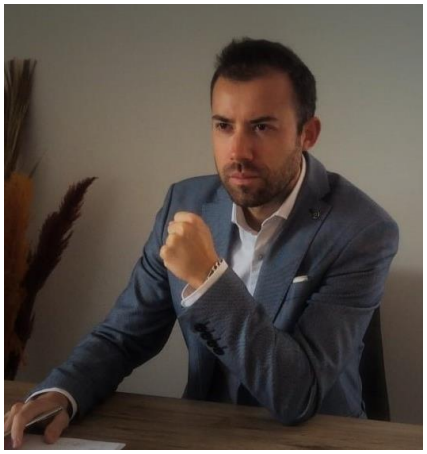
L'accélération de la résilience numérique du secteur protéiforme de la santé en France



Rodolphe BACA
Responsable région AURA
ATOS Cybersécurité Services

Introduction

Ensemble nous développerons la thématique de la cybersécurité dans le secteur de la santé en France. Comme à notre accoutumée nous allons rester purement factuel, dans l'analyse rigoureuse des chiffres, des situations dans leur globalité, mais aussi dans leur spécificité. Personne ne peut se targuer de tout connaitre, et s'auto-proclamer expert est souvent gage du contraire. Nous resterons le plus humble possible, sans moralisation, sans critique facile, sans leçon à donner, et surtout, en évitant le sensationnalisme.

Le ton étant donné, commençons par notre ambition dans cet essai. Volontairement destiné à un large public, nous ferons essentiellement une description de l'actuel, en expliquant les situations passées et présentes, et en projetant le futur. Cela fait déjà 2 ans que les premiers exercices de crise d'origine cybersécurité, financés par le ministère de la santé via l'INSTRUCTION N° SHFDS/FSSI/2023/15 du 30 janvier 2023 ont eu lieu. Par ce dispositif, les ARS (Agences Régionales de Santé) et pour certaines via leur GraDeS (Groupement Régional au Développement de la e-Santé) ont pu suivre l'évolution grandissante de la prise en compte du sujet cyber au sein des directions des structures.

Notre retour d'expérience est le suivant. Nous avons pu effectuer à ce jour avec mon équipe, un petit peu plus de 100 exercices, qu'ils aient été du kit débutant, intermédiaire, confirmé ou encore intégralement adapté. Nous avons pratiqué ceci en sanitaire et médico-social dans le secteur public, établissements supports de GHT ou CH et autres, dans le secteur privé lucratif et non lucratif. Par ailleurs, nous réalisons quotidiennement des analyses de risques, des audits de maturité, des pentests, des mises en conformité, des évolutions d'architectures, des intégrations de logiciels, du SOC, de la réponse à incident, mais également au plus proche des services de santé, avec des évolutions des dispositifs de crise, notamment les fameux « PCRA ».

C'est grâce à cette palette et cette vision à 360° que nous pouvons aujourd'hui vous expliquer ce que sont les SI de santé, expliquer la réglementation en vigueur, retranscrire les réels impacts des cyberattaques récentes, expliquer l'écosystème actuel, enfin, faire une projection des attendus et des incertitudes actuelles. Ceci tendra à argumenter notre optimisme quant à l'accélération de la résilience numérique du secteur protéiforme de la santé en France.

Existe-t-il un SI de santé, ou bien des SI de santé ? Comment inclure la cybersécurité dans un secteur où sa place parait logique, mais en pratique complexe à mettre en œuvre ?

Encore une fois, conservons à l'esprit que nous n'estimons pas tout savoir de tous les établissements de santé en France. Nous donnons notre vision, qui

comme tout sujet, est libre d'interprétation et d'amélioration continue.

Nous avons rencontré les architectures de SI de santé suivante :

- La première correspond aux structures disposant de serveurs physiques hébergés en interne des bâtiments de la structure de santé, sur lesquels repose une forte virtualisation de serveurs. Les sauvegardes sont fréquemment internalisées mais cloisonnées dans des VLAN isolées, ou encore complètement externalisées. L'administration des réseaux et des systèmes est effectuée en interne par les équipes d'une Direction du Numérique, ou une Direction des SI. L'équipe dispose de professionnels de la cybersécurité notamment d'un RSSI et d'adjoints selon la nécessité, et surtout le budget dédié. Le recours a de l'hébergement externe existe mais assez peu sur des fonctions critiques telles que le Dossier Patient Informatisé (DPI), ou le logiciel de Gestion Administrative du Patient (GAP). Ceci s'explique par la confiance, justifiée, en l'architecture et la sécurité de cette partie du SI pour maintenir les besoins de continuité et d'urgence de l'établissement. Pour faire simple, un prestataire externe ne ferait pas forcément mieux en termes de capacité, et surtout pas au même tarif… D'autres parties du SI, notamment dans les fonctions supports, tels que des logiciels Sage ou Bluekango se retrouvent plus fréquemment hébergés par leurs éditeurs.
Dans la majeure partie des cas, cette situation décrit les SI des établissements supports de Groupements Hospitaliers Territoriaux (GHT), c'est-à-dire les établissements publics les plus importants des métropoles / départements.

- La seconde correspond à des établissements avec peu ou prou la même architecture, mais cette fois des budgets plus faibles et des tensions de disponibilités de personnels IT élevées. Il s'agit également d'établissement, disons « périphérique » aux plus gros établissements régionaux publics, dont les budgets sont liés directement à l'activité et donc à la PMSI (Programme de Médicalisation des SI). Pour faire simple, plus l'établissement a d'activité, plus son budget est élevé. Assez logique … Mais intrinsèquement pour les structures disons secondaires, les capacités de défense, et de résilience y sont donc plus faibles. Est-ce une explication au fait que les structures de santé cyber-attaquées récemment, correspondent pleinement à ceci (Dax, Villefranche, Versailles, Sud Francilien, Brest, Armentières…), lorsque des structures telles que l'AP-HP, les HCL sur Lyon, l'AP-HM à Marseille n'ont jusqu'alors pas été frappées par des blocages de leur SI via rançongiciel …

- La troisième correspond à des établissements privés à but lucratif, disposant d'un gigantesque SI centralisé dans un/des datacenters en France, et où les structures de santé ne disposent physiquement chez elles, que de serveurs de « rebond » pour accéder aux ressources centralisées. Cette structure permet ainsi de centraliser l'administration, les dépenses, les compétences, les trajectoires et stratégies. Fréquemment leur robustesse et résilience sont plus élevées que la moyenne du secteur de la santé. Les cliniques, EHPAD ou autres structures fréquemment « rachetées » et donc intégrées au Groupe, viennent ainsi rejoindre ce SI afin d'y bénéficier de la maturité cyber. Volontairement nous simplifions les difficultés d'intégration et la gestion des changements de ce type de projet de migration car ce n'est pas le sujet ici …

- La quatrième correspond aux structures privées lucratives ou non-lucratives, à taille plus modérée, disposant d'infogéreurs, et qui parfois doivent jongler entre plusieurs infogéreurs en parallèles car les établissements de santé sont géographiquement éloignés. Ceci amène à une disparité de la maturité des établissements de ces groupements ou associations du fait de leur dépendances à leurs infogéreurs.

Une fois que l'on a décrit la grande majorité des architectures des SI de santé en France, il convient d'expliquer que malgré ces différences, au final, quand nous ouvrons le capot, le contenu de ces SI est très similaire, lié directement aux métiers de la santé : admettre et soigner les patients, organiser les moyens techniques de soin, disposer de services supports RH et financiers pour effectuer les activités.

Ainsi, nous retrouverons quasi-obligatoirement les artefacts suivants :

- Un Dossier Patient Informatisé (DPI), contenant, selon la solution éditeur retenue, le plan de soin, l'historique des prescriptions, les soins et injections effectuées, les relevés divers …
- Une Gestion Administrative du Patient (GAP), débutant à l'admission du patient permettant de suivre son parcours au sein de la structure, de son entrée à sa sortie, fréquemment l'outil contient ou est directement interconnecté avec la PMSI afin de disposer et centraliser l'activité de l'établissement avant transfert vers notamment l'ARS et la CPAM. C'est via l'étape de la GAP qu'est, normalement, réglée la problématique de l'identitovigilance.
- Un outil d'imagerie/radiologie/scanner venant alimenter ou non le DPI, et outil de PACS (archivage et transmission d'image).
- Un outil lié aux résultats de laboratoires s'il est internalisé.
- Un outil de gestion de la pharmacie, commande, stock et gestion du parcours du médicament.
- …

« Les Hospices civils de Lyon (HCL) comptent plus de 500 applications sur 14 sites différents et l'Assistance publique-Hôpitaux de Paris (AP-HP) utilise près d'un millier d'applications sur 40 sites », *La sécurité informatique des établissements de santé, Cour des Comptes, S2024-1456.*

A retenir, on voit déjà que pour soigner un patient, une suite de logiciels est interconnectée en permanence pour assurer à chaque étape, une gestion numérique du soin. La situation serait idyllique si un seul outil pouvait effectuer l'ensemble. Aussi, il serait utopique de penser que ces outils communiquent « facilement » entre eux. Selon leur mode de communication, leur écriture, leur versioning, ils pourront ou non s'interconnecter, et transmettre des informations vers les autres outils. Mais tout de même on peut concéder que leur développement est dans la majeure partie des cas, orientée vers leur interopérabilité. Mais pas forcément l'interopérabilité avec des outils de cybersécurité …

Nous avons ainsi rencontré des structures où les RSI nous ont confié qu'ils avaient dû déconnecter leur antivirus sur le serveur de DPI car cela l'empêchait de « fonctionner » correctement. Cela peut nous paraitre insensé car nous sommes des acteurs de la cybersécurité. Mais c'est oublier que la priorité des structures est de soigner leur patient. Si un élément se met sur cette route, il doit logiquement s'adapter ou être « retiré ». La cybersécurité doit s'adapter à son contexte, jamais l'inverse. Ainsi on peut trouver aberrant que des ordinateurs dans les services contenant des données personnelles sensibles sur la santé des patients, soient laissés ouverts et accessible à tous. Mais d'une part, quel est le risque réel ? De savoir que la personne dans la chambre 102 s'est cassé la jambe, ou est atteinte d'Alzheimer ? Personne n'a jamais vu d'attaquants venir physiquement voler des données de cette façon. De plus, un éventuel curieux serait vite interrompu par le personnel soignant. Ces PC ne sont jamais verrouillés car le besoin métier est de pouvoir accéder aisément à l'information de traitement, quid du nombre de fois où les soignants devraient taper leur code sinon. Ou bien, quid du personnel soignant devant se connecter via une carte d'authentification, et qui malencontreusement oublie cette carte dans la veste qu'il portait hier : il ne va donc pas soigner pour la journée ? Le sujet est sérieux, il convient d'aller plus loin dans la réflexion pour apporter une vraie valeur ajoutée.

A partir de ceci, comment alors améliorer la résilience ? Afin de répondre aux précédents programmes et à la certification HAS, les établissements ont dû mettre en place des modes dégradés. Fréquemment, il s'agit d'un PC de secours, contenant une extraction automatique du DPI en version PDF, mis à jour à des temporalités différentes (toutes les 30mn, toutes les heures, 3 fois par jour …). Il permet en cas de panne informatique ou d'électricité, d'accéder de manière secondaire à l'information sur son patient. C'est une réponse intéressante à ces risques, mais à l'époque de leur mise en place, les attaques cyber via ransomware n'étaient pas autant présentes et puissantes. Aujourd'hui, c'est certes une réponse intéressante, mais uniquement si leur configuration est effectuée

pour prévenir ce risque cyber. Lorsque l'informatique tombe du fait d'une cyber attaque, c'est le retour au mode papier. Lequel est illustré par des caisses complètes de documents vierges, permettant de noter la prise de température, les injections effectuées, les prescriptions, les observations … qui ne peuvent plus s'effectuer sur les ordinateurs ou tablettes. On pourrait ainsi penser que ces PC de secours, du fait de leur importance sont plus robustes, mieux sécurisés. Malheureusement ce n'est pas forcément le cas. Dans le meilleur des mondes, ils devraient être isolés dans un pan du réseau différent ayant toutes ses communications filtrées afin d'empêcher la propagation d'un ransomware à leur espace. Leur moyen de communication avec le reste du SI devrait également diverger, on parle de rupture protocolaire (le même principe, en parallèle, s'appliquant au durcissement d'Active Directory …). Pour faire simple, lors d'accompagnement sur un audit du dispositif de crise, il est nécessaire d'auditer l'architecture, ainsi que fréquemment réaliser un Pentest, afin de se placer dans la peau d'un attaquant et trouver les failles de sécurité du dispositif nominal, et du dispositif de secours.

Aussi, outre les logiciels critiques et secondaires, les SI de santé voient de plus en plus s'intégrer des logiciels tiers nécessaires aux soins, mais source majeure de vulnérabilité. Ainsi on voit se multiplier les objets connectés (frigo connectés, dispositifs anti-fugue, appels malades, robots X ou Y …) ainsi que l'ouverture du SI à de multiples parties prenantes. Pour simplifier, au quotidien, pour le besoin des soins, on multiplie des sources potentielles de vulnérabilités et donc de risques réels pour l'ensemble de la structure de santé. On ne répètera jamais assez la nécessité de disposer d'excellents architectes afin de construire des réseaux cloisonnés.

Si l'on prend un exemple médiatique récent, il est apparu que les appareils Contec CMS8000, transmettaient des flux d'information sur l'identité de patients et leurs constantes vitales, vers des IP localisées dans une université chinoise. Ceci étant codé en dur dans le logiciel de l'équipement. Pour beaucoup, adepte du sensationnalisme médiatique ou « Linkedinique », on y a vu un espionnage chinois dans la santé des patients français. C'est certes vrai, mais c'est extrêmement naïf de penser que d'une part c'est un exemple isolé, et que d'autre part cela aurait fonctionné. Pour régler le sujet et empêcher tout transfert d'information d'un SI vers une IP externe, on passe par des équipements de filtrage appelés Firewall et Proxy. Dans une configuration de base, les firewalls filtrent les communications de chaque machine, ou type de machines, à accéder ou n'être accessible qu'à des adresses ou groupe d'adresses autorisés. C'est-à-dire qu'il ne rentre et ne sort, que des IP validées en amont. C'est ce que l'on appelle maitriser sa matrice de flux.

Ainsi, dans 99% des cas, aucune donnée de patient français n'a été transmise directement vers la Chine, car tous les firewalls empêchent par défaut ce type de communication. C'est la différence entre la cybersécurité sur Linkedin avec un titre tapageur et la réelle cybersécurité de ceux qui travaillent au quotidien.

Pour conclure cette thématique, on pourra parler de la hausse récente de la maturité des structures de santé grâce au domaine 1 du programme CaRE que l'on développera après. Il convient de noter que 3 sujets étaient ambitionnés :

- Le durcissement de l'Active Directory des établissements,
- Le renforcement de l'exposition sur internet,
- La prise de conscience du Top management par la réalisation des exercices de crise cybersécurité.

Suite à la réalisation des actions, soit directement en interne soit via des prestataires industriels, les structures peuvent obtenir le financement des travaux selon leur éligibilité et le montant maximal qui leur est alloué. Très clairement, cette année 2024, et début 2025, a confirmé que cette première étape a considérablement amélioré la résilience des établissements de santé.

Finalement, nous espérons avoir pu démontrer que derrière la pensée d'un secteur de santé homogène,

il y a vraiment des SI totalement différents et sujets à des risques plus ou moins élevés.

Un accroissement réglementaire, une organisation institutionnelle en constante évolution, des financements fluctuants : signe d'une stratégie par à-coup plus que par planification à long terme

Depuis 10 ans on observe une augmentation du nombre d'établissement de santé avec l'obligation légale d'intégrer les risques et des objectifs en termes de cybersécurité.

Cela a commencé par la première loi de programmation militaire (LPM), faisant entrer une grosse dizaine d'établissements publics sous le champ d'application des opérateurs d'importances vitales (OIV). Bien que la liste des OIV ne soit pas communicable (Article R1332-3 du code de la Défense) il est très simple de trouver les établissements de santé qualifiés : ils disposent obligatoirement d'un Officier de Sécurité, information malheureusement trop souvent partagée sur Linkedin (pour booster son égo) ou autres réseaux professionnels. Pour rappel, si cette liste est confidentielle, il convient de maintenir le même degré de confidentialité concernant son appartenance au procédé… Le décret 2015-351 du 17 mars 2015 précise les moyens de contrôle de ces OIV une fois par an, par l'Etat, l'ANSSI ou un industriel qualifié PASSI LPM.

Ensuite, par le biais de la loi de transposition de NIS1, les Opérateurs de Services Essentiels (OSE) ont été identifiés et ils avaient l'obligation, sous contrôle de l'ANSSI, d'identifier et désigner leur Système d'Information Essentiel (SIE). Bien que la quasi-totalité l'ait fait, nous avons reçu récemment d'un établissement support de GHT une demande d'accompagnement pour l'identification de ses SIE. Preuve qu'en 2025, 7 ans après l'obligation initiale, il y a toujours un retard conséquent, indicateur soit de la méconnaissance, soit de l'incapacité budgétaire de la structure à prendre en charge le sujet. L'Etat estimant surement, que vu leur activité, et donc logiquement leur budget, il n'était pas nécessaire de prévoir un financement pour répondre à cette obligation légale. On est ainsi passé d'environ 10 structures, à environ 130 structures à devoir intégrer une conformité légale sur la cybersécurité. Sachant que les obligations entre LPM et NIS 1 ne sont bien-sûr pas les mêmes, même si les 23 objectifs de NIS1 n'étaient pas franchement complexes…

Aujourd'hui, début juin 2025, les travaux sur la transposition de NIS2 se poursuivent. Sans entrer dans les détails, deux terminologies feront leur apparition : les entités essentielles (EE) et les entités importantes (EI). Dans la santé, il y aura environ 800 future EE, et 1200 future EI. Ajoutant le fait que cette fois, les objectifs de sécurité seront bien plus précis et complexes. On change d'échelle. L'ANSSI avait déjà les plus grands maux à contrôler avant NIS2, avec un budget rapiécé en 2025, bon courage … Ceci expliquant d'ailleurs, la sous-traitance grandissante vers des opérateurs privés entre l'évolution de la qualification PASSI et la création de PACS. A l'heure où les menaces de guerre hybride via la cybersécurité sont à un niveau jamais égalé, nul doute que cette trajectoire devra faire l'objet d'analyse de la part de nos Parlementaires, et il vaudrait mieux que cela soit en amont, et non en aval d'une crise majeure ...

Outre NIS2, on parle également du Cyber Resilience Act (CRA) dont l'objectif est de contraindre les fournisseurs par le renforcement de la sécurité des produits qu'ils commercialisent. Cependant, les outils connectés liés au secteur de la santé sont exclus de CRA, car ils sont déjà « couverts » par le RÈGLEMENT (UE) 2017/745 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 5 avril 2017 relatif aux dispositifs médicaux. On parle du marquage « CE ». Or pour les professionnels de la cybersécurité, nous savons très bien que ce marquage n'a aucune valeur réelle et n'est pas un gage de résilience cyber du dispositif. Voilà ainsi une opportunité gâchée d'obliger les fournisseurs de dispositifs médicaux à mettre en place un haut niveau de cybersécurité. Enfin sur ce sujet, à l'heure où NIS2 pense la cybersécurité dans toute la chaîne de sous-traitance, nous savons d'ores et déjà que les établissements de santé ne pourront jamais être « pleinement »

conformes, car ils hébergent en leur sein, des dispositifs médicaux non-conformes. Il n'est pas certain qu'une justification technique, de type « cloisonnement » dans des VLAN spécifiques soit suffisante … On verra donc.

Concernant l'organisation de l'Etat sur la cybersécurité dans la santé, on voit depuis 10 ans que des initiatives sont prises, puis qu'à la faveur du positionnement du sujet numérique dans les gouvernements successifs, des évolutions ont lieu. Aujourd'hui, le sujet est sous pilotage de la Délégation du Numérique en Santé (DNS), structure tutelle de l'Agence du Numérique en Santé (ANS), et du Fonctionnaire de sécurité des SI (FSSI) auprès du Haut Fonctionnaire de Défense et de Sécurité (HFDS) du ministère de la Santé. Vous me suivez toujours ? Je vous assure que ça s'est pourtant simplifié.

Cette gouvernance est en charge de la planification à l'échelle nationale de la stratégie numérique des établissements sanitaires et médico-sociaux. Pour cela, le Ségur du numérique a vu le jour, financé par l'Union Européenne à hauteur de 2 milliards d'euros à sa présentation en 2021. L'ambition était « de généraliser le partage fluide et sécurisé des données de santé entre professionnels de santé, du social et du médico-social et avec l'usager pour mieux prévenir, mieux soigner et mieux accompagner ». Difficile aujourd'hui de retrouver l'information, mais à l'origine la somme destinée à la cybersécurité des établissements de santé, était chiffrée à… 0€. Dans le détail, on peut encore trouver sur internet des publications de 2022, notamment ici, la répartition originelle : 1,4 milliard sur le partage de données de santé, et 600 millions dédiés au secteur médico-social. Depuis, la communication a étonnamment changé, et on trouve en 2024 sur le site du Ségur du numérique, un volet sur la cybersécurité notamment via le programme CaRE. Quelle est la raison de cette évolution ? La volonté de l'Etat au sortir des cyberattaques de 2021 et 2022 d'améliorer la résilience des structures. Ainsi, des sommes initialement prévues ailleurs, ont été déplacées vers la création du programme CaRE, et ce uniquement car, comme le dit la Cour des Comptes, il y a eu « une sous-consommation de crédits prévus pour le développement des usages numériques en santé par les médecins de ville. » Merci donc aux médecins de ne pas aimer le numérique, ceci a permis de financer CaRE sur 2023 et 2024. Or, sur 2025, la Cour indique textuellement que « les modalités du financement du programme CaRE entre 2025 et 2027 devront être précisées. » Nous sommes en fin mai 2025, le domaine 2 du programme CaRE n'est toujours pas paru. Des indices nous avaient pourtant été laissés, notamment par le biais de la Cour des Comptes.

C'est donc l'opportunité de crédit qui a permis la construction d'un financement ponctuel du domaine 1 de CaRE, et non une stratégie coordonnée et planifiée dans le temps.

Au sein des régions, et sous pilotage des ARS, les Groupements Régionaux au Développement de la e-Santé (GRADeS) disposent eux-aussi de financement afin d'accompagner sur leur territoire l'amélioration de la maturité cyber de tous les établissements de santé. En Auvergne-Rhône Alpes il s'agit du GCS SARA. On parle des Centres Régionaux de Ressources Cyber (CRRC). Leurs objectifs et financements sont prévus sur cette INSTRUCTION N° DNS/2024/54 du 2 juillet 2024 relative aux missions des centres régionaux de ressources cybersécurité (CRRC) et à leur financement.

Au final, tant qu'une ligne de financement précise sur le programme CaRE n'aura pas été inscrite, il y a fort à parier que la cybersécurité ne sera financée que grâce au hasard des budgets et crédits.

Dans cette optique, et prenant en considération que la cybersécurité dans le domaine de la santé ne s'est améliorée qu'avec des financements de l'Etat, peut-on raisonnablement penser que la conformité à NIS 2 soit envisageable sur les 3 prochaines années ? Pas si sûr. Laissons donc le hasard décider de la résilience des établissements de santé face aux futures cyberattaques dans un monde toujours plus numérique et belliqueux.