Le Mans - du 1er au 3 avril 2014

24 heures de débats, d'échanges et de convivialité

3ème congrès national

Sécurité des systèmes d'Information de Santé

Agir pour bâtir ensemble une sécurité durable des systèmes d'information de santé.

www.apssis.com

Le Mans DHMAGAZINE LE MAGAZINE DU DÉCIDEUR HOSPITALIER DSiH

Sommaire

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

www.apssis.com
secretaire@apssis.com

Monsieur Philippe LOUDENOT

Ministère des Affaires Sociales et de la Santé

La SSI au coeur de la santé

Philippe Loudenot vient de quitter le poste de fonctionnaire de sécurité des systèmes d'information auprès du Premier Ministre pour rejoindre à nouveau l'équipe du Haut fonctionnaire de défense et de sécurité des ministères chargés des affaires sociales. Ancien responsable national de la sécurité des systèmes d'information du service de santé des armées, il dispose d'une connaissance approfondie du monde de la santé.

Ancien auditeur de l'institut des hautes études de la défense nationale, il est chargé de cours SSI au profit de différentes universités et écoles d'Ingénieurs.
Présent dans la vie associative des experts en Sécurité du Système d'Information, il est membre du conseil d'administration de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information, du CESIN et du club EBIOS.

Madame Sophie VULLIET-TAVERNIER

Directrice des Etudes, de l'Innovation et de la Prospective - CNIL

Santé et bien-être dans le monde numérique : quelle vision prospective pour la protection des données de santé ?

Directeur des affaires juridiques, internationales et de l'expertise, de la CNIL de 2007 à 2010, Sophie Vulliet-Tavernier a pris la responsabilité, début 2011, de la Direction des Études, de l'Innovation et de la Prospective. Cette Direction, nouvellement créée, est chargée de la veille prospective et a pour mission de mieux identifier et comprendre les évolutions des technologies et des usages du numérique dans tous les domaines qui relèvent de la compétence de la CNIL, d'évaluer les enjeux de protection des données qui en découlent et ainsi de l'éclairer dans ses décisions et modes d'intervention.

Sophie VULLIET-TAVERNIER est diplômée de l'université de droit et de sciences sociales de Paris II et de l'Institut Français de Presse (DEA de sciences politiques, DESS de droit de la Défense, Maîtrises en Droit Public et en Sciences de l'information).

Madame Auriane LEMESLE

RSSI GCS Télésanté Centre

Madame Astrid LANG

RSSI S.I. Patient - AP-HP

RSSI Santé: Un métier à construire. Réalités et prospective

Auriane LEMESLE

Auriane Lemesle est Responsable de la Sécurité des Systèmes d'Information (RSSI) au Groupement de Coopération Sanitaire (GCS) TéléSanté Centre depuis avril 2012. Après un Master I en « Sciences, Technologies et Organisation de la Santé », elle a validé deux Master II « Risques sanitaires dans les structures de soins et industries de produits de santé » et « Management de la Sécurité des Systèmes d'Information de Santé » à l'ISSBA d'Angers. Sa formation a été ponctuée par 10 mois de stage au CHU d'Angers autour de la gestion des risques liés au SI au niveau des laboratoires de biologie médicale ainsi que par la mise en place de procédures de secours pour la prescription d'examens de biologie médicale en cas de panne informatique.

L'animation et la coordination d'une démarche sécurité à l'échelle régionale sont les deux composantes essentielles de son rôle de RSSI. Fédérer les acteurs et installer une mutualisation entre des établissements de tailles, moyens et activités différents, sur une thématique souvent peu maîtrisée est la première mission qu'elle assure. En parallèle, il a été nécessaire de répondre à la volonté des membres du GCS de créer et développer des services aux adhérents. La sensibilisation étant la pierre angulaire d'une démarche sécurité, il est indispensable de diversifier les supports et les outils de communication pour les adapter au public concerné (tutelles, décideurs, professionnels de santé, équipe système d'information). Comment trouver le juste équilibre entre actions collectives et accompagnements individuels des établissements ?

Astrid LANG

Avec plus de 30 ans d'expérience de direction de projets dans le contexte hospitalier, Astrid Lang a rejoint en 1988 l'AP-HP pour mener, dans le contexte médical, médico-technique, finance/achat/logistique/patrimoine, des opérations d'informatisation des services sur l'ensemble des hôpitaux de l'AP-HP. Elle est depuis 5 ans RSSI du Système d'Information Patient de l'AP-HP.

Dans une organisation de refonte du système d'information lié au patient et impactant 80 000 utilisateurs, dans un contexte particulièrement sensible et critique, avec des professionnels de santé exigeants en termes d'accès et utilisation de l'information de santé, sa mission dans son domaine est large et variée ; elle porte en particulier sur la sécurisation des accès (internes et tiers) et dans l'utilisation du dossier électronique du patient, tant pour la production de soins que la recherche, ainsi que l'accompagnement au quotidien des équipes au respect de la sécurité et de la réglementation ; elle apporte sa connaissance terrain aux travaux transverses de sécurisation du SI menés à l'AP-HP.

Par ailleurs, elle participe activement aux travaux relatifs à la sécurité du SI Santé que mènent l'ASIP et l'ARS IdF, ainsi qu'au Segment SSI du groupement d'achat UNI-HA ; depuis 2013, elle coordonne le Groupe de travail SSI Santé du Clusif, et organise les réunions du Club des RSSI des CHU.

Monsieur Guillaume DERAEDT

RSSI CHRU de Lille

Monsieur Cédric CARTAU

RSSI CHU Nantes

RSSI Santé: Un métier à construire. Réalités et prospective

Guillaume DERAEDT

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 (SMSI) au CHRU de Lille. Le SMSI 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. Guillaume est également Coordinateur national du groupement d'achat inter hospitalier UniHA/NTICsécurité (45 adhérents). 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.

Guillaume a enfin dirigé 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.

Cédric CARTAU

Cédric Cartau a exercé des fonctions d'ingénieur système au CHU de Reims et dirigé les équipes techniques et applicatives de la DSI du CHU de Rennes.

Actuellement Responsable Sécurité SI au CHU de NANTES, il est également RSSI mutualisé pour le compte du GCS eSanté Pays de Loire. Egalement auteur de plusieurs ouvrages aux Presses de l'EHESP (dont «La sécurité du système d'information des établissements de santé» paru en 2012), il dispense depuis 2007 plusieurs modules d'enseignement à l'EHESP.

Résumé de la conférence :

Le système de santé français a pour mission de gérer les informations relatives à la santé des citoyens. Vaste enjeu à l'ère du numérique et de la nécessaire transmission des données médicales aux nombreux acteurs qui composent la chaîne des soins, afin de rendre les parcours plus efficients.

Sécuriser les systèmes d'information d'un Etablissement de Santé, quel qu'il soit, nécessite la mise en œuvre de techniques, de procédures, de processus et la sensibilisation de tous les professionnels.

Là où il faudrait quelques centaines de professionnels, il n'en existe aujourd'hui que quelques dizaines. RSSI de CHU, RSSI régional « mutualisé », Référent SSI, Ingénieur Sécurité sont des métiers en construction, avec l'émergence d'un maillage territorial devant permettre de déployer les Politiques de Sécurité avec des moyens relatifs.

4 Professionnels nous parlent de leur métier, de leur quotidien, des actions qu'ils mènent dans leurs sphères de responsabilité et des enjeux de leur mission.

Monsieur Gérard PELIKS
Forum ATENA, Consultant AIRBUS Defense & Space

Le Big Data, applications dans le domaine de la santé et de la sécurité des systèmes d'information

Gérard Peliks est expert en sécurité de l'Information. Il préside l'atelier sécurité de l'association Forum ATENA, dans lequel il organise de grands évènements autour de sujets comme la cybersécurité, le futur de l'Internet et la cyberstratégie. Il coordonne l'écriture de livres collectifs sur la sécurité de l'information. Il est membre du conseil d'administration de l'ARCSI (Association des Réservistes du Chiffre et de la Sécurité de l'Information), membre de la réserve citoyenne de cyberdéfense de la gendarmerie nationale, et anime les « Lundi de l'IE » du Cercle d'Intelligence Economique du Medef Ile-de-France. Gérard Peliks est chargé de cours sur différentes facettes de la sécurité, dans le cadre de Mastères de l'Institut Mines-Télécom et du Pôle Léonard de Vinci.

Résumé de l'intervention :

Le Big Data, est-ce une grande opportunité ou seulement une grande illusion ? Est-ce une innovation de rupture ou seulement du buzz sur Internet et dans d'autres média ?
Avec le Big Data, on parle en effet d'un nouveau paradigme qui va changer les interactions entre l'utilisateur, les ordinateurs et autres objets connectés. Grace aux algorithmes du Big Data bien maîtrisés, l'ordinateur fait des découvertes par lui-même, en trouvant des liens statistiques au sein de milliards de données même si celles-ci évoluent très vite et sont constituées de structures très différentes.
Nous définirons ce qu'est le Big Data ou déferlante informationnelle avec calculs massivement parallèles et visualisation pertinentes des résultats obtenus. Nous analyserons comment l'Open Data et le Small Data concourent à apporter au Big Data la possibilité de valoriser l'information existante. Nous évoquerons, sans entrer dans la technique, comment les logiciels libres tels que Hadoop, MapReduce, Hive permettent des traitements de gros volumes de données qui auraient été impensables avec les outils classiques.
Dans le domaine de la santé, le Big Data peut apporter des réponses dans la prédiction des épidémies, dans la connaissance de la génomique, dans l'utilisation de l'imagerie médicale. Dans le domaine de la sécurité de l'Information, il permet d'analyser rapidement des quantités phénoménales d'évènements pour détecter des signaux faibles et lents qui permettent de déceler des attaques persistantes avancées.

Monsieur Sébastien WETTER
Responsable de l'offre sécurité - ENOVACOM

Audit & traçabilité des logs : Centraliser et simplifier la gestion des traces applicatives

Après 5 années passées en SSII au service de diverses DSI, 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 ARS, GCS ou encore des établissements de santé. 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. Depuis deux ans maintenant, il intervient chez Enovacom en tant que responsable offres sur toute la gamme sécurité.

Résumé de l'intervention :

Le nombre d'applications du SIH et la volumétrie des logs générés rendent difficile, voire impossible l'exploitation des traces produites sous des formes et formats hétérogènes. Rechercher les actions d'un utilisateur au sein du SIH, consulter la liste des personnes ayant eu accès aux données d'un patient, toutes applications confondues… Sans système de gestion de logs, ceci peut prendre plusieurs jours, rien que pour retrouver, isoler et interpréter les données concernées.

Enovacom, dans la continuité de son offre sécurité, propose une solution simple et adaptée aux établissements de santé, capable de centraliser et d'homogénéiser la gestion des logs. Les bénéfices de cette solution ?

- Simplifier l'audit du SIH & la production des rapports d'audit
- Répondre aux critères d'Hôpital Numérique & suivre les recommandations de la PGSSI-S
- Faciliter l'accès aux preuves suite à une intrusion malveillante
- Assurer la traçabilité avec la corrélation des logs remontés par application

enovacom

Monsieur Julien Lavesque
Directeur technique - ITrust

Top 10 des vulnérabilités

Julien Lavesque, Directeur technique d'ITrust, est Diplômé de l'ENSEEIHT. Il est intervenu dans différentes missions d'expertise telles que la PKI pour un grand-compte aéronautique. Chargé de la direction technique, il intervient en tant qu'expert en sécurité auprès des clients d'ITrust.

Résumé de l'intervention :

Exclusif ! Retour d'expérience des 7 dernières années d'audit intrusif : les 10 failles de sécurité qui correspondent à 99% des failles de sécurité dans les entreprises.
Comment sécuriser vos données informatiques par l'application de bonnes pratiques simples?
Ce n'est pas une surprise, l'année écoulée a encore été riche en actualité concernant la cybercriminalité. Cette criminalité est d'ailleurs devenue un enjeu stratégique pour toutes les entreprises PME ou grands comptes. Les budgets ne pouvant pas suivre cette augmentation de risque, il nous a semblé pertinent d'expliquer comment une entreprise peut se sécuriser simplement par la mise en place de bonnes pratiques essentielles. Corriger ces 10 principales vulnérabilités permettrait d'élever grandement le niveau de sécurité d'une organisation.

ITrust
IT Security Services

Monsieur Jean-François PARGUET
Directeur Pôle Technique et Sécurité et RSSI de l'ASIP Santé
Avec Auriane LEMESLE, RSSI GCS TéléSanté Centre et Pierre TAVEAU, RSSI CHU de Poitiers

PGSSI-S : un outil au service des Etablissements de Santé

Né en 1960, Jean-François Parguet est Ingénieur diplômé de l'Ecole Française d'Electronique et d'Informatique (EFREI).
A là tête du Pôle Technique et Sécurité de l'ASIP Santé, Il est en charge :

- De concevoir et promouvoir le corpus de référentiels technique et sécurité qui va encadrer et favoriser la dématérialisation progressive des données et leur traitement automatisé dans les systèmes d'information de santé Français. A ce jour ont été élaborés par le pôle : l'identifiant national de santé de nos concitoyens, le cadre d'interopérabilité des systèmes d'information de santé, la procédure d'agrément des hébergeurs de données de santé, le modèle d'architecture des projets dossier médical personnel (DMP) et messagerie sécurisée de santé (MSS), la politique générale de sécurité des SI de santé (PGSSI).
- De développer puis porter les infrastructures nationales constitutives de l'Espace National de Confiance du secteur de la santé et en particulier, le répertoire partagé des professionnels de santé (RPPS) et le système de gestion des produits de certification (CPS - Carte de Professionnel de Santé et certificats logiciels). A ce titre nous sommes un des premiers prestataires de service de certification (PSCE) en France avec environ 1 million de cartes sur le terrain et sommes donc un acteur majeur de l'authentification et de la signature électronique.

De 1984 à 1990, Jean-François Parguet, successivement chez Steria puis Telesystemes, est en charge de la réalisation de grands projets informatiques : le nœud de transit international de télécommunication (NTI 2 G) de France Telecom, le système de commandement des missiles HADES (CORHAD) pour Thomson DTC...
De 1991 à 2002, il intègre le Groupe ON-X Consulting, au sein duquel il est successivement associé du pôle « systèmes d'information» puis directeur associé du « pôle sécurité». En complément des activités de gestion du centre de profit, il exerce le rôle de directeur opérationnel des projets de maîtrise d'œuvre ou de conseil les plus sensibles au profit de ses clients, parmi lesquels : la CNAMTS, le Ministère de la Défense, la Fédération Nationale du Crédit Agricole, la direction du renseignement militaire, Eurocontrol, Pernod-Ricard, BNP-Paribas.

Maître Omar YAHIA
Avocat au Barreau de Paris

Externaliser le codage PMSI : risques et solutions - Qu'est-ce qu'une donnée de santé à caractère personnel ? Faire intervenir une société extérieure : est-ce bien légal ? Qui a légalement accès aux données de santé ? Réglementation : failles et solutions

Vice-président de l'APSSIS, Maître Omar YAHIA, Avocat au barreau de Paris, s'est très tôt spécialisé en droit de la santé (droit hospitalier, droit médical et droit pharmaceutique). Il conseille, représente et défend les intérêts des établissements de santé, des professionnels de santé et des opérateurs/prestataires. Formateur, chroniqueur et consultant, Maître YAHIA intervient tant en conseil qu'en contentieux, en droit de la santé numérique (télémédecine, e-santé, LAP/LAD), droit financier et en ressources humaines.

Résumé de l'intervention :

L'amélioration du codage PMSI représente un enjeu crucial pour les établissements de santé. Ce codage, soumis à des règles de complexité croissante que le praticien seul ne peut maîtriser, conduit les établissements de santé à le « professionnaliser » et à l'optimiser. Il ne s'agit pas, en parlant d'optimisation, de pervertir les règles ou de tenter de biaiser le codage en sa faveur, mais simplement de coder le RSS correctement et de façon exhaustive. Cette démarche d'optimisation suppose, pour certains établissements, d'externaliser les données de santé en en confiant le retraitement à des sociétés spécialisées, ce qui pose des difficultés au plan de la confidentialité des données et concernant les moyens de sécuriser leur accès (anonymisation et droit d'accès).

Monsieur Tristan SAVALLE
ADVENS

Docteur Alain FACON
Médecin Anesthésiste Réanimateur au CHRU de Lille et Chef de service adjoint du SAMU du Nord

Monsieur Guillaume DERAEDT
RSSI CHRU de Lille

La contribution de la fonction sécurité aux performances d'un service d'urgence: Le Service d'Aide Médicale d'Urgence du CHRU de Lille

Tristan SAVALLE

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).

Alain FACON

Le Docteur Alain FACON est Médecin Anesthésiste Réanimateur au CHRU de Lille et Chef de service adjoint du SAMU du Nord. Il est également Médecin responsable de l'unité de régulation médicale du SAMU et Médecin responsable du Centre d'Enseignement des Soins d'urgence du Nord. Il participe au pilotage du projet RAMUR (mise en place d'un réseau régional de l'Aide Médicale Urgente dans la Région Nord Pas de Calais) en collaboration avec le SAMU du Pas de Calais.

Guillaume DERAEDT

Voir page 4

Madame Chantal BOUDET
ARS Pays de Loire

Emergence de nouvelles missions : mise en place de référents sécurité des systèmes d'informations

Diplômée de l'université de Rennes I (DESS gestion des ressources humaines), Chantal Boudet est également titulaire d'un diplôme d'infirmière, de cadre de santé et de responsable qualité.
Après avoir occupé des fonctions d'infirmière et de cadre de santé pendant dix ans, Chantal Boudet prend la direction d'un établissement de santé en janvier 1997, et poursuivra ses fonctions de directrice jusqu'en 2006, date à laquelle elle entre comme chargée de mission efficience des organisations au sein des ARH d'Auvergne et de Rhône-Alpes.
A la création des ARS, en avril 2010, elle est nommée responsable du pôle professionnels de santé, qualité et performance de l'ARS Rhône-Alpes.
Depuis le 1er avril 2012, Chantal Boudet a rejoint l'Agence Régionale de Santé des Pays de la Loire au sein de laquelle elle occupe les fonctions d'adjointe au directeur de l'efficience de l'offre et de responsable du département des systèmes d'information partagés et de télémédecine.

Résumé de l'intervention :

L'amélioration de notre système de santé repose sur les systèmes d'information; c'est aujourd'hui un fait admis par l'ensemble de la communauté des acteurs de santé.
Leurs déploiements doivent s'opérer avec les garanties de disponibilité, d'intégrité, de confidentialité et de preuves optimales. C'est devenu un objectif bien identifié.
Comment atteindre un tel objectif dans un contexte très contraint par les ressources (budgétaires et humaines) ? L'attente des acteurs de terrain est forte. L'ARS Pays de la Loire a lancé une dynamique régionale en accompagnant les établissements de santé afin d'initier de manière opérationnelle et pérenne les processus métier indispensables à la prise en compte de la sécurité des systèmes d'information. La démarche, ainsi qu'une première évaluation de ces actions, feront l'objet de l'intervention.

Monsieur Jacques FOUCAULT

Consultant sénior - Directeur du pôle conseil de Tibco

Monsieur Philippe MATHON

Consultant/Architecte sécurité

Directeur technique sécurité de Tibco Services

Monsieur Yannick BOUCARD

Directeur du Pôle Santé chez Tibco

Et si l'Utilisateur était le meilleur anticorps contre la menace informatique

Jacques FOUCAULT

Après avec été Directeur Marketing marché de la santé chez Digital Equipment, Jacques a assuré la présidence de la société Capaciti, société spécialisée dans la sécurité des Systèmes d'information. Depuis 2012, il anime le pôle Conseil de Tibco et intervient principalement dans le monde hospitalier où il réalise des missions de schéma directeur informatique, d'analyse de risques et de gouvernance du SIH.

Auditeur ISO 19011, certifié ISO 27001 et Itil V3, Jacques est membre actif de l'Association Française de l'Audit et du Conseil Informatique (AFAI) et officie régulièrement au sein du Club de la Sécurité Informatique Français (CLUSIF).

Philippe MATHON

Philippe a commencé sa carrière en tant qu' Ingénieur-formateur et Consultant, partageant auprès des professionnels de l'informatique son expertise des systèmes et réseaux et de la mise en œuvre de solutions. Certifié auprès de nombreux éditeurs/constructeurs, il est également auteur de nombreux ouvrages sur les systèmes, le réseau et la sécurité, reconnus pour leurs qualités techniques et pédagogiques et traduits en plusieurs langues. C'est à l'aube des années 2000 qu'il se découvre une passion pour la sécurité des systèmes d'information, devenant un spécialiste de cette thématique. En tant que consultant sécurité, il fut amené à travailler avec tous types d'entreprises, du secteur privé comme public, de la PME aux entreprises du CAC40.

Ses missions traitent aussi bien d'intégration de solution à valeur ajoutée et d'assistance à maitrise d'ouvrage.

Et si l'Utilisateur était le meilleur anticorps contre la menace informatique

Yannick BOUCARD

Après avoir démarré sa carrière chez Digital Equipement Corporation à Nantes en tant qu'Ingénieur Commercial Services, Yannick BOUCARD a créé CAPACITI en 1999 et a occupé les postes de Directeur Commercial et Directeur Général. Cette société était spécialisée dans la sécurité des Systèmes d'Information. Il a rejoint le groupe TIBCO en 2012 en tant que directeur Régional. Fort de sa connaissance du secteur de la santé et de l'offre de services de TIBCO, début 2013, il crée le pôle santé qui a pour mission de développer l'empreinte de TIBCO auprès des établissements publics et privés de santé.

Moniteur de plongée, il s'intéresse de très près aux risques et à la manière de les traiter dans ce milieu hostile.

Résumé de la conférence :

Comment passer d'un utilisateur concerné par la menace informatique à un utilisateur impliqué dans le dispositif de prévention et de protection contre la menace ? Si un anticorps est une protéine complexe utilisée par le système immunitaire pour détecter et neutraliser les agents pathogènes, l'homme est un « actif » complexe du système d'information qui doit permettre de diminuer la potentialité des menaces et leurs impacts.

Cette conférence a pour objectif de vous présenter une méthode rationnelle pour faire passer vos utilisateurs concernés en utilisateurs impliqués et vous expliquer la manière de la mettre en œuvre facilement dans vos différents établissements.

Monsieur Didier ALAIN

Manager ANAP

Débat - RSSI Santé : « Un métier d'avenir »

Didier ALAIN est responsable du programme « Optimisation de l'usage des SI pour les établissements sanitaires et médicosociaux » à l'ANAP, et Maître de Conférence Associé à l'Université d'Angers, responsable du parcours de formation « Management des Systèmes d'Information en Santé ». De double formation en sciences humaines et systèmes d'information, il a travaillé près de 20 ans dans les hôpitaux (DIM, pilotage médico-économique, DSIO). A été pendant plusieurs années associé d'une entreprise d'édition de logiciel et a occupé des responsabilités nationales en lien avec les systèmes d'information dans une fédération hospitalière.

Résumé de l'intervention :

RSSI Santé : un métier d'avenir aux multiples facettes.

Faisant écho à la séquence RSSI, Didier ALAIN, Manager ANAP, anime le débat !

Comment répondre aux besoins avec les forces en présence ?

Quel avenir pour le métier de RSSI Santé ?

Quels leviers pour le développement d'une large acculturation à la sécurité des SI de Santé ?

Quels rôles et responsabilités pour les professionnels en charge du déploiement opérationnel des PSSI ?

Animée par Monsieur Vincent TRELY

Président de l'APSSIS

Monsieur Hervé SCHAUER

CEO HSC

Monsieur Benoit DULONDEL

ASINHPA

Table Ronde : Du bon usage des Normes ISO dans la Sécurité des SI de Santé

La sécurité des systèmes d'information est un sujet « actif » depuis plus de 20 ans. En particulier, des normes et des standards, des « bonnes pratiques » éprouvées sont mis à la disposition des professionnels pour les accompagner dans la mise en œuvre des PSSI.

Comment ces normes peuvent-elles aider les RSSI Santé ?
Quel usage efficient peut-on faire de ces bases de connaissances ?
Les Etablissements de Santé devront-ils un jour faire l'objet d'une certification ? Et si oui, dans quel but ?

Monsieur Olivier CARBONNEAUX
Directeur Santé - ARUBA NETWORKS

Une sécurité en strates commence par un contrôle des réseaux physiques, filaire et sans fil : NAC et BYOD, deux acronymes pour la même problématique ?

Olivier Carbonneaux , 52 ans, est Directeur Santé pour Aruba Networks France depuis septembre 2011. Auparavant, il démarre les activités de Trapeze Networks, une startup américaine dédiée aux architectures de mobilité en France de 2005 à 2010. Cette société est acquise par Juniper Networks fin 2010. C'est de 1995 à 2005, au sein de Symbol Technologies, qu'il débute son activité Santé, prenant en compte très tôt les impératifs de production de soins sur les infrastructures de communication.
Ancien rugbyman de niveau national, la volonté de travail en équipes et en écosystèmes est toujours là, et il cherche en permanence à fédérer les initiatives pour développer les bonnes pratiques. Il est impliqué en tant que partenaire des associations Athos et APSSIS, et est un ancien membre de Continua. A titre personnel, il est président d'une association promouvant l'Europe.

Résumé de l'intervention :

La sécurité d'accès aux réseaux, filaires et sans fil, est désormais au premier plan en 2014. Longtemps focalisé sur la sécurité des données via les connexions applicatives, le secteur commence à édicter des bonnes pratiques voir les récents guides édités par l'ASIP sur l'utilisation de la carte CPS pour ouvrir une session Microsoft ou la mise en place de réseaux wifi. Il est surtout intéressant de constater le bénéfice tangible pour les équipes réseau et système de disposer d'un réseau qui s'auto configure. Le déploiement du CHU Toulouse servira de fil conducteur pour illustrer ces deux aspects.

ARUBA networks

Monsieur Yves NORMAND

Consultant SSI, RSSI et CIL au sein du Syndicat Interhospitalier de Bretagne (S.I.B)

Monsieur Christian ESPIASSE

RSSI et CIL au GIP MiPih

Monsieur Vincent REGNAULT

Responsable du Système d'information et CIL du Centre Hospitalier du Pays des Hautes Falaises (Fécamp)

Editeurs et hébergeurs de logiciels traitant de données de santé, le contrat de confiance ! Les exigences des acteurs : le patient, l'acteur de santé, l'établissement, l'éditeur, l'hébergeur et l'Etat.

Yves NORMAND

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.

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, de sa pédagogie, Yves Normand intervient aujourd'hui pour les établissements de santé adhérents du SIB, pour les accompagner sur les thèmes de l'analyse des risques, audit SSI, PSSI, Charte, PCA/PRA, formation/sensibilisation,…

Il intervient également en tant que formateur SSI auprès de l'EHESP, l'UTC, Rennes 1, l'Université d'Angers, SHAM.

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).

Editeurs et hébergeurs de logiciels traitant de données de santé, le contrat de confiance ! Les exigences des acteurs : le patient, l'acteur de santé, l'établissement, l'éditeur, l'hébergeur et l'Etat.

Christian ESPIASSE

Il a pour mission d'assurer la sécurité des informations hébergées et tout particulièrement les données de santé à caractère personnel.

Il inscrit son action dans une stratégie d'acceptation s'appuyant principalement sur :

- Une pédagogie de simplification dont l'objectif est de changer l'image de contrainte austère dont souffre la sécurité et que véhiculent trop souvent les gourous, les spécialistes, la technique, les normes et le jargon…
- Une aide des institutions au travers des lois, décrets, règlements, échanges, audits, contrôles etc... Puissant argumentaire à disposition du RSSI pour convaincre sa direction et les résistances.

Pour Christian Espiasse le RSSI doit être discret et au service des acteurs de santé. La sécurité doit leur offrir un espace de confiance dans lequel ils pourront se consacrer à leur métier c'est-à-dire la prise en charge et le soin des patients.

Vincent REGNAULT

Fort d'une grande expérience des systèmes d'information en milieu hospitalier, il s'est spécialisé depuis quelques années sur les aspects conformité et respect des obligations légales.

Il intervient régulièrement dans les différents centres de formation de l'ANFH sur les sujets tels que l'impact sur l'informatisation de la production de soins.

Tout au long de l'année 2013, il coordonne le remplacement du système d'information du Centre Hospitalier de Fécamp en mode Info géré (Gestion Administrative du Patient, Application DIM, Gestion Economique et Financière, Gestion des Ressources Humaines, Mise en place du Dossier Patient Informatisé).

En septembre 2013, il décide de conserver son poste au Centre Hospitalier tout en créant le Groupement d'Intérêt Économique DATA SANTE et devenant ainsi Directeur Associé du GIE spécialiste de la conformité des systèmes d'information de santé.

Il a réalisé plusieurs écrits particulièrement sur la fonction mutualisée du Correspondant Informatique et Libertés.

Résumé de la conférence :

« Editeurs et hébergeurs de logiciels traitant de données de santé, le contrat de confiance ! Les exigences des acteurs : le patient, l'acteur de santé, l'établissement, l'éditeur, l'hébergeur et l'Etat. »

Choisir un dossier patient informatisé d'un éditeur avec une infogérance applicative, et choisir un hébergeur de données de santé à caractère personnel agréé avec une infogérance technique, tel peut être le pari ambitieux d'un établissement de santé.

Au-delà des promesses de davantage de qualité, de sécurité et de moindre coût, cette démarche est l'occasion de mettre en lumière les attentes des professionnels de santé, utilisateurs de l'application, mais aussi de la mise en œuvre des politiques institutionnelles et des règlementations applicables.

Trois acteurs essentiels du projet, l'établissement, l'éditeur et l'hébergeur exposeront les attentes, les contraintes, les exigences que chacun est tenu de respecter.

Ils tenteront de démontrer que les relations et les échanges entre institutions, établissement, personnel médical, éditeurs, hébergeurs, concourent à davantage de qualité de sécurité et de confiance en l'outil informatique. Le patient doit en être le bénéficiaire.

Cette conférence est animée par :

- Le CHI du Pays des hautes falaises, Fécamp
- Le MIPIH et le SIB, représentant l'Asinhpa (Association des structures d'informatique hospitalière publique autonomes), au travers de son groupe sécurité (regroupant CPage, MIPIH, SIB, SIIH, SIL).

Monsieur Serge BERNARD
Directeur Général CH ANNECY

Le SI de demain et sa sécurité, au carrefour du parcours Patient et des Territoires

Observateur et acteur engagé du monde hospitalier, Serge BERNARD dispose d'une expertise reconnue dans l'apport du numérique et des technologies innovantes au sein de l'Hôpital.
Qu'il s'agisse de e-learning, de distribution robotisée du médicament ou du déploiement d'outils plus élaborés au sein des territoires de santé, il s'attache à concilier le développement des usages et l'action des professionnels dans une vision de médecine connectée facilitant «le travailler ensemble».
A la tête d'une Communauté Hospitalière de Territoire (CHT) récemment mise en place en Haute-Savoie, il gère le regroupement des centres hospitaliers d'Annecy et de Saint-Julien en Genevois. Cette fusion se traduit par la création du nouveau Centre Hospitalier Annecy Genevois (CHANGE).
En charge de la Communauté hospitalière de territoire (CHT) récemment créée en Haute Savoie, Serge BERNARD est également responsable de la fusion entre les hôpitaux d'Annecy et de Saint Julien en Genevois, qui a amené à la création du Centre hospitalier Annecy Genevois le 1er janvier 2014, offrant des soins de qualité sur un bassin de vie allant de Genève (Suisse) aux frontières du département de l'Isère, pour environ 3 millions de personnes, proposant une technologie de pointe pour en faire une des toutes premières références hospitalières en Rhône-Alpes.
Attaché à des méthodes de «team management», il exerce également des fonctions au sein des instances de concertations régionales, CRSA et CSOS.

Résumé de l'intervention :

L'ère du numérique s'installe progressivement dans le champ de la santé, au point d'y occuper une place de plus en plus grande, avec un contenu prometteur, riche d'innovations. Ce mouvement se double d'une accélération indiscutable, qui impacte le citoyen de son domicile à son lieu de travail sans oublier l'émergence d'une nouvelle économie.
Les politiques publiques, nationales et régionales multiplient les initiatives dynamisant une pépinière d'entreprises, qui du cinéma d'animation à la robotique en passant par les applications numériques de toutes natures participent de l'excellence française. Des segments particuliers apparaissent notamment dans le domaine médical, créant de la valeur et opérant un lien fort entre les mondes scientifique et industriel.
On observe dans un tel contexte, que les hôpitaux tant publics que privés, n'ont pas à souffrir d'un quelconque retard vis-à-vis de leurs homologues européens ou américains.
Ces données - somme toute - rassurantes ne doivent pas masquer quelques insuffisances ou difficultés structurelles qui ne sont pas de bons exemples de la singularité française, voire de l'exception française. Il convient énergiquement de bien les appréhender et les faire évoluer.
Notre intervention visera à mieux identifier et ouvrir à nos réflexions les marges de progression qui existent aussi bien à l'intérieur de nos organisations qu'à l'extérieur.
C'est l'enjeu d'une évolution vers une médecine connectée, plus efficiente avec un espace territorial conciliant une réponse de proximité à l'organisation d'un parcours de santé personnalisé.
La sécurité des SI est une des clés de cette profonde mutation.
La contribution et l'engagement des différents acteurs sont aussi des déterminants essentiels, qui se doivent d'être réinterrogés, afin de relever ces nouveaux défis.

Monsieur Bernard BENSADOUN
Directeur Général Délégué
Groupe Hospitalier Privé VEDICI - NANTES

Informatique de Santé : en finir avec l'hypocrisie !

Bernard Bensadoun est Ingénieur de formation. Après un parcours de dix ans dans l'industrie biomédicale, il intègre le CHU de Nantes, en tant que Directeur adjoint en charge du médicotechnique. Il poursuit sa carrière au Centre de Lutte contre le Cancer René Gauducheau de Nantes, où il prend la responsabilité des secteurs biomédicaux, achats et communication avant de devenir Directeur Général Adjoint du Centre. En 2009, il intègre l'ECHO, établissements multi-sites, référent pour la dialyse sur les régions Bretagne et pays de la Loire, dont il prend la Direction Générale.
Bernard Bensadoun est actuellement Directeur Général Délégué du groupe Vedici, pour lequel il gère quatre établissements du secteur sanitaire, à Nantes.
Au travers de ses différentes expériences professionnelles, qui lui ont permis d'évoluer dans les principaux modes de structuration de l'offre de soins (Public/ ESPIC/ Privé commercial - établissement polyvalent, mono disciplinaire, multi sites...) Bernard Bensadoun a fait le constat d'une uniformité des attentes des professionnels de soins, fondées sur l'échange de données et l'accessibilité simple aux informations pertinentes pour les prises en charges. En parallèle, il observe une complexité exagérée de l'offre et une rigidité législative décourageante.
C'est cette vision des systèmes d'information en santé, qu'il a prévu d'aborder au cours de son intervention.

Résumé de l'intervention :

Dans le Monde de la santé, parler informatique rime très vite avec complexité. On nous excipe successivement la confidentialité des données, leur intégrité et la protection des patients, quand on ne mets pas en avant les volumes astronomiques des données transmises (explorations médico-techniques – Imagerie..). Les normes sont légions et au bout du compte, Directions des Systèmes d'Information et professionnels de santé finissent par se décourager ou par monter des systèmes totalement propriétaires et peu interopérables…
Tout cela est-il bien raisonnable, quand on regarde d'autres secteurs d'activité qui ont réussi leur mutation vers le «tout communicant», malgré des contraintes tout aussi importantes.
La banques, la justice, les jeux vidéo en ligne, et le téléchargement de films ont réglé depuis bien longtemps les aspects intégrité / confidentialité et volume de chargement.
Pourquoi, le secteur de la santé n'arrive-t-il pas à en faire de même ? Quels sont les freins ? Y-a-t-il des intérêts qui neutralisent le système ?
Voilà quelques-uns des aspects qui seront abordés dans l'intervention de Bernard Bensadoun.

Monsieur Philippe ROUSSEL
Directeur d'Hôpital
Vice-Président du CNEH

Débat :
Du rôle du Directeur Général dans la Politique de Sécurité des Etablissements de Santé

Philippe ROUSSEL est Vice-Président du Centre National de l'Expertise Hospitalière. Il est Référent des formations SI et IT, et Responsable des missions d'études HIMSS et RSNA. Directeur d'hôpital, ancien élève de l'EHESP, il a dirigé notamment le Centre hospitalier du Mans, l'Hôpital Marie-Lannelongue, et des hôpitaux mutualistes.

Résumé de la conférence :

Tout le monde en est conscient, tout le monde le dit et l'écrit : pas de Politique de Sécurité des Systèmes d'Information sans une implication forte des Directions Générales !
Quel est le rôle de la DG dans la mise en œuvre d'une PSSI ?
Comment la DG doit accompagner / supporter le RSSI ?
Pourquoi une PSSI est un projet d'établissement et non pas une liste de considérations techniques dédiée à la Direction Informatique ?
Philippe ROUSSEL, Directeur d'Hôpital, anime le débat.