spécialiste la question de la Sécurité du Système d'Information (pour les SIS et/ou les SIH) dans un premier temps, et, dans un second temps, à traiter la complémentarité mais aussi la dualité voire l'antagonisme entre cette sécurité-security (ou sécurité-immunité) et cette sécurité-safety (ou sécurité-innocuité) ; autrement dit : « plus on sécurise (au sens de security) et moins on sécurise (au sens de safety) ».

Parallèlement, une problématique tout aussi centrale et tout aussi spécifique pour tous ces systèmes d'information liés à la prise en charge du soigné consiste à aborder de manière générale / généraliste mais aussi de façon plus spéciale / spécialiste la question de la Sécurité du Système d'Information dans un premier temps, et, dans un second temps, à traiter sa complémentarité mais aussi sa dualité voire son antagonisme avoir cette nécessaire liberté-intimité (ou séclusion-privacy) ; autrement dit : « plus on sécurise (au sens de security) et moins on respecte / rassure (au sens de privacy) ».

Finalement, quelques questions-clé sont à examiner :

- doit-on se contenter de PSSI standards pour protéger tous les S.I. de la sphère Santé / Social ?
- peut-on imposer aux SIS / SIH qu'ils soient équitablement respectueux des droits de l'usager ?
- veut-on exiger des SIS / SIH qu'ils soient sûrs de fonctionnement ? Pourquoi ? comment ?
- comment suggérer aux responsables de SIS / SIH : sécurité ET sûreté ET équité respectueuse ?



Monsieur
Lazaro PEJSACHOWUCZ
Président du CLUSIF

Héberger des données de santé : quels prérequis techniques et organisationnels ? Cloud et SaaS bientôt au Cœur du système

Très présent dans la vie associative des experts en Sécurité du Système d'Information, Lazaro Pejsachowicz est Président du Clusif (Club de la Sécurité des Systèmes d'Information Français).
Il est Responsable de la Sécurité du Système d'Information de la Direction Délégué aux Systèmes d'Information de la CNAMTS (Caisse Nationale d'Assurance Maladie des Travailleurs Salariés) poste qu'il a assumé en août 2002.

Il possède la certification PROCSSI et celle de « Lead Auditor ISO/IEC 27001 »

Il a été chargé du cours d'Administration de la Sécurité à l'Université de Tours.

Lazaro est diplômé de la Faculté des Sciences Exactes de l'Université de Buenos Aires (Argentine) où il a suivi des études en Mathématiques et Informatique Scientifique. Il a débuté comme enseignant dans plusieurs Universités argentines (Buenos Aires, Olavarria, Lujan, UTN). Il a été informaticien en Suisse (ONU, Gènève) puis en France, dans des grandes Sociétés de Service en Ingénierie Informatique (Cap Sesa, Sema Group) principalement dans le domaine des Systèmes d'Autorisation Bancaires.
Par la suite il a exercé pendant plus de dix années chez Bull SA en tant que Responsable de la Sécurité et des Evolutions du Système d'Information de Bull Infrastructure et Système, avant de rejoindre, en 2001, France Telecom e-business, filiale FT dédié à l'hébergement de sites en tant que Responsable Sécurité des plates-formes.
Il a intégré en août 2002 la Direction Systèmes d'Information de la Caisse Nationale d'Assurance Maladie des Travailleurs Salariés, en tant que RSSI.

Lazaro a participé à de nombreux séminaires et congres sur la sécurité en Europe et aux Etats Unis (Net-Focus, Fraud & Security à Londres, Virus & Security à New York , CISO Summit à Nice, Budapest et Madrid...).

Résumé de l'intervention
Les Systèmes d'Information Hospitaliers (SIH) ont entamé leur mutation en Système d'Information de Santé (SIS) articulés autour du parcours de soins du patient et des prises en charge par tous les professionnels de santé.
Cela nécessite l'hébergement, le partage et la mise à disposition de l'information médicale entre ces acteurs. Les projets impliquent désormais des maitrises d'ouvrage « polycéphales » comprenant des établissements publics et privés de santé, des collectivités locales portant les projets de maison de santé, des libéraux, des réseaux de soins, des plateaux techniques publics et privés, des groupements de Coopération Sanitaire le tout sous l'impulsion et l'œil vigilant des Agences Régionales de Santé.
Cela implique également la mise en œuvre de solutions techniques et organisationnelles partagées par tous, intégrant les systèmes existants et développant les nouveaux usages tels que la télémédecine avec ses multiples facettes (téléconsultation, téléexpertise, télésurveillance, ...) ou bien le DMP dans le respect des contraintes et des attentes opérationnelles des professionnels.
Signes forts que l'hébergement sera au cœur des systèmes d'information de santé, le « Plan Hôpital Numérique », au travers de ses prérequis, réaffirme les fondements de l'hébergement comme socle indispensable au développement des usages et des échanges. Lequel est assorti d'une garantie d'une très haute disponibilité dans l'acheminement des données.

L'arrivée du Cloud n'augure-t-elle pas d'une tempête au cœur de nos systèmes d'information de santé ?

Monsieur Christian ESPIASSE

RSSI du MIPIH

Monsieur Frédéric CIRILLO

RSIO CH Nevers, Collège DSIO

Monsieur Gilbert MARTIN

RSIO CH Dax, Collège DSIO

Monsieur Tristan SAVALLE

Responsable de Marché ADVENS

Monsieur Olivier ZMIROU

Directeur IT Division AGFA HealthCare

Monsieur Tristan SAVALLE
Responsable de Marché ADVENS

La sécurité des SI Santé : un retour d'expérience

Tristan Savalle dispose de plus de 15 ans d'expérience dans le domaine de la sécurité de l'information acquise dans un grand cabinet de conseil Parisien au sein duquel il a porté la démarche ISO 27001 et la réflexion autour des SMSI pendant plusieurs années. Il est ainsi l'auteur d'un livre blanc sur la norme ISO 27001.
Tristan intervient désormais comme directeur de mission dans des projets complexes, notamment pour la mise en place de fonctions sécurité ou de SMSI dans le secteur de la santé. Il pilote des analyses de risques menées avec les populations métiers. Il accompagne les clients d'Advens dans leurs réflexions stratégiques de sécurité.
Il anime des réflexions et des séminaires sur les problématiques de sécurité de l'information auprès de la communauté (journées du MIPIH, congrès du Mans, manifestations des ARS...)
Il est certifié ITIL Foundation, ISO 27001 Lead Auditor (LSTI) et Certified Information System Security Professional (CISSP).

Résumé de l'intervention
Voir page 18

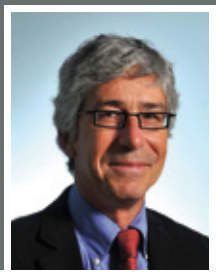
Monsieur Guillaume DERAEDT
RSSI CHRU de Lille

La sécurité des SI Santé : un retour d'expérience

Guillaume Deraedt est Responsable de la Sécurité des Système d'Information et Correspondant Informatique et Liberté du CHRU de Lille. Guillaume est actuellement responsable de la mise en place d'un Système de Management de la Sécurité du Système d'Information (SMSSI) au CHRU de Lille
Le SMSSI permet à la Direction Générale de l'établissement de prendre les décisions éclairées en matière de sécurité informatique et de maintenir la Politique de Sécurité du Système d'Information à l'état de l'art, en contribuant à l'efficacité des pôles : Direction de projet à la mise en œuvre d'un SMSI certifié ISO 27 001 transversal au CHRU de Lille.
Guillaume est également Coordinateur national du groupement d'achat inter hospitalier UniHA/NTIC-sécurité (45 adhérents dont notamment l'AP-HM, l'AP-HM, les Hospices Civiles de Lyon)
Sur sollicitation de la DHOS, direction d'un projet d'achat regroupant à ce jour 45 établissements hospitaliers majeurs. Il concerne la SSI (Sécurité du Système d'Information) et plus particulièrement la PSSI (Politique de Sécurité des Systèmes d'Information), la sensibilisation à la SSI, la gestion des identités et des rôles, l'authentification des utilisateurs, la traçabilité ainsi que la gouvernance et la sécurité des postes de travail. Ces marchés sont réalisés en mode collaboration via l'animation d'un groupe de 20 experts SSI santé selon les normes ISO 27 000x, le RGS, la PSSI ministérielle Santé. Projet réalisé avec le soutien de l'ASIP Santé et du service du HFSD du ministère de la Santé, de la jeunesse et des sports (FSSI Santé). 15 marchés publiques attribués et opérationnels, 3 marchés publiques en cours de publication.

Guillaume a enfin dirigé Directeur d'un projet national de livre blanc de la sécurité informatique des dispositifs biomédicaux (2009-2010) et a été directeur du Projet Carte d'Etablissement du CHRU de Lille (Projet référence Nationale – 12 000 cartes), de 2006 à 2010.

Résumé de l'intervention
Voir page 18



Professeur Benoit VALLET
Président de CME CHRU de Lille

La sécurité des SI Santé : un retour d'expérience

Président de la Commission Médicale d'Etablissement du CHRU de Lille depuis 2003, le Professeur Benoît Vallet est également membre du Bureau de la Conférence Nationale des PCME. Il a également été membre du Conseil Exécutif de 2006 à 2010, puis du Directoire de 2010 à 2011.
Depuis sa promotion au rang de Professeur Première Classe en 2005, son engagement hospitalo-universitaire a été poursuivi des les trois axes suivants : le soin, l'enseignement et la recherche.
En ce qui concerne la recherche, son appartenance à l'équipe EA 2689 depuis 2009 lui a permis d'encadrer des Masters, des Thèses d'Université et une Habilitation à Diriger des Recherches. Les travaux de recherches cliniques l'ont également autorisé l'encadrement de Thèses et Mémoires d'Anesthésie Réanimation. Ces travaux lui ont également permis, et depuis 2005 d'être coauteur de plus de 50 publications dans des revues avec comité de lecture.
Pour l'enseignement, il a continué sa participation au DES, Maîtrise et Masters de l'Université de Lille II, aux Cours Européens de plusieurs régions françaises et au DU d'hémodynamique de la Faculté Paris Sud. Président de la Collégiale des PU-PH d'Anesthésie Réanimation depuis 2010, il a pu prendre une part active aux réflexions échanges et travaux de la Commission Nationale de l'Internat et du Post Internat.

Membre de l'European Board of Anesthesia (EBA) au titre de l'Union Européenne des Médecins spécialistes depuis 2009, le Professeur a été élu par neuf des sections de l'UEMS ouvrant sur la Réanimation, Président du Multidisciplinary Joint Committee of Intensive Care Medicine (UEMS) depuis septembre 2010.
Au titre du soin et des fonctions hospitalières, Chef du Pôle d'Anesthésie Réanimation du CHRU de Lille de 2010 à 2011, le Professeur Vallet est depuis septembre 2010, Responsable de la Clinique d'Anesthésie Réanimation (Gynécologique, Obstétrique, Pédiatrie) de l'Hôpital Jeanne de Flandre.

Résumé de l'intervention
Voir page 18

La sécurité des SI Santé : un retour d'expérience

Résumé de l'intervention

Le secteur de la santé vit actuellement une révolution, avec un Système d'Information toujours plus au cœur des soins : de nouveaux usages, de nouvelles habitudes pour s'adapter à un nouveau contexte et à améliorer les réseaux de soins à l'échelle nationale voire internationale.

Si les enjeux de sécurité et de fiabilité sont de mieux en mieux compris par les établissements, la prise en compte de ces enjeux au quotidien se heurte encore à des organisations complexes et déjà fortement occupées, et à un marché de solutions SI ne prenant, encore trop souvent, pas assez en compte les spécificités du secteur.

Dès lors, une démarche de proximité est nécessaire pour le pilote de la sécurité au sein de chaque établissement (le RSSI lorsqu'il existe). Quand les standards et les normes de sécurité ne sont plus suffisantes, il convient de comprendre les attentes de chaque population, médicale, soignante, administrative, technique, SI... pour les rationaliser et bien sûr tenter d'y répondre.

Il convient aussi de prévoir un plan d'action sécurité non seulement cohérent avec la stratégie SI, mais visant les mêmes objectifs. Comment penser sécuriser l'accès aux données si l'outil informatique permettant d'y accéder n'est pas adapté ? Comment prévoir des procédures dégradées quand les procédures quotidiennes elles-mêmes ne sont pas claires ?

L'objectif de notre conférence est de présenter une approche de prise en compte de la sécurité avec les métiers et avec les équipes SI pour contribuer à leur efficacité ... et pour qu'ils le sachent !

Docteur Dirk COLAERT
Chief Medical Officer – AGFA HealthCare

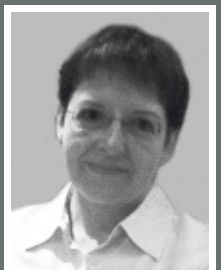
Patient Safety au sein des SI de Santé : enjeux et structuration de traitement

Résumé de l'intervention
La sécurité du patient est un sujet récurrent au sein de la communauté médicale. Et ceci non seulement à cause de l'expansion de l'utilisation de la technologie de l'information. Les hôpitaux doivent délivrer des services fiables même s'ils n'utilisent pas l'informatique. Les soins de santé ne scorent pas bien en ce qui concerne la sécurité du patient. Les soins médicaux deviennent de plus en plus complexes et multidisciplinaires. Par conséquent la probabilité que des situations de plus en plus néfastes arrivent devient même plus réelle. D'où l'idée que l'informatique peut aider, mais aussi produire de nouveaux risques. Dans notre société existe une nouvelle tendance de considérer le logiciel médical comme un appareil médical avec tous ses avantages et désavantages.

Appareil médical ou non, quand un mal arrive à un patient, les vendeurs du logiciel auront à prouver qu'ils ont fait tout le nécessaire pour éviter ce mal. Une analyse du risque sévère doit être réalisée avant le lancement de produit au marché et bien sûr aussi chaque fois qu'une plainte d'un client survient. Plus qu'on sera tôt pour découvrir des situations nocives, plus qu'on pourra diminuer le coût de la solution.

Tout de même nous pouvons faire mieux: nous pouvons utiliser l'informatique pour retracer de manière active des situations nocives en surveillant constamment à l'aide d'un moniteur des données cliniques dans le Système d'Information Clinique et en procurant un tableau de bord pour la sécurité du patient qui présente la performation actuelle de l'hôpital. Comme il y a différentes sources de données dans l'hôpital, ceci nécessite une plate-forme sémantique et interopérable au sein de l'hôpital. Au moment que vous avez ça, vous pouvez suivre sur un moniteur les scores de sécurité du patient aussi bien au niveau hospitalier qu'au niveau régional. Ceci peut être réalisé d'une manière anonyme. Ainsi un hôpital peut voir ses propres résultats comparés aux résultats anonymes de ses égaux.

Ce n'est qu'en mesurant des indicateurs que nous pouvons créer des preuves d'évidence de notre niveau de performance et notre niveau d'amélioration.



Madame
Kristina KERMANSHAHCHE
Chief Architect Healthcare – INTEL CORP

Security and Big Data Implications of Personalized Medecine

Traduction simultanée

Kristina Kermanshahche est architecte en chef Santé chez Intel Corporation. Ses domaines d'expertise sont le Big Data et l'analytique au service de la santé et des sciences du vivant, pour accompagner la transformation à la croisée des technologies d'échanges de données de sante, du cloud et du calcul haute performance (HPC).
Elle travaille en collaboration avec un écosystème de partenaires pour faire émerger la médecine de précision, et accélérer l'adoption de clouds sécurisés de santé partout dans le monde.
Kristina Kermanshahche agit également en temps que conseil stratégique auprès de nombreux gouvernements et collectivités territoriales, de ministères de la santé, et de nombreuses instances publiques partout dans le monde.
Ses domaines de recherche couvrent les architectures orientées service appliquées aux politiques de santé publique, la gestion des affections chroniques depuis le domicile jusqu'aux essais cliniques, et l'informatique biomédicale.

Résumé de l'intervention
Le séquençage du genome et la médecine personnalisée sont à notre porte. Ils vont peser lourdement sur notre informatique et vont nécessiter la mise en œuvre de technologies « Big Data ».

Avec la baisse de coût du séquençage (bientôt aux environs de 1000$), nous pouvons commencer à envisager l'individualisation des thérapies, et cela change radicalement la donne. Il ne s'agit plus seulement de faire baisser le coût du séquençage, mais de gérer l'explosion de données qui en découle pour obtenir des résultats probants sur la santé du patient , en particulier :

• D'analyser les données aval , issues de la multiplication des paramètres et de leur dynamique,et provenant de sources diverses, de différents formats.

• De stocker, transférer et administrer données et processus ;

• et peut-être plus paradoxalement, de les interpréter pour accélérer la mise en œuvre immédiate des découvertes cliniques les plus récentes .

Plus nous nous rapprochons de l'échelle de « l'infiniment petit » (tant pour la technologie, que pour la prise en charge des maladies), plus la complexité du problème s'accroit .

Aujourd'hui la sécurité des « clouds » et du « big data » des données de santé est un vrai sujet :

• Quels sont les enjeux de sécurité posés par l'hébergement et l'analyse de données de santé sur le cloud ?

• Quand fait il sens de choisir des solutions de cloud privés, ou de déborder sur des cloud publics ?

• Comment mettre en œuvre des solutions de haute disponibilité, et/ou comment permettre l'accès à distance à un dossier patient consolidé, en situation de mobilité, quel que soit l'outil numérique dont on dispose ?

• Comment concilier plan de reprise d'activité en cas de panne avec les contraintes de transparence et de conformité posées par la législation, par exemple en matière de protection des données personnelles ?

A partir d'un certain nombres d'exemples concrets, nous aborderons les architectures et les solutions permettant d'assurer la sécurité de bout en bout pour la médecine individualisée à l'heure du Big data.

Monsieur Sébastien WETTER
Expert SSI - ENOVACOM

Gestion des identités : une pièce maîtresse de l'échiquier sécurité

Après 5 années passées en SSII au service de diverses DSI, dans des secteurs variés comme la publicité, l'édition, le packaging ou encore le juridique, Sébastien Wetter a eu l'occasion de se bâtir de fortes compétences en système d'information et notamment en architecture et urbanisation. C'est alors qu'il entre dans le cabinet de conseil Stream Consulting, en tant que consultant en systèmes d'informations, lui permettant de mettre en application ses compétences dans différents contextes, comme la santé, et de compléter celles-ci par l'acquisition de méthodologies projets éprouvées. Il intervient alors pour plusieurs ARH, ARS, GCS ou encore établissements. Par la suite, il se spécialise dans le domaine décisionnel et l'interopérabilité. Au cours de l'évolution de ce cabinet de conseil, Sébastien s'est vu confié la responsabilité du pilotage d'un pôle middleware, intégrant le management d'une équipe de développement. Aujourd'hui, il intervient chez Enovacom en tant qu'ingénieur produit sur toute la gamme sécurité.

Résumé de l'intervention
Ces dernières années ont été marquées par une recherche renforcée d'une efficience opérationnelle au sein des établissements de santé. Ces besoins d'optimisation, tant en termes de coût, que d'organisation, ont grandement participé à la croissance de l'informatisation et de la dématérialisation des données de santé. Ces évolutions et les adaptions perpétuelles du système d'information conduisent plus que jamais à prendre en considération les différentes menaces pesant sur les données médicales.

L'enjeu d'un projet de sécurité est donc prioritairement de répondre à ces menaces majeures portant sur la disponibilité, l'intégrité et la confidentialité de l'information. De nombreux outils ou méthodologies sont disponibles pour se lancer dans une démarche de sécurisation.

La question qui se pose alors pour un Directeur des Système d'Information est alors : par où commencer ?
Au milieu des différentes briques à mettre en place au sein du système d'information, la gestion des identités est un élément crucial et incontournable pour entreprendre la première étape de sa sécurisation.

Après 5 années passées en SSII au service de diverses DSI, dans des secteurs variés comme la publicité, l'édition, le packaging ou encore le juridique, Sébastien Wetter a eu l'occasion de se bâtir de fortes compétences en système d'information et notamment en architecture et urbanisation. C'est alors qu'il entre dans le cabinet de conseil Stream Consulting, en tant que consultant en systèmes d'informations, lui permettant de mettre en application ses compétences dans différents contextes, comme la santé, et de compléter celles-ci par l'acquisition de méthodologies projets éprouvées. Il intervient alors pour plusieurs ARH, ARS, GCS ou encore établissements. Par la suite, il se spécialise dans le domaine décisionnel et l'interopérabilité. Au cours de l'évolution de ce cabinet de conseil, Sébastien s'est vu confié la responsabilité du pilotage d'un pôle middleware, intégrant le management d'une équipe de développement. Aujourd'hui, il intervient chez Enovacom en tant qu'ingénieur produit sur toute la gamme sécurité.

Docteur
Valérie SERRA-MAUDET
Chef de Service en Chirurgie,
Chef de Projet Hôpital Numérique – CH LE MANS

La SSI au cœur des processus médicaux : une libre lecture des avantages !

Chirurgien depuis 1992, Praticien hospitalier depuis 1995, et Chef de service depuis 2009, Valérie SERRA-MAUDET est Vice-Présidente de CME de 2003 à 2010 puis devient Chef de Projet Médical sur le déploiement du Dossier Patient Informatisé au Centre Hospitalier du Mans, animant des groupes de Médecins et dirigeant la partie médicale du Projet.

Résumé de l'intervention
Parler de SSI dans le monde de la santé, c'est aussi parler des hommes et des femmes qui utilisent les outils, parler de leur vision de cette sécurité , de la confiance qu'ils accordent -ou pas- au systéme, de ce qui aujourd'hui et demain saura les mettre sur la voie de cette confiance. En parler du «dedans», de la place d'un utilisateur de base, mais aussi du poste de responsable d'un projet d'informatisation du dossier , donc d'un changement des pratiques de soignants , c'est le modeste objectif de cette présentation.

Docteur Jacques LUCAS
Vice-Président du Conseil National de l'Ordre des Médecins

Les sécurités informatiques : obligations déontologiques

Résumé de l'intervention
Traiter des sécurités des systèmes d'information en santé et des bases informatiques contenant des données personnelles de santé n'est pas un exercice de style pour le CNOM. En effet, l'impératif déontologique est inscrit, pour tout médecin, dans l'article R 4127-4 du code de la santé publique (CSP), portant déontologie médicale : « Le secret professionnel, institué dans l'intérêt des patients, s'impose à tout médecin dans les conditions établies par la loi. Le secret couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris ».

Dans les établissements de santé, le secret médical est entendu comme étant le secret professionnel partagé par les professionnels de santé qui constituent l'équipe de soins au sens de l'article L. 1110-4, alinéa 3 du CSP.

La limitation législative de cette « équipe de soins » aux seuls établissements de santé fait aujourd'hui débat et conduit à élargir la réflexion sur le partage, les échanges et les accès aux données personnelles de santé « hors les murs » de l'établissement. C'est un des objectifs du DMP, du dossier communicant de cancérologie et celui de la fluidité des échanges informatisés à partir des bases de données par messageries, etc.

Dans cet ensemble complexe, l'intrusion informatique malveillante ou non autorisée pourrait entrainer la divulgation d'une information à caractère secret, paralyser le système ou pervertir les données. Les règles de sécurité doivent donc être strictement respectées. Elles constituent à ce titre une exigence déontologique. Elles doivent l'être d'ailleurs tant pour ce qui concerne la protection de la confidentialité que pour ce qui s'attache à la robustesse, à la disponibilité et à la fiabilité des systèmes d'information.

La confidentialité

Les professionnels de santé ayant accès aux bases de données doivent être authentifiés et leurs accès doivent être tracés par le système. La loi impose la Carte de Professionnel de Santé (CPS) pour l'accès aux données. Ce dispositif devrait être utilisé pour tous les accès aux bases informatiques stockant ou hébergeant des données personnelles de santé. Cependant une authentification sans contact - comme la CPS3 le permettra désormais - est indispensable pour toutes les activités mobiles. En outre, ses « dispositifs équivalents », sont prévus par la loi. Si le Directeur de l'Etablissement porte la responsabilité de la sécurité des SIS dans le respect de la loi, les médecins doivent être impliqués dans la définition de la politique de confidentialité de l'établissement, comme dans les formations des professionnels de santé et les auxiliaires avec lesquels ils exercent. La « sécurité déontologique » est une première marche fondamentale dans la sécurité informatique d'ensemble. Aucun accès ne devrait pouvoir avoir lieu sans reconnaissance de l'habilitation formelle par le système, distinguant rigoureusement les données administratives des données médicales. En outre, l'accès aux données personnelles de santé est clairement restreint par la loi du 4 mars 2002 à l'équipe soins qui prend en charge un patient pour une pathologie ou un épisode de soins. Ces données ne devraient pas être accessibles aux autres unités de l'établissement qui ne concourent pas directement à la prise en charge de cette pathologie ou de cet épisode. Selon le CNOM, l'accès aux données par une autre équipe de soins pour un autre motif d'hospitalisation ultérieure doit recueillir le consentement exprès du patient. Le système d'information de l'établissement doit prévoir cette situation.

La sécurité informatique d'ensemble

A la qualité déontologique, respectant le droit des patients à la confidentialité de leurs données personnelles de santé et le secret qui les protège s'associe la qualité des prises en charge médicales ou médico-sociales. Le système d'information doit permettre de protéger le « temps médical » en structurant de façon fiable les données personnelles des patients et en permettant un accès rapide aux bases de données, pour la qualité et/ou l'urgence du soin. Les médecins et professionnels de santé doivent respecter des procédures propres à garantir la sécurité informatique du système d'information qui concourt à la qualité du soin.

Monsieur
Etienne CHEVILLARD
RSSI – SIGMA INFORMATIQUE

Monsieur Jean-Pierre STEHLY
Ingénieur SIGMA INFORMATIQUE

Données de santé, Cloud & SaaS : dépasser les peurs !

Etienne Chevillard est Responsable de la Sécurité des Systèmes d'Information (RSSI) de Sigma Informatique.
Il intervient depuis plus de 10 ans dans le domaine de la sécurité de l'information. D'abord ingénieur en sécurité des systèmes et réseaux au sein de Silicomp-AQL, puis consultant en sécurité des SI pour Orange Business Services, il réalise plusieurs missions de conseil, d'expertise technique et d'audit de sécurité. Il accompagne ainsi plusieurs établissements de santé dans la définition et la mise en œuvre de leur Politique de sécurité.

Depuis mars 2010, date à laquelle il rejoint Sigma Informatique, il pilote le processus de management des risques IT au sein de la société, met en place un Système de Management de la Sécurité de l'Information basé sur les normes ISO 27001, 27002 et 27005, et conduit la réalisation du dossier de demande d'agrément hébergeur de données de santé ainsi que les actions d'amélioration associées.

Etienne Chevillard anime depuis 2008 les forums Sécurité et Management de l'Information de l'association ADN'Ouest.

Ingénieur CNAM, Etienne Chevillard est certifié CISSP (Certified Information Systems Security Professional) depuis 2007.

Jean-Pierre Stehly est Ingénieur d'Affaires Infogérance pour Sigma Informatique.

Expert dans l'élaboration des offres SaaS pour Sigma Informatique et auprès des éditeurs partenaires, Jean-Pierre Stehly prend en 2008 la responsabilité du développement de l'activité d'infogérance de Systèmes d'Information de Santé et de données sensibles auprès de grands comptes.

Après une première expérience dans les réseaux informatiques comme ingénieur puis architecte pour une grande SSII, il occupe le poste de Chef de Projet puis de Responsable Technique de l'agence parisienne d'une filiale IBM en charge du déploiement d'applications destinées aux collectivités locales et territoriales.

Directeur Technique d'une multinationale, il élabore le plan de consolidation du centre de traitement, prend en charge le déploiement à l'international de systèmes d'autorisations bancaires aux normes EMV et pilote la mise en production de la première solution de carte virtuelle dynamique pour le compte d'un grand opérateur.

Résumé de l'intervention
Voir page 22

Données de santé, Cloud & SaaS : dépasser les peurs !

Résumé de l'intervention
L'antinomie entre le Cloud Computing et la protection des données de santé à caractère personnel nécessite de la part des industriels une réflexion sur le fond conduisant à construire en collaboration avec les différents acteurs du domaine, un modèle capable de concilier mutualisation de ressources, sécurité de l'information médicale et conformité à la réglementation en conservant les avantages financiers du modèle.

Notre conférence aura pour objectifs de :

• Démystifier les concepts du Cloud Computing

• Exposer en tant qu'industriel spécialiste du domaine notre compréhension de ces concepts et notre vision des apports de l'approche Cloud pour l'e-santé

• Rappeler les interrogations et les craintes des décideurs au moment d'externaliser leurs données de santé face aux offres de service de type Cloud (IaaS, PaaS ou SaaS)

• Proposer les critères permettant d'accompagner ces décideurs dans le choix de leur prestataire

Monsieur
Philippe de la GARDETTE
PDG Nexthink

Monsieur Guillaume DERAEDT
Coordinateur national segment SSI UniHA

Les 40 règles d'hygiène informatique de l'ANSSI s'applique-t-elle à la communauté hospitalière ?

Philippe de La Gardette, Directeur Général de Nexthink en France depuis début 2007, a contribué au succès du lancement de Nexthink. Serial entrepreneur depuis près de 20 ans, il a créé et développé plusieurs sociétés dans le monde de l'édition de logiciel.

Guillaume DERAERDT : cf page 16

Résumé de l'intervention
L'ANSSI vient de publier son premier guide d'hygiène informatique à destination des grandes entreprises, administrations et OIV. Les 40 règles de base seront reprises dans la future PGSSI en préparation à la DGSIS et deviendront probablement obligatoires. Sont-elles compatibles avec les contraintes inhérentes aux activités de la communauté hospitalière ? Comment connaître et documenter la situation actuelle afin de pouvoir planifier un programme d'amélioration et de mise en conformité ?
On sait que 90% des incidents sont de sources internes. Dans la mesure où 20% de mesures adéquates de base, d'hygiène sécuritaire simple, règlent 80% des problèmes et des causes d'évènements indésirables, la sécurité ne peut pas être réduite à un simple problème de moyens, mais elle devient la résultante de la mise en œuvre d'une réelle gouvernance des Systèmes d'Information de Santé, de compétences et d'appropriation par l'ensemble des acteurs.
Gouverner, c'est savoir. Savoir d'où l'on vient et où on veut aller. Mais c'est surtout définir sa trajectoire de progrès et la mesurer de façon permanente. Il s'agit de la prise de conscience et de la mesure irréfutable de l'état de maîtrise des risques IT dans les hôpitaux et de leurs impacts directs et indirects pour les professionnels de santé (risques métiers) et les directions générales (risques légaux) sur les 5 axes suivants : mesure du niveau de standardisation du parc de postes, mesure de l'efficacité des politiques de sécurité, mesure du niveau de conformité applicative, mesure de la disponibilité des SIH et du ressenti utilisateur, enfin la mesure de l'activité et des usages des SIH.
Plus d'une centaine d'hôpitaux sont donc actuellement équipés de la solution NEXThink, représentant des GCS, CHRU, CHU, CH, HL, PSI ainsi que le Service de Santé des Armées.

NEXThink est titulaire du lot 8 : « Gouvernance des postes de travail et traçabilité des activités » du marché UniHA GAC SSI.

La prise d'empreinte et la cartographie de l'existant, l'identification documentée des risques IT et métiers, la mise en évidence des pistes d'amélioration et/ou de remédiation, et enfin le contrôle strict des procédures et du maintien en conditions opérationnelles et de sécurité pour documenter la check-list de l'ANSSI peuvent être faits dans le cadre des UO du Lot 8 de ce marché UniHA.

Monsieur
Jean-François PARGUET
Directeur du pôle Technique et Sécurité
ASIP Santé

Madame Frédérique POTHIER
Chargée de Mission SSI – Ministère des Affaires Sociales et de la Santé - DSSIS

Des référentiels de sécurité en Santé

En 2006, Jean-François Parguet intègre le GIP DMP, actuelle ASIP Santé.
Il est actuellement Directeur du pôle Technique et Sécurité et Responsable de la Sécurité des Systèmes d'Information (RSSI).
A ce titre il a la responsabilité de la production avec les acteurs concernés :

• des référentiels d'interopérabilité, d'architecture et de sécurité et en particulier :
- Le référentiel d'identification des patients, (INS)
- Le cadre d'interopérabilité des SI de santé, (CI-SIS)
- La politique générale de sécurité des SI de santé, (PGSSI-S)
- La procédure d'agrément des hébergeurs de données de santé pour sa composante exigences de sécurité, (PIAHDS)

• des infrastructures nationales participant à l'espace national de confiance
- produits de certification de la famille cartes de professionnels de santé (CPS)
- référentiels d'acteurs du secteur de la santé (RPPS et RASS).

Résumé de l'intervention
Le développement de l'usage des technologies de l'information et de la communication et son corolaire, la dématérialisation des données de santé, constituent un levier majeur de la modernisation du système de santé et contribue à l'amélioration de la qualité de la prise en charge des patients. Par ailleurs cette dématérialisation massive des données de santé les expose inévitablement à des risques de sécurité inhérents aux systèmes d'information. Une refonte globale et structurelle de la sécurité des systèmes d'information de santé est donc nécessaire pour créer un espace numérique de confiance favorable à la dématérialisation, au partage et à l'échange de données de santé. Elle conditionne l'adhésion des patients et des professionnels de santé aux nouvelles pratiques liées à l'informatisation (hôpital numérique, télémédecine, mobilité, ...) et aux orientations technologiques actuellement privilégiées (hébergement de données, hébergement de services avec la multiplication des offres de logiciels en mode SaaS, mutualisation de ressources informatiques, Cloud, ...).
Vont vous être présentés à ce titre les principaux référentiels impliqués dans la dématérialisation des données de santé et permettant de bâtir l'espace national de confiance dans la santé : référentiels d'identité, référentiels d'interopérabilité, référentiels de sécurité.

Monsieur Hervé SCHAUER
CEO HSC

De la qualification des prestataires en sécurité de l' information

Après des études d'informatique à l'Université Paris 6 (Jussieu), Hervé Schauer s'affirme très tôt comme un des pionniers de la sécurité informatique en France, avec (entre autres) la publication dès 1987 d'une série d'articles sur la sécurité Unix et la détection d'intrusion.
En 1989 il fonde son propre cabinet (Hervé Schauer Consultants). Il est l'inventeur du relayage applicatif (proxy firewall) pour l'agence française de l'espace (CNES) en 1991, présenté au Usenix Security Symposium en 1992, mais n'a pas brèveté son invention, ainsi celle-ci a été utilisée librement par la suite dans la majorité des firewalls commerciaux.
Hervé Schauer a publié ou contribué à de nombreux ouvrages et articles , notamment sur la sécurité Internet, le cloisonnement de réseaux, dont il est à l'origine, l'authentification, la sécurité des technologies sans fil, les normes ISO 27001 et ISO 27005, etc.
Hervé Schauer est conférencier invité et instructeur lors de nombreuses conférences spécialisées en Europe et au-delà.
Hervé Schauer a été consultant pour plus de 200 sociétés françaises et mondiales, des opérateurs de télécommunication, des gouvernements et des organisations internationales.
Il est conseiller scientifique pour plusieurs start-ups, des entreprises établies et des sociétés de capital-risque.
Hervé Schauer a également des responsabilités dans de nombreuses associations, il anime notamment le groupe Sécurité Unix et Réseaux de l'OSSIR depuis 1989, a co-fondé l'OSSIR et les chapitres français de l' ISO et de l'ISSA, et a lancé le Club 27001 (chapitre français de l'ISMS Users Group).
Hervé Schauer est correspondant régulier sur la sécurité de l'information auprès de journalistes de la presse spécialisée.
Hervé Schauer est certifié CISSP par ISC2 (2004), ITIL Foundations (2007) et Information Security Foundation (2010) par EXIN, ISO 27001 Lead Auditor (2005), ISO 27001 Lead Implementer (2006) et ISO 27005 Risk Manager (2008) par LSTI, et QSA par le PCI-Council (2011), certifié GSLC (GIAC Security Leadership Certification) par GIAC (2012) et il a été enregistré ISMS provisional auditor par RABQSA (2007).

Résumé de l'intervention
Le RSSI a besoin d'auditeurs pour atteindre ses objectifs de sécurité.
Le choix d'un prestataire d'audit de sécurité dans la santé où les économies imposent la sélection de moins-disant ne permet pas toujours de bénéficier du résultat attendu. Le RGS (Référentiel Général de Sécurité) prévoit la qualification des prestataires d'audit de sécurité et l'ANSSI démarre la préfiguration du processus en cette fin d'année 2012. D'autres pays comme la Grande-Bretagne ont mis en oeuvre dès 2006 ce principe de qualification par les experts de l'état des prestataires d'audit privés que les donneurs d'ordre n'ayant pas les moyens de contrôler la compétence et la probité des candidats pourront sélectionner en tout confiance. Hervé Schauer présente cette certification des prestataires d'audit en sécurité des systèmes d'information, des principes de la certification aux objectifs qu'ils faudrait atteindre pour que le système soit le plus utile, en passant par l'intérêt et l'importance d'une telle qualification pour la monde de la santé.

Monsieur
Jean-François LOUAPRE
Responsable Sécurité AG2R La Mondiale
Vice-Président du CESIN

Quelles menaces et comment l'écosystème de santé doit-il s'organiser ?

Jean-François est le Responsable Sécurité du groupe AG 2R LA MONDIALE . Il est en charge, outre de la sécurité des systèmes d'informations, de la continuité des activités du groupe et de la sécurité des personnes et des biens. Il a rejoint AG 2R en 2007, en tant que RSSI, à l'issue de son parcours de 7 ans au sein de la Deutsche Bank, tout d'abord comme RSSI de la filiale française, puis comme coordinateur du programme de contrôle des risques informatiques pour 22 pays de la zone EMEA. Son expérience préalable de 10 ans a été acquise en sécurité informatique, système et réseau au sein de diverses SSII. Jean-François est également certifié CISM et ISO 27001 Lead Auditor, il participe activement aux travaux du groupe de travail NetFocus France et du Cercle européen de la sécurité des SI ainsi qu'à l'élaboration des manuels de préparation à la certification CISM (QAT de l'ISACA).

Monsieur Eric GROSPEILLER

FSSI Ministère des Affaires Sociales et de la Santé

Monsieur Cédric CARTAU

RSSI CHU Nantes

Madame Laëtitia MESSNER

DGOS

Madame Kristina KERMANSHAHCHE

Chief Architect Healthcare – INTEL CORP