L'hôpital de demain, *vu par* Guy Vallancien

Fondateur et président de la Convention on Health Analysis and Management (Cham), de même que de l'École européenne de chirurgie, également membre de l'Académie nationale de médecine et de chirurgie, Guy Vallancien a le regard qui porte loin. Le chirurgien urologue observe avec bienveillance l'arrivée du numérique à l'hôpital et perçoit les bouleversements profonds qui l'accompagnent. Il répond aux questions de DSIH sur les thèmes qui seront débattus à l'occasion du prochain Congrès de l'Apssis*, où vous pourrez venir l'écouter.

Dans son dernier livre, *La Médecine sans médecin ? Le numérique au service du malade*, Guy Vallancien livre sa réflexion sur la mutation entamée avec l'invention du stéthoscope, qui aujourd'hui s'accélère. Pour lui, le médecin de demain, délivré de ses tâches administratives et des actes que pourront accomplir les machines, retrouvera le temps de l'écoute et de l'attention pour chacun de ses patients. Le médecin de demain sera un médecin humaniste.
Nous l'avons interrogé sur le fonctionnement de l'hôpital numérique dont il prédit l'avènement.

À quoi ressemblera selon vous l'hôpital de demain ?
D'abord, il faudra moins d'hôpitaux de manière à concentrer les moyens humains et matériels sur des plateformes ayant toutes les possibilités d'action. Ensuite, ces hôpitaux devront être modulables. Les technologies évoluent constamment, et si l'on ne modifie pas les murs, l'architecture viendra très vite nous contraindre. Pour l'hôpital Georges-Pompidou, par exemple, il aura fallu attendre 20 ans entre la pose de la première pierre et l'ouverture de l'établissement. Entretemps, les scanners ont augmenté de volume et les portes du service de radiologie étaient devenues trop petites. Il a fallu les remplacer.
Les hôpitaux devront s'adapter en permanence à l'arrivée des nouvelles technologies. On peut imaginer un système de cloisons dont on peut modifier l'agencement pour former des pièces plus ou moins grandes. Par ailleurs, l'hôpital de demain sera connecté à un point inimaginable ! Les prises de rendez-vous et les inscriptions pour une hospitalisation se feront par Internet. Les files d'attente interminables seront ainsi épargnées aux patients.

« Des ingénieurs opérateurs assureront des opérations chirurgicales dans des domaines très spécialisés. »

La télémédecine entrera en force dans ces hôpitaux connectés avec les réseaux de soins de ville, les médecins généralistes et les familles. Enfin, il faudra un système d'évaluation des pratiques hospitalières par les malades. Des évaluations seront réalisées de chez eux à l'aide de questionnaires qui seront ensuite envoyés à un logiciel de traitement des données statistiques afin d'apprécier les améliorations possibles. L'hôpital de demain, c'est connexion tous azimuts, informatisation, évaluation et amélioration !

Quelle place occuperont l'ingénieur, l'informaticien et le *data scientist* ?
Ces métiers auront un rôle clé dans l'hôpital numérique. Ils trouveront leur place dans les blocs opératoires, sur les plateaux techniques lourds, en réanimation... Partout où la technicité sera nécessaire. L'échange entre le personnel soignant et les ingénieurs permettra d'améliorer en permanence le matériel et les outils informatiques qui nous aident à mieux faire notre métier. Des ingénieurs opérateurs assureront aussi sans doute, entièrement ou partiellement, des opérations, dans des domaines très spécialisés. Ils le feront grâce aux outils les plus sophistiqués qu'ils auront eux-mêmes mis au point avec d'autres ingénieurs, ceux que l'on trouve dans les laboratoires de recherche ou dans l'industrie. Les informaticiens aideront à nous organiser dans cet hôpital de plus en plus informatisé. Quant aux *data scientists*, ils auront un travail de relations humaines, de communication et d'écoute afin de répondre aux demandes des praticiens qui souhaitent évaluer leur pratique. Les datas, ces milliards de données, sont inutiles si l'on ne se pose pas la bonne question pour leur donner du sens. Les *data scientists* nous aideront à mieux définir nos questions pour mieux y répondre.

Dans cet hôpital numérique, comment seront protégées les données des patients ?
Les moyens informatiques pour protéger ces données existent. On pourra imiter ce que font les banques pour protéger les dossiers de leurs clients. Tous les domaines sont touchés par le piratage. La santé n'échappe pas non plus aux obstacles inhérents au respect de la confidentialité des données. C'est à nous de mettre en place les pare-feu et les solutions informatiques nécessaires. Mais le travail se fera au jour le jour. Les malades ne sont pas très inquiets de la protection de leurs données. Ce qu'ils veulent, c'est être bien traités. On craint que les assureurs ne s'emparent des données des patients, mais c'est déjà le cas. On sait très bien que les gens qui fument paieront leurs assurances plus cher. Je ne vois pas comment l'on pourra faire autrement. On fait beaucoup de bruit autour de la protection des données, mais l'évolution inéluctable du tsunami informatique ne doit pas être ralentie pour autant.

■ **Propos recueillis par Oriane Dioux**

**Association pour la promotion de la sécurité des systèmes d'information de santé. Le congrès se déroulera au Mans, entre le 4 et le 6 avril. http://www.apssis.com/#/2016-agenda-activites/504573406*

Damien Bancal, traqueur de pirates

Les failles des systèmes informatiques, c'est son dada. Depuis 25 ans, Damien Bancal, journaliste indépendant, a mis sa passion pour l'informatique au profit de la lutte contre la cybercriminalité. Il sera au Congrès de l'Apssis*. *DSIH* l'a rencontré.

Sans relâche, Damien Bancal traque les failles dans les systèmes informatiques et avertit leurs propriétaires de leur existence ou de l'intrusion de pirates. Ces découvertes, il les relate sur son site Web, ***zataz.com***, conçu pour le grand public afin de montrer que le piratage, « *ça n'arrive pas qu'aux autres* ». Ce site se décline sous une version plus professionnelle, destinée aux PME et PMI : *datasecuritybreach.fr*. Le journaliste spécialiste de la cybercriminalité intervient aussi, sous une casquette d'enseignant, pour la licence professionnelle de « collaborateur pour la défense et l'anti-intrusion des systèmes informatiques » de l'université de Valenciennes sur le site de Maubeuge. Il apprend aux futurs informaticiens à réfléchir comme des pirates « *car le meilleur moyen de se protéger, c'est de penser comme eux* ».

60 000 entreprises et administrations alertées en 18 ans

Dès ses débuts, le journaliste voit dans le domaine de la sécurité informatique un sujet porteur. Il ne s'est pas trompé. Depuis le lancement de ***zataz.com***, qui a soufflé ses 18 bougies l'année dernière, il peut se féliciter d'avoir aidé bénévolement plus de 60 000 entreprises et administrations en repérant des failles, soit directement, soit grâce au concours des internautes qui les lui rapportent via le protocole d'alerte de son site.
Et le volume de travail gonfle avec les années. Entre 2014 et 2015, il enregistre une hausse de 42 % des remontées aux entreprises. « *C'est fou ! Je n'en ai jamais eu autant. Je reçois une dizaine d'informations par semaine sur des bases de données piratées.* »
Sans surprise, la santé n'est pas épargnée : rien qu'en 2015, plus de 400 pharmacies, deux ordres de professionnels de la santé et près de 300 cliniques et hôpitaux ont été piratés.

Les laboratoires de biologie médicale sont aussi de bonnes cibles. « *Un laboratoire s'est retrouvé en proie à un chantage numérique organisé par le groupe de pirates Rex Mundi qui a volé l'intégralité de sa base de données comprenant les noms, prénoms et identifiants des patients. Les pirates ont imposé une rançon de 20 000 euros et menacé de tout diffuser sur Internet si le laboratoire ne sortait pas les sous. Ce type d'attaque permet à n'importe qui de consulter les résultats d'analyse de sang des patients. Côté sécurité, c'est un peu léger !* »

> « LE MEILLEUR MOYEN DE SE PROTÉGER, C'EST DE PENSER COMME LES PIRATES ! »

Le Black Market pour monnayer les données de santé

Ces données, parfois également extorquées sur les serveurs des cliniques et des hôpitaux, se monnayent sur le Black Market, le fameux marché noir de l'Internet. « *J'ai rencontré sur la toile des pirates qui les ont revendues pour 200 euros. L'identité des patients est largement suffisante pour monter de jolies escroqueries. Comme envoyer par mail des phishings ciblés au nom de la Caisse d'allocations familiales, par exemple, et récupérer les données bancaires. Sans oublier l'usurpation d'identité, qui devient facile avec un numéro de sécurité sociale !* »

Sur son site, Damien Bancal a aussi rapporté les infiltrations, nombreuses en 2015, de sites Internet ayant pignon sur rue (comme la Haute Autorité de santé) afin d'y insérer des liens vers de fausses pharmacies en ligne ou des boutiques de contrefaçon de médicaments.

Autre sujet d'inquiétude pour le spécialiste : les montres et objets connectés au service de la santé. « *Apple va sortir une montre qui vérifiera entre autres la glycémie. Une mine d'informations sera récoltée à notre poignet. Or il est très clairement annoncé que ces données seront stockées, le plus souvent dans un pays étranger, sur des serveurs et des disques durs que nous ne contrôlons pas. Que vont-elles devenir ?* »
Selon lui, il est donc plus que temps pour la médecine de se protéger : « *Face à des professionnels de la malveillance qui ont compris qu'il y avait beaucoup d'argent à empocher, il est important que le secteur médical sécurise les données ultrasensibles qu'il a en main. L'informatique, c'est nous qui devons la maîtriser. Le problème est que c'est elle qui nous maîtrise, de plus en plus.* »

Oriane Dioux

**Association pour la promotion de la sécurité des systèmes d'information de santé. Le congrès se déroulera au Mans, entre le 4 et le 6 avril. http://www.apssis.com/#/2016-agenda-activites/504573406*

Ça n'arrive pas qu'aux autres !

Philippe Loudenot était invité par Alsace e-santé à porter un regard global sur la vulnérabilité des systèmes d'information en santé. Le fonctionnaire de sécurité des systèmes d'information (FSSI) auprès des ministères sociaux n'a pas manqué de suggérer des pistes pour y remédier

Pour **Philippe Loudenot,** fonctionnaire de sécurité des systèmes d'information (FSSI) auprès des ministères sociaux, « *il n'y a rien de honteux à s'être fait pirater. S'en rendre compte est déjà la marque d'un système géré.* »

Appliquée à la santé, la sécurité soulève des questions complexes et suppose, comme dans d'autres domaines, des règles de bon sens. Tel était le leitmotiv de Philippe Loudenot, FSSI auprès des ministères sociaux, livrant à son auditoire rassemblé à Strasbourg, le 6 octobre dernier pour une Journée « Innovation & Sécurité en santé numérique* », des constats très inquiétants, voire un tantinet alarmistes. « *La sécurité est toujours vue par l'utilisateur comme un frein. C'est au contraire un facteur d'innovation, un outil qui permettrait de valoriser un organisme à la condition de la prendre en compte dès le départ* », a-t-il insisté avant d'ajouter : « *Il faut cesser de faire du "spécifique santé" en matière de sécurité. En réalité, il s'agit des mêmes problématiques que pour d'autres secteurs ; seules les obligations de résultat changent.* »

> « *On peut prendre le contrôle total d'un établissement de santé en une matinée.* »

À cet effet, le Référentiel général de sécurité (RGS) exige d'analyser en amont les risques spécifiques à chaque métier. Les risques résiduels doivent également être identifiés afin de mettre en œuvre les moyens les plus adéquats en fonction du besoin. Mais, comme le déplore Philippe Loudenot, ce travail préalable est rarement effectué. Concernant la politique de sécurité des systèmes d'information pour les ministères chargés des Affaires sociales, il souligne qu'il existe un « *document consensuel qui permet de mettre en place une gouvernance de la sécurité des systèmes d'information au sein des établissements de santé* ».

Des mots de passe visibles à l'accueil

En matière de respect des règles, les professionnels de santé, et de façon plus globale les établissements de santé, ne sont pas toujours bons élèves. Le conférencier a rappelé que la sécurité ne se rapporte d'ailleurs pas seulement à Internet, citant l'exemple de documents papier non protégés, rangés à proximité d'un photocopieur libre d'accès, ou le simple fait de discuter de cas cliniques devant la machine à café... Parfois, le bon sens pratique permet donc d'éviter des déconvenues.

Les chiffres donnés par le FSSI sont explicites : depuis le 1er janvier 2015, sur toutes les attaques visant des établissements de santé, 66 % correspondaient à de « simples » incidents et 34 % à de véritables attaques internes ou externes. Plus inquiétant : parmi ces attaques, seules 11 % ont été bloquées.

En place depuis près d'un an, Philippe Loudenot a pris le parti d'envoyer systématiquement des alertes aux établissements de santé en les avertissant des attaques majeures en cours.

Quelques exemples supplémentaires permettent de mieux comprendre certaines vulnérabilités pesant sur les systèmes d'information de santé : déviances par rapport aux protocoles, mauvaise organisation, codes d'accès aux intranets affichés à l'accueil, systèmes d'exploitation obsolètes et parfois non mis à jour (Windows XP, voire antérieurs), absence de maintien en conditions de sécurité, téléchargements de films en torrent sur les serveurs des établissements, visite de sites d'« anatomie comparée » (en clair, classés X !).

Mais il existe aussi des comportements « irresponsables » aux yeux du spécialiste : « *Le fait de partager des données personnelles de patients sur Facebook relève de l'inconscience, tout comme celui de s'inscrire sur des sites de rencontres extraconjugales avec son adresse professionnelle et le mot de passe associé.* » En l'espèce, des adresses de messagerie relevant d'établissements de santé ou... du ministère !

Inclure les acteurs du biomédical

Outre la vigilance, la pédagogie au sein des équipes et le bon sens, Philippe Loudenot plaide pour la réalisation dans les établissements d'une cartographie des systèmes d'information de santé incluant notamment le biomédical et les systèmes de gestion centralisés ou de bâtiment. Autre piste : ajouter des clauses de sécurité des systèmes d'information de santé lors des procédures d'achat. « *Les mises à jour des environnements informatiques doivent être réalisées et il faut à tout prix éviter le "tout ce qui n'est pas explicitement interdit est autorisé".* » L'idée étant une nouvelle fois que les enjeux de la sécurité ne doivent pas être considérés comme un centre de coût mais comme un outil de création de valeur.

« *Il n'y a rien de honteux à s'être fait pirater, a conclu le conférencier. S'en rendre compte est déjà la marque d'un système géré. L'important est de faire remonter l'information pour rendre service à la communauté, par le biais de la chaîne de sécurité [ssi@sg.social.gouv.fr]. Il en va parfois de la santé, voire de la vie des patients !* »

■ Guillaume Bouvy-Vuchkan

*https://www.alsace-esante.fr/journee-innovation-securite-en-sante-numerique-une-1ere-rencontre-reussie-pour-les-decideurs-en

Rendez-vous

Vous retrouverez Philippe Loudenot au programme du Congrès Apssis (Association pour la promotion de la sécurité des systèmes d'information de santé) au Mans, le 4 avril prochain.

http://www.apssis.com/2016-agenda-activites/504573406