Informatique de santé et cybersécurité : prospectives 2037

Cédric CARTAU
RSSI et DPO
CHU DE NANTES et GHT44

Attaques cyber des hôpitaux, crise COVID, informatisation des soins, objets connectés : autant d'évolutions – ou de révolutions – qui se déroulent sous nos yeux, pas au même rythme ni à la même échelle de temps, et qui vont bouleverser le paysage de la santé numérique dans les prochaines décennies. Petite tentative prospective sans prétention.

Les prospectives en informatique constituent un excellent exercice de voltige avec chute assurée – n'était-ce pas cet ancien président d'IBM qui pensait qu'il n'y avait pas besoin dans le monde de plus de cinq ordinateurs, ou de Bill Gates qui affirmait en son temps qu'avec 640 Ko de RAM il y en avait bien assez ? Mais même hasardeux, l'exercice n'en reste pas moins grisant, et nous proposons de phosphorer à ce que seront les SI de santé dans 15 ans, avec leur corollaire cybersécurité.

En 2037, nous aurons changé au moins quatre fois de Président de la République, au moins autant de fois de premiers ministres sans parler du ministre de la santé, et sans parler des modifications réglementaires qui continueront de s'empiler. Avant de se projeter dans 17 ans, prenons un moment pour regarder 17 ans en arrière : il y avait quoi en 2003 ?

Back to the Future

En 2003, le principal enjeu de la SSI est d'avoir un AV à jour, les ingénieurs systèmes sont essentiellement préoccupés par l'efficacité des filtres antispam. La DMZ compte rarement plus de dix @IP (en 2003 au CHU de REIMS il y avait 5 @IP dans la DMZ), seul un CHU a nommé un RSSI (Strasbourg).

Presque aucun établissement de santé n'a dédoublé son datacenter, et la préoccupation majeure de la messagerie est d'attribuer une BAL à chaque agent. D'ailleurs une bonne partie des équipes de direction n'ont pas de BAL et n'en voient même pas l'utilité : suggérer qu'un DG puisse taper lui-même un mail peut envoyer un informaticien directement au goulag.

Le Wifi n'est quasiment jamais déployé, sauf exception notable, quant à la sauvegarde, elle est faite sur bande, les bandes sont changées chaque jour par des pupitreurs, quelquefois les bandes sont déplacées pour être mises en sécurité. Le firewall est souvent un équipement en rack dont peu de gens s'occupent, le nombre de PC d'un établissement est en général égal à son nombre de lits, les smartphones n'existent pas, le dernier gadget à la mode est le Palm voire le Blackberry pour les plus hypes.

Les connexions ADSL commencent à peine à se démocratiser auprès du grand public (à peine 1 million d'abonnés en 2002), le téléchargement illégal est un concept inexistant, autant que Youtube et Dailymotion. Facebook n'existe pas encore.

Les audits techniques de sécurité sont inconnus, les audits organisationnels sont rarissimes, sauf conflit patent entre la DSI et la DG et d'ailleurs la norme ISO 27 001 est inconnue (elle sera reprise de la BSI par l'ISO en 2005).

L'informatique est essentiellement administrative : le cœur de métier (unités de soins) est peu équipé : le plan hôpital 2007… ne sera lancé qu'en 2004.

Une panne de 72 heures de l'informatique d'un établissement n'impacte pas le processus de soins, le hacker le plus dangereux dont on ait souvenir est un adolescent qui s'amuse à pirater le PABX (Kevin Mitnick).

Le seul organisme étatique traitant de question de sécurité est le GMSIH. L'ASIP santé, avec son rôle plus opérationnel, n'est créée qu'en 2009.

Les problématiques d'habilitation n'existent pas : Enron, Jérôme Kerviel et Bâle 2 ne sont pas encore arrivés.

Quand on demande à un informaticien de disserter sur la sécurité informatique, il pense à la longueur des mots de passe et au compte admin système du contrôleur AD (vécu).

Quand on demande à un DSI ce qu'il pense de la sécurité informatique, il pense à la panne du serveur de paye (vécu aussi).

Quand on demande à un DG ce qu'il pense de la sécurité informatique, il ne pense à rien.

Mais tout ça, c'était avant.

Prospectives : évolution de l'informatique de santé.

Alors que la médecine n'a connu que trois révolutions majeures en 2 000 ans (rupture de paradigme au sens kantien du terme : les antibiotiques, l'anesthésie et l'imagerie médicale), au moins six tendances vont se dégager dans les prochaines décennies.

Première tendance lourde : la génomique.

Le séquençage du génome est une réalité depuis plus de 10 ans, et tout un chacun peut se faire analyser son ADN sur des sites tels 23andme.com (avec certes des interrogations sur le devenir de ses données). L'analyse du génome va devenir courante, telles les scènes du film d'anticipation « Bienvenue à Gattaca » : avant toute prise en charge médicale, le génome sera séquencé et cet acte sera aussi banal que peu couteux.

Deuxième tendance : l'intervention directement sur le génome, avec en toile de fond la médecine personnalisée : un médicament sera conçu et fabriqué pour une personne précise, dans un contexte précis et pour un objectif thérapeutique précis.

Troisième tendance lourde : le recours de plus en plus banal au transhumanisme, modification volontaire du corps humain soit par implants, soit directement par modification du génome. Des outils existent déjà, tel le CRISPR-CAS9.

Quatrième tendance, conséquence des deux précédentes : la notion de fontaine de jouvence. Le recours à l'acte médical ne se limitera plus au traitement d'une pathologie, mais va s'étendre à la notion de bien-être. La chirurgie esthétique, inventée à la fin de la première Guerre Mondiale pour réparer les « gueules cassées » est maintenant utilisée à des fins essentiellement esthétiques.

Cinquième tendance : le self quantifying permanent. Les objets connectés tels les montres ou les smartphones permettent déjà de mesurer en temps réel quantité de paramètres telle l'activité physique, le rythme cardiaque, le taux de sucre, etc.

Sixième tendance : la télémédecine généralisée. Plus de 30 % d'actes seront réalisés hors présentiel patient/médecin. La crise sanitaire COVID19 a été un

accélérateur foudroyant de ce type de pratiques, et les pays nordiques (Suède et Norvège entre autres) sont très en avance sur nous, configuration géographique et climat obligent.

Quels outils en face de ces besoins ?

Face à ces tendances lourdes, les DSI devront mettre en place des démarches, des infrastructures, des outils, des compétences.

Vers HIMSS niveau 7

La France accuse un retard considérable dans la maturité des SI des établissements de santé, dont la majeure partie de dépasse pas le niveau 3 ou 4 sur une échelle HIMSS qui va de 1 à 7. Le niveau 7 est la cible, il faudra au bas mot quinze ans pour le voir se généraliser et cela nécessitera au minimum un triplement des budgets SI.

Le Big Data et les centres de calcul

Ce niveau 7 nécessite de monter des infrastructures de stockage et d'analyse. Le Health Data Hub est une réponse à certains besoins mais ne couvre pas ou peu le champ du soin aigu. Les établissements de santé vont devoir mettre en production des Cliniques de données, de consultation des données d'ambulatoire des données, tel ce qui a été mis en place par le Pr Pierre-Antoine GOURRAUD au CHU de NANTES avec la société WEDATA.

Explosion des IoT : le self quantifying va se traduire par une explosion des gadgets grands publics, l'IoT verra la même courbe dans le domaine professionnel. Les actes médicaux répétitifs (prendre la tension, peser le patient, etc.) peuvent déjà être pour partie réalisés et automatisés.

Forte technicisation des actes médicaux : en 2030 les chirurgiens n'opèreront plus avec leurs mains : ils piloteront des joysticks.

Dispositifs médicaux implantés de nouvelle génération

Prothèses, humains augmentés, capteurs, pilules connectées, etc. : autant d'objet qui vont devenir banals, que ce soit pour suivre une pathologie chronique, pour surveiller un patient au bloc ou en réanimation.

Porosité des réseaux informatiques

Si le BYOD, qui avait le vent en poupe il y a à peine cinq ans, a disparu des écrans radars des fournisseurs. L'ouverture massive des réseaux (LAN) des établissements de santé vont faire que « dedans » ou « dehors » du LAN ne va plus avoir le même sens qu'aujourd'hui. Le débat Cloud / On Premise n'aura plus de sens : les infrastructures IT seront mixtes, réparties à la fois sur les datacenters internes de l'établissement et sur un ou plusieurs Cloud publics ou privés. L'interopérabilité technique ou sémantique sera la principale, sinon la seule valeur ajoutée d'une DSI.

Ouverture massive des DPI

En 2020 il est possible de consulter ses comptes bancaires, son abonnement à Fnac ou ses livraisons Chronopost directement sur son smartphone, mais toujours pas son dossier médical auprès de l'établissement public ou privé de la ville. Cet anachronisme va disparaître.

Nouveaux matériaux

Impression 3D, matériaux composites et nanomatériaux : certains éléments – par exemple les prothèses de hanches – seront « imprimés » en 3D quelques heures avant l'opération.

Vers la certification ISO comme centre de gravité

Pendant des décennies, la valeur ajoutée d'une DSI – son centre de gravité – aura été sa capacité à maîtriser des technologies pointues : serveurs, stockage,

virtualisation. À ces compétences s'est progressivement ajoutée depuis les années 1990 la maîtrise du fonctionnel métier. Dans la prochaine décennie, les DSI seront certifiées – ISO 9000, ITIL, ISO 27001, etc. – ou devront tirer le rideau : le centre de gravité passera alors sur la maîtrise des processus et de la qualité de services.

Quelles nouvelles menaces ?

Mais face à ces enjeux de santé et à l'évolution des outils qui les supportent, apparaîtront des nouvelles menaces.

Professionnalisation de la malveillance IT…

Il n'est de secret pour personne que les état dits « voyous » constituent une des premières sources d'attaque. Et dans le même temps on a des STUXNET ou des FLAME conçus par nos « amis » américains.

…et pourtant toujours l'adolescent dans son garage.

La cyber est l'arme du pauvre, et c'est justement ce qui la rend dangereuse.

De l'allégorie des missionnaires dans la savane pour adapter sa stratégie de cyber résilience

Deux missionnaires dans la savane tombent nez à nez avec un lion, et se mettent à courir à toutes jambes. L'un demande à son copain : « tu crois que l'on arrivera à courir plus vite que le lion ? ». L'autre lui répond : « pas du tout, mais je ne cherche pas à courir plus vite que le lion, je cherche juste à courir plus vite que toi ».

Généralisation des 0-Day

Conséquence de la professionnalisation, le marché des 0-Day est mondial, nul n'est à l'abri. Ce marché s'organise, avec ses producteurs, ses brokers, ses revendeurs.

Multiplication des périphériques

Et ce sont tous potentiellement des sources de vulnérabilité et donc d'attaque. Il y a vingt ans, il n'y avait que des PC. Maintenant il y a des PC, des PC portables, des tablettes, des smartphones, des photocopieurs multifonction, des caméra IP connectées, etc. Si quelqu'un a réussi à patcher ses caméra IP, je veux bien qu'il m'explique comment il s'y est pris.

Multiplication des attaques en déni/usurpation d'identité

Si la grande mode des années 2000 était les attaques en déni de service (DOS, dDOS, etc.), cela rapporte clairement beaucoup plus de réaliser des attaques en déni ou usurpation d'identité : fraude au président, détournement de factures fournisseur, etc.

Nouvel or noir que représentent les bases de données médicales : les bases de données médicales deviennent une cible pour la connaissance médicale et statistique qu'elles représentent et pas pour la valeur marchande du dossier de Mme DUPONT.

Multiplication des procédures juridiques

Les établissements vont devoir faire la preuve par la trace, avec forte contraintes sur les systèmes de traçabilité interne avec valeur probante.

Composants IoT frelatés

Il va être nécessaire de déployer à l'échelon national ou européen une base d'IoT-vigilance, au même titre qu'il existe une pharmaco-vigilance.

Disparition de la téléphonie, du biomed, de la logistique en tant que domaines « à part ».

En 2037, on aura bien du mal à dire si un serveur abrite une application médicale, biomédicale, téléphonie, etc.

Quelles prospectives pour la sécurité des SI de santé ?

Dans certains domaines il va falloir opérer des changements de paradigmes radicaux, car les outils, les processus et les compétences actuels ne vont plus être suffisants ou tout simplement appropriés.

Il va falloir dans un premier temps acter la fin des outils mastodontes : nécessité d'agilité dans le déploiement d'outils légers, peu chers et pointus. Également intégrer la problématique IoT, notamment dans le domaine des prothèses, des dispositifs médicaux, etc.

Il va falloir également prendre en compte les menaces 0-Day et APT, l'infrastructure de protection antivirale va devoir se complexifier et intégrer de l'analyse en mode comportemental à tous les niveaux du modèle OSI.

L'enjeu des établissements de santé sera d'amener la protection au même niveau que les banques et les telco, et avec la migration d'une partie du SI dans le Cloud, généraliser les solutions de chiffrement.

Il faudra aussi intégrer l'explosion des terminaux : en 2020 il y aura plus de terminaux que d'agents, en 2030 le rapport sera passé à 2 pour 1 voire 3 pour 1. Les smartphones, les MFP et autres caméra IP constituent la prochaine plateforme privilégiée d'attaques.

Il va être nécessaire de déployer la traçabilité généralisée, analyser régulièrement les traces par déploiement d'un SIEM, d'un SOC ou toute technologie qui sera en cours à cette date.

Il va être nécessaire de revoir les processus de recrutement dans le secteur IT, on assiste à la fin des divas techniques : l'ultra compétence technique ne sera plus suffisante, la culture processus et qualité sera indispensable avec en ligne de mire l'aviation civile.

Il sera nécessaire d'acquérir des outils de déréférencement, de surveillance et de protection de e-réputation : Maltego, XMCO, etc.

Il sera indispensable, et cela va être très complexe à mettre en œuvre, de prendre conscience des exigences croissantes de la patientèle concernant les notions d'accord explicite.

Conclusion

Le lecteur est en droit de se demander pourquoi diable ais-je choisi la date de 2037 pour cible temporelle : pourquoi pas 2040, 2100, 2025 ? La réponse est simple : 2037 est la date de mon départ à la retraite, enfin si Dieu et la CNAV le veulent bien. Et quand je vois tout ce qui va nous tomber dessus et comment on va s'amuser comme des petits fous à déployer et à sécuriser tout cela, j'espère pouvoir repousser un peu, pas vous ?

Bibliographie

« Les décisions absurdes », Christian Morel, deux tomes

« Une brève histoire du futur », Michio Kaku

« La mort de la mort », Dr Laurent Alexandre

« Le Big Data, penser l'homme et le monde autrement », Gilles Babinet

« Culturama », Aiden Erez

« La sécurité du système d'information des établissements de santé », Cédric Cartau