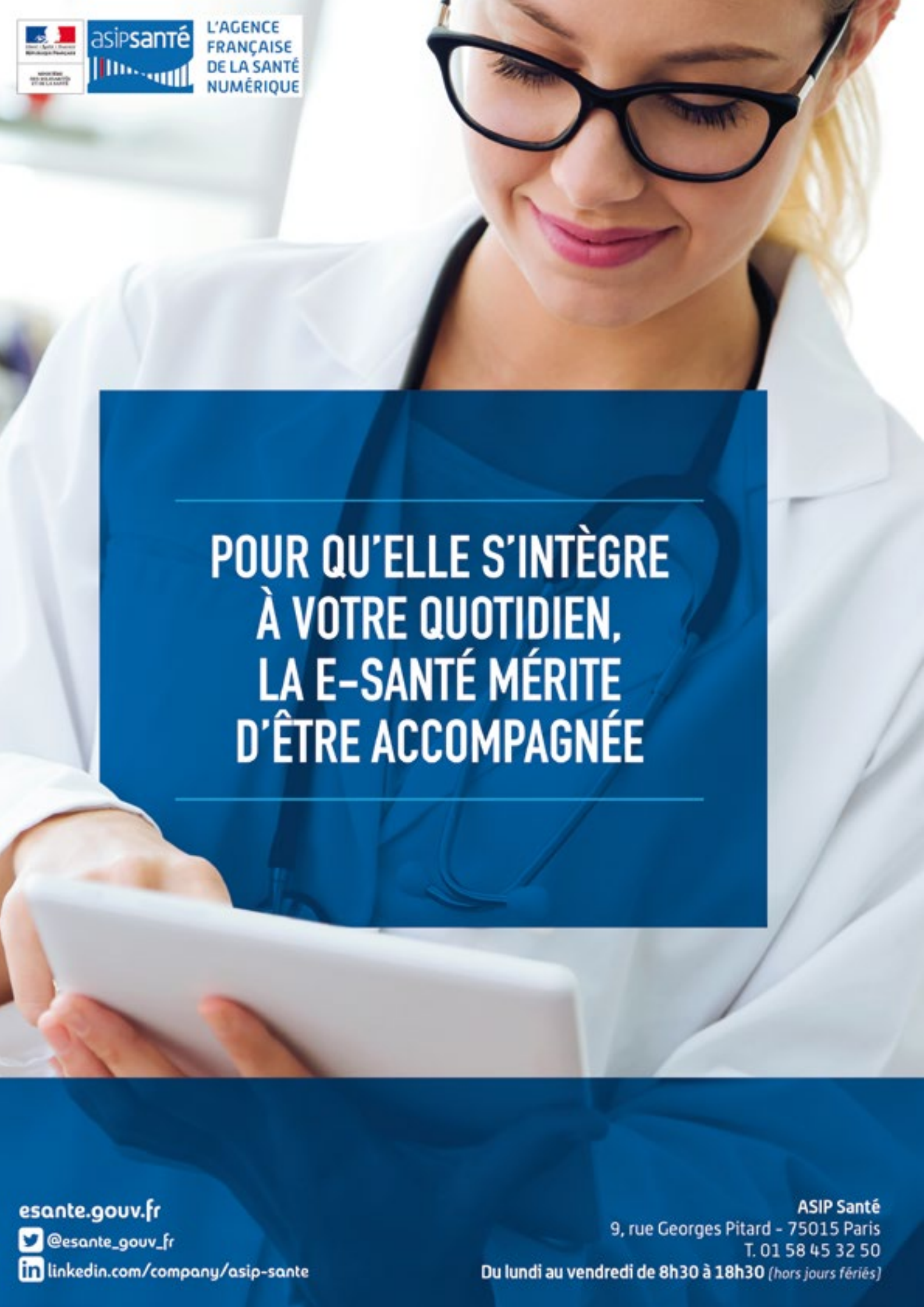
Témoignages exclusifs
de 40 professionnels
de la SSI Santé

APSSIS

OUVRAGE COLLECTIF
SSI SANTÉ

Janvier 2019



asipsanté
L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

POUR QU'ELLE S'INTÈGRE À VOTRE QUOTIDIEN, LA E-SANTÉ MÉRITE D'ÊTRE ACCOMPAGNÉE

esante.gouv.fr
@esante_gouv_fr
linkedin.com/company/asip-sante

ASIP Santé
9, rue Georges Pitard - 75015 Paris
T. 01 58 45 32 50
Du lundi au vendredi de 8h30 à 18h30 *(hors jours fériés)*

PRÉAMBULE

Vincent Trély - Président de l'APSSIS

Chères lectrices, Chers lecteurs,

C'est une joie et un honneur de vous présenter le premier Ouvrage collectif dédié à la sécurité des systèmes d'information de santé, produit par l'APSSIS, avec le support de l'ASIP Santé, et grâce à la bienveillance et à la passion qui animent cet écosystème !

Imaginé en 2016, planifié en 2017, produit entre mars et décembre 2018, cet Ouvrage collectif APSSIS réunit plus de 40 productions. La rédaction d'articles et de retours d'expériences a été proposée à un large panel de Professionnels de la SSI Santé, leur laissant le choix du ou des sujet(s) et surtout, la liberté de se faire plaisir et de donner à leurs propos la ou les tonalité(s) de leur choix !

L'objectif initial était de donner la parole au terrain, par la plume de celles et ceux qui « exercent la SSI », qui mettent en œuvre les principes de la cybersécurité au cœur des organisations, tant sur le volet « technique » que sur le volet « politique » et qui connaissent succès et échecs, facilités et difficultés, joies et doutes, mais sont toujours accompagnés par la passion.

L'ouvrage est organisé en sept thématiques : Normes et référentiels, Gouvernance de la SSI Santé, Technologies de sécurité, RGPD et cybersécurité, Processus et procédures, Conformité et audits, et Prospective. Les articles de nos auteurs ont été rassemblés par thématique, afin de proposer une lisibilité agréable et fluide.

2019 est une année importante pour la sécurité des SI de santé. Les nouvelles organisations territoriales génèrent de croissantes demandes de partage, de mobilité et d'accès permanents aux données de santé. Les architectures techniques et logicielles, les solutions d'interopérabilité, les réseaux d'échanges, les outils de sécurité et tous les composants techniques, logiciels et humains qui collectent et manipulent ces données doivent être sûrs, robustes, en plus de se conformer aux lois, instructions et bonnes pratiques connues.
Le cheminement des SI de santé vers l'hyper connexion, les mettant au centre de systèmes exogènes multiples – IoT, monitoring et supervision distants des patients, IA spécialisées, systèmes régaliens – doit positionner leur sécurité et leur conformité au top des priorités. C'est l'obligation portée par le système de santé, au bénéfice de la confiance numérique et du bien-être des patients et des professionnels de santé usagers !

Bonne lecture !

APSSIS

SOMMAIRE

PRÉAMBULE — P. 01

PROPOS INTRODUCTIFS — P. 05 À 07

du FSSI du Ministère des Solidarités et de la Santé, **Philippe Loudenot**

0.1 NORMES ET RÉFÉRENTIELS — P. 08

L'hébergement de données de santé à caractère personnel, **Marguerite Brac de la Perrière**
ISO 27001, l'odyssée de la sécurité numérique, **Philippe Tourron**
ISO 27001, de la difficulté présumée à l'utilité véritable, **Pascal Sabatier**
Les 3 C de la sécurité des SI : conformité, communication, confiance, **Guillaume Jeunot**
Une cartographie unifiée des SI ou comment maîtriser ses risques, **Didier Pescarmona**
(L'inévitable) guide d'hygiène de l'ANSSI, **Cédric Cartau**

0.2 GOUVERNANCE DE LA SSI SANTÉ — P. 22

Direction du Système d'Information : cap sur l'océan du numérique, **Didier Bonnet**
Quand sécurité des SI, qualité et gestion des risques ne font qu'un, **Elodie Jamet**
Fonctions et priorités du RSSI, **Nour Kadi**
RSSI / chargé de sécurité : des liens étroits, **Stéphan Thamier**
Certification HAS : retour d'expérience, **Yohann Fourchon**
Une approche de la sécurité sous l'angle des projets, **Thierry Veauvy**
Sensibiliser, sans relâche, **Christophe Le Callonec**
La « gamification » ou « jeux sérieux » au service de la sensibilisation !, **Auriane Lemesle**
Le CHU de Rouen vise l'unité d'actions, **Jacques Ferrand et Cédric Hamelin**

0.3 TECHNOLOGIES DE SÉCURITÉ — P. 38

Annuaire et IAM : les véritables enjeux, **Cédric Cartau**
Annuaire et IAM : retour d'expérience du CH Alpes-Isère, **Benjamin Delubac**
Simplifier la gestion des mots de passe, **Sébastien Wetter**
Sécuriser l'Active Directory de l'établissement de santé, **Christophe Jodry**
Les données de santé sensibles doivent être chiffrées et signées, **Gérard Peliks**
Un partenariat qui simplifie l'échange de données par MSSanté, **Sébastien Wetter**
Face au phishing : scoring et sensibilisation, **Michael Roman**
Et si le risque venait de l'intérieur ?, **William Culbert**
Tests d'intrusion et scans de vulnérabilité : in-dis-pen-sables, **Frédéric Cabon**
Scanners de vulnérabilités : connaître son SI pour mieux le protéger, **Charles Blanc-Rolin**
L'intérêt d'un cloud hybride, **Didier Verbeke**
Solution de prise en main à distance : un choix loin d'être anodin, **William Culbert**
Intelligence artificielle et outils de cyber-sécurité, **Loïc Guezo**

04 RGPD ET CYBERSÉCURITÉ — P. 62

RGPD et contrats des fournisseurs IT Santé : peut mieux faire ?, **François Coupez**
Data Protection Officer : quel positionnement, quel périmètre, **Fabien Dachicourt**
Le point de vue d'un chargé de mission en ARS, **Guy Marty**
Comment faciliter la mise en œuvre du RGPD dans les laboratoires de biologie médicale, **Bruno Gauthier**
Ce qu'il faut savoir à propos du Privacy Impact Assessment, **Cédric Cartau**
ACSS : une réponse à la menace de cybersécurité dans le secteur santé, **ASIP Santé**

05 PROCESSUS ET PROCÉDURES — P. 78

L'appui et les solutions de l'ASIP Santé, **Alain Espinoux**
Connectivité et vulnérabilités, **Gérard Gaston**
Les cinq temps de la gestion des incidents SSI, **Cédric Cartau**
Outiller le processus de gestion des changements, **Stéphane Moneger**
L'enjeu de la gestion contractuelle dans l'atteinte de la conformité des SI en santé, **Pauline Berry et Isabelle Zablit**

06 CONFORMITÉ ET AUDITS — P. 90

La démarche d'homologation de sécurité des systèmes de santé : susciter l'adhésion, **Astrid Lang**
Comment organiser le suivi de conformité interne, **Lénaïc Plouvier**
Cahier spécial Audit, **Mauro Israel**
- Les concepts et principes de l'audit
- Le déroulement d'un audit
- La check-list de la cybersécurité

07 PROSPECTIVE — P. 110

Si on adoptait l'angle de vision du patient…, **Philippe Ameline**
2028 : année zéro, **Auriane Lemesle**
Un permis pour l'accès au SI, **Cédric Cartau**
L'éducation au numérique : un investissement d'avenir, **Dominique Lehalle**

BIBLIOGRAPHIE — P. 118 & P. 119
WEBOGRAPHIE — P. 120 & P. 121
REMERCIEMENTS — P. 122 & P. 123

PROPOS INTRODUCTIFS

du FSSI du Ministère des Solidarités et de la Santé, **Philippe Loudenot**

Cybersécurité : des risques liés au métier

Philippe Loudenot, Fonctionnaire de Sécurité des Systèmes d'Information (FSSI) du Ministère des Solidarités et de la Santé, appelle à un changement urgent de vision concernant la protection de l'information et du numérique. Aujourd'hui, sous-estimer le risque et, surtout, ne pas le prendre au bon niveau, constitue une menace pour l'avenir des organisations de santé.

Ancien responsable national de la sécurité des systèmes d'information du service de santé des armées, et ancien FSSI des Services de Matignon, **Philippe Loudenot** 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 (ARCSI), du CESIN et du club EBIOS.

L'utilisation des technologies de l'information et de la communication appliquées au domaine de la santé doit être abordée selon différents angles :

- Technique, avec les outils permettant aux professionnels de santé de partager les informations de santé, de gérer l'ensemble de ces données pour assurer un meilleur suivi des patients, sans oublier l'ensemble des systèmes offrant une aide au diagnostic, une délivrance et/ou un contrôle de traitement
- Prospectif, avec le développement de solutions de télémédecine/télésanté, que ce soit pour l'hospitalisation à domicile ou le suivi de pathologies chroniques
- Économique, avec un objectif de diminution de coûts tout en augmentant la qualité des soins

> « De nombreuses organisations continuent à n'envisager la cybersécurité que dans le champ du service ou de la direction informatique. Cela doit changer. »

Au regard de ces aspects, l'intérêt des systèmes d'information dans le monde de la santé ne peut être mis en cause : travail des professionnels facilité mais, surtout, et c'est l'objectif premier, meilleure prise en charge des patients. L'avènement du « tsunami numérique » est un fait constaté tous les jours. Source de progrès et d'augmentation de chances pour les patients (nous sommes tous concernés, patients avérés ou en devenir), il est désormais impossible d'éviter le débat sur les dépendances aux technologies numériques. Le numérique se trouve partout, même là où il n'était pas attendu :

- Systèmes d'information hospitaliers
- Dispositifs biomédicaux
- Objets connectés
- Systèmes centralisés de gestion technique ou de bâtiment

Il est devenu vital en matière de prise de décision. Il permet l'optimisation de processus ou de savoir-faire et l'industrialisation dans tous les domaines. L'accès aux données et aux informations constituent des atouts clefs pour l'ensemble des professionnels de santé, leurs organisations et, avant tout, leurs patients.

Une surface d'attaque sérieusement augmentée avec les objets connectés

Cependant l'adoption et la présence exponentielle du numérique s'accompagnent d'un manque de compréhension des enjeux. Nous sommes devenus vulnérables.
Concernant particulièrement les établissements de santé et médico-sociaux, il apparaît que la révolution numérique est bien au rendez-vous. Mais il est urgent d'opérer un changement de vision concernant la protection de l'information et du numérique. Le risque en matière de cybersécurité est désormais clairement présent. Le sous-estimer, ou ne pas le prendre au bon niveau, constitue ainsi une menace pour l'avenir d'une organisation. Malgré cela, de nombreuses organisations continuent à n'envisager la cybersécurité que dans le champ du service ou de la direction informatique. Cela doit changer.

A l'horizon 2020, plus de 50 milliards d'objets seront connectés à Internet directement ou via le réseau d'une entité. La plupart d'entre eux sera à peine protégés, ce qui augmente sérieusement la surface d'attaque susceptible d'être utilisée par les pirates pour s'introduire dans nos appareils, nos systèmes, nos organismes, nos maisons et nos vies personnelles. Les risques liés au numérique sont passés, en quelques années, d'une dimension quasi anecdotique à une menace multiple, structurée et organisée, pouvant provoquer des dégâts techniques, d'image de marque, juridiques et financiers considérables. Pouvant aussi mettre potentiel-

Cybersécurité : des risques liés au métier

lement en jeu la vie des personnes.
L'évolution des traitements de l'information, la mise en place de convergences technologiques (ordinateurs, réseaux, protocoles d'échanges, appareils biomédicaux) font des systèmes d'information numériques autant de cibles. Des incidents et attaques sont régulièrement déclarés. Les attaques sont lancées non seulement par des individus, des groupes d'individus, guidés par l'appât du gain, mais elles peuvent aussi être menées par des Etats ou de grandes organisations pour déstabiliser un pays. Par chance, aucun incident d'ampleur équivalente à ce qui est arrivé en 2017 en Angleterre (avec l'arrêt d'activité d'établissements de santé pendant plusieurs jours et l'évacuation d'une partie de leurs patients) n'est arrivé chez nous. Mais, légitimement nous pouvons nous poser la question : combien de temps serons-nous encore épargnés ?

Sensibiliser, plutôt que faire peur

Les différents incidents révélés ces dernières années par les médias démontrent régulièrement que la cybersécurité n'est finalement prise en compte qu'à l'issue d'une crise qui peut malheureusement être majeure, et contribuer à la disparition d'un organisme. *« Les hommes n'acceptent le changement que dans la nécessité et ne voient la nécessité que dans la crise ».* Cette maxime d'un des pères de la construction européenne, Jean Monnet, se mesure tous les jours en matière d'incidents numériques.
Disposer d'une information confidentielle mais fausse, d'un secret mais diffusé à tous, d'un besoin de connaissance immédiat mais non disponible, ne présente plus aucun intérêt. Si, dans le secteur de la santé, il n'y a pas eu de mort directe par perte de confidentialité, il n'en est pas de même avec la perte d'intégrité d'un résultat médical…
Ces menaces ne peuvent être annihilées, mais elles peuvent être contenues.Présenté comme cela, c'est très inquiétant. Mais, plutôt que faire peur, il est beaucoup plus important de sensibiliser, de faire prendre conscience, au-delà de la menace, des impacts potentiels pour un organisme ; et ainsi pouvoir rebondir. Le point positif, c'est que l'on sait comment faire. Encore faut-il le faire.
Mettre en œuvre une gouvernance SSI de façon performante et peu coûteuse c'est possible ! Cela permet en outre de réellement commencer à faire du préventif et non du curatif, de limiter les surcoûts directs ou indirects – et de très loin supérieurs – induits obligatoirement par tout incident ou piratage d'un système d'information.

L'obligation de déclarer les incidents numériques

La meilleure façon de se protéger consiste à adopter un processus de gestion des risques dans une démarche d'amélioration continue, en prenant en considération les vrais besoins en matière de sécurité. Cette approche reste bien la mieux adaptée aux besoins réels, la plus efficace et la moins chère. Une telle mise en œuvre permet de faire de la cybersécurité une véritable source de création de valeur et de ne plus l'identifier comme une contrainte légitime mais pesante.

Concernant le secteur de la santé, une avancée majeure a été réalisée en 2016, à l'initiative du député Gérard Bapt, qui a proposé un amendement dans le cadre de la loi de santé. Cet amendement est aujourd'hui intégré et est devenu l'article L.1111-8-2 du Code de la santé publique. Il fait désormais obligation de déclarer les incidents numériques. L'objectif n'est pas de savoir qui ni combien, mais il est bien de venir en appui aux établissements sanitaires et particulièrement les plus fragiles en matière de sécurité numérique. Cela permet également de tirer le meilleur des retours d'expérience et de proposer un ensemble de fiches « réflexes » ou techniques pour améliorer le niveau de sécurité.

Les bonnes pratiques

Au regard des incidents signalés, de façon obligatoire depuis le 1er octobre 2017 (et volontaire depuis 2014), un socle de bonnes pratiques a pu être identifié :

- Il ne peut y avoir de bonne transformation numérique si la sécurité n'est pas considérée comme un des piliers fondamentaux. Si cela est fait, on s'aperçoit vite que **la cybersécurité est un vecteur de performance**
- Une direction d'établissement ne peut plus cantonner le Responsable de la sécurité des systèmes d'information (RSSI) aux seuls services ou directions informatiques. Ce dernier doit partager, être l'interprète des métiers (services médicaux, biomédicaux, administratifs, moyens généraux…) et les accompagner pour apporter ce qui est attendu : **la confiance** dans les systèmes mis en œuvre. Le RSSI doit désormais rendre compte à la direction
- Il doit prendre en charge la protection de l'information et du numérique **dans toute son amplitude** : infrastructures réseaux, applications, dispositifs numériques adjoints ou embarqués dans les dispositifs biomédicaux, de gestion centralisée de bâtiment ou technique et de l'IOT[1] en général
- Techniquement, les réseaux doivent être **cloisonnés** ou les dispositifs les plus fragiles **confinés** (par retour d'expérience, ce point est malheureusement encore trop peu mis en place).

1 Internet des objets

Cybersécurité : des risques liés au métier

Les outils de la prévention

L'hygiène numérique doit être de mise. Mais, au-delà de l'hygiène, n'hésitons pas à établir la comparaison avec la prophylaxie. En médecine, elle désigne un processus actif ou passif ayant pour but de prévenir l'apparition, la propagation ou l'aggravation d'une maladie. Elle est au centre des campagnes de prévention, selon le principe qu'il « vaut mieux prévenir que guérir », pour un patient comme pour la société. En matière de prophylaxie, on distingue quatre stades de prévention. Ces mesures reposent sur tout un ensemble d'outils, depuis l'information et l'hygiène jusqu'à la remédiation, en passant par l'immunisation, le dépistage précoce et la quarantaine pour aboutir éventuellement à un ensemble de mesures palliatives, ou d'abandon si le rapport bénéfices/investissements est en trop grand déséquilibre.
À ce titre, les campagnes de mises à jour systématiques (patchs, signatures anti-malware, etc.), la déclaration des incidents (ANSSI, ACSS Santé[2], cybermalveillance.gouv.fr, …), ainsi que les démarches diverses d'hygiène SSI, le dépistage précoce de certaines exploitations et vulnérabilités (nouveau malware, par exemple) sont autant d'entreprises prophylactiques. Jusqu'à envisager le stade ultime où il est plus raisonnable de sacrifier une partie des systèmes plutôt que de gangréner la totalité d'un établissement.

La sécurité dès la conception

Enfin, un des leviers les plus puissants reste la sensibilisation des acteurs. Chaque établissement, chaque RSSI a un devoir de sensibilisation, sensibilisation encore, sensibilisation toujours, et accompagnement de l'ensemble des acteurs. Il faut leur expliquer les enjeux, non pas nécessairement en brandissant les menaces mais en parlant des impacts induits par un incident numérique.
A quoi sert d'imposer un badge ou une carte professionnelle dans un établissement si tous les acteurs n'en connaissent pas les règles ; d'imposer la sécurisation d'un système numérique si les comportements sur le poste de travail sont contraires à la politique de sécurité en vigueur ; de laisser le numérique envahir les pratiques (en apportant un réel bénéfice métier) si aucune mesure de prévention n'est prise pour un plan de continuité d'activité ?
Il faut donc instiller ces notions dans toutes les fibres les plus élémentaires d'une organisation, en termes de technologie (en intégrant la *security by design,* ou la prise en compte de la sécurité dès la conception d'un dispositif ou d'une application) et en termes de comportements.
La protection de l'information et du numérique doit évoluer et ne plus se concentrer sur la peur et le risque pour parvenir à intégrer le fait que le développement et le maintien de la confiance peuvent constituer et constitueront un facteur de différenciation. La cybersécurité n'est plus un risque informatique mais un risque lié au métier.

> « Les hommes n'acceptent le changement que dans la nécessité et ne voient la nécessité que dans la crise (Jean Monnet) »

2 Cellule Accompagnement Cybersécurité des Structures de Santé
(cf. page 74)

0.1

0.1 NORMES ET RÉFÉRENTIELS

L'hébergement de données de santé à caractère personnel, **Marguerite Brac de la Perrière** P. 09 & 11
ISO 27001, l'odyssée de la sécurité numérique, **Philippe Tourron** P. 12 & 13
ISO 27001, de la difficulté présumée à l'utilité véritable, **Pascal Sabatier** P. 14 & 15
Les 3 C de la sécurité des SI : conformité, communication, confiance, **Guillaume Jeunot** P. 16 & 17
Une cartographie unifiée des SI ou comment maîtriser ses risques, **Didier Pescarmona** P. 18 & 19
(L'inévitable) guide d'hygiène de l'ANSSI, **Cédric Cartau** P. 20

L'hébergement de données de santé à caractère personnel

L'obligation générale de sécurité rappelée par le RGPD renvoie aux référentiels et bonnes pratiques sectoriels. En matière d'hébergement de données de santé, ces textes, relatifs à l'obligation d'agrément ou de certification des hébergeurs, ont largement évolué ces derniers mois. Faisons le point sur le cadre juridique applicable et son périmètre.

Maître Marguerite Brac de la Perrière, directrice du département Santé numérique du cabinet Alain Bensoussan Avocats, a une activité dédiée au secteur de la santé et des nouvelles technologies. Elle conseille des groupements de coopération sanitaires, des autorités, des établissements de santé, des éditeurs, des hébergeurs, des groupes de grande consommation, des mutuelles et assurances ainsi que des startups, principalement en matière de protection des données à caractère personnel, partage et échange des données, hébergement des données de santé, télémédecine, objets connectés et contrats informatiques et de licence.

Depuis le 25 mai 2018, le RGPD impose aux responsables de traitements et sous-traitants, « compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les droits et libertés des personnes physiques », de mettre en œuvre « les mesures techniques et organisationnelle appropriées afin de garantir un niveau de sécurité adapté au risque »[1], étant rappelé que toute infraction à ces dispositions expose à de lourdes sanctions[2].
Cette obligation générale de sécurité, en ce qu'elle doit être adaptée aux risques, et conduire à la mise en œuvre de mesures appropriées, renvoie aux référentiels et bonnes pratiques sectoriels.

Or, en matière d'hébergement de données de santé, ce référentiel sectoriel est celui relatif à l'obligation d'agrément ou de certification des hébergeurs qui a largement évolué ces derniers mois.
L'heure est donc venue de faire un point sur le cadre juridique applicable à l'hébergement de données de santé à caractère personnel, et son périmètre d'application.

1 Art 32 RGPD
2 Art. 83 RGPD

1 Obligation d'agrément ou de certification à la charge de l'hébergeur

Les dispositions de l'article L1111-8 CSP (Code de la Santé Publique) relatives à l'hébergement des données de santé ont été reformulées par la loi de modernisation de notre système de santé du 26 janvier 2016[3], mettant à la charge de l'hébergeur de données de santé l'obligation d'être agréé ou certifié, et non plus, comme dans la version antérieure du texte, à la charge du responsable de traitement l'obligation de recourir à un hébergeur agréé.

Désormais, **l'obligation légale de l'hébergeur** est la suivante :
« *Toute personne qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, réalise cet hébergement dans les conditions prévues au présent article* »[4].

> « C'est sur l'hébergeur que pèse la responsabilité d'être certifié ou agréé, et non plus sur les professionnels, établissements de santé et personnes concernées que pèse l'obligation de déposer les données auprès d'un hébergeur agréé »

L'hébergeur de ces données de santé à caractère personnel doit être titulaire d'un **certificat de conformité**[5]. Le décret du 26 février 2018[6] est venu définir et préciser la typologie des activités d'hébergement concernées et les conditions de délivrance du certificat[7].
Dans le cadre d'un service d'archivage électronique[8], notons que l'hébergeur doit être agréé par le ministre chargé de la Culture pour la conservation de ces données sur support papier ou sur support numérique. Un projet de décret soumis à consultation auprès de la commission européenne

3 Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé
4 Art. L1111-8 I CSP
5 Art. L1111-8 II CSP
6 Décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel
7 R1111-8-8 et suivants CSP
8 Art. L1111-8 III CSP

précise le périmètre des activités concernées ainsi que les conditions d'obtention de l'agrément. Si l'hébergeur est désormais visé, en premier lieu, par les dispositions précitées, **les responsables de traitements** qui confient l'hébergement de leurs données ne sont pas en reste, au titre :

- d'une part, du RGPD, et en particulier de leurs obligations de recourir à un sous-traitant présentant des garanties suffisantes, et de mettre en œuvre les mesures de sécurité appropriées ;
- d'autre part, du décret relatif à l'hébergement de données de santé, qui met à la charge des responsables de traitement l'obligation de s'assurer que l'hébergeur est titulaire du certificat de conformité concerné[9].

2 Elargissement légal du périmètre des acteurs concernés

C'est donc sur l'hébergeur que pèse la responsabilité d'être certifié ou agréé, et non plus, comme dans la version antérieure du texte[10], sur les professionnels de santé, établissements de santé et personnes concernées que pèse l'obligation de déposer les données auprès d'un hébergeur agréé.
Ce faisant le périmètre des acteurs concernés par les dispositions de l'article L1111-8 du code de la santé publique (CSP) a évolué ; il n'est plus circonscrit à une typologie délimitée.
Au titre de ces dispositions, c'est maintenant la nature des données, plus précisément leur origine, qui conditionne l'applicabilité des dispositions précitées.

3 Evolution légale du périmètre des données concernées

Ce sont désormais les données à caractère personnel du secteur sanitaire, mais aussi social et médico-social qui sont concernées.
En revanche, d'après la lettre du texte de l'article L1111-8 CSP, ce seraient uniquement les données recueillies à l'occasion de ces activités, et non plus également les données produites à ces occasions qui doivent être hébergées en environnement agréé ou certifié.
Pourtant, toujours d'après la lettre du même texte, pour que les dispositions soient applicables, il faudrait que l'hébergement soit réalisé pour le compte de personnes à l'origine de la production ou du recueil de ces données ou le patient lui-même.
La formulation de ces dispositions et leur articulation entre elles sont, à cet égard, pour le moins obscures, si ce n'est contradictoires.

4 Définition des activités concernées

Le décret du 26 février 2018[11] est venu définir et préciser la typologie des activités d'hébergement concernées :

- négativement, en excluant du périmètre des activités soumises à l'obligation d'agrément ou de certification, l'hébergement pour une courte période des données susvisées pour effectuer un traitement de saisie, de mise en forme, de matérialisation ou de dématérialisation de ces données[12] ;
- positivement, en proposant une liste limitative d'activités d'hébergement de données de santé à caractère personnel[13].

Ainsi, est considérée comme une activité d'hébergement de données de santé à caractère personnel, tout ou partie des activités suivantes :

- « 1° La mise à disposition et le maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé ;
- 2° La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé;
- 3° La mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;
- 4° La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;
- 5° L'administration et l'exploitation du système d'information contenant les données de santé ;
- 6° La sauvegarde des données de santé ».

Ces dispositions ont été schématisées[14] dans le référentiel d'accréditation, sous la forme du tableau suivant.
Il y a lieu de relever que les terminologies employées dans

9 Art. R1111-8-8 CSP
10 L1111-8 CSP version en vigueur avant le 28-01-2016
11 Décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel
12 Art. R1111-8-8 I 2° CSP
13 R1111-9 CSP
14 ASIP - référentiel d'accréditation HDS v1.1.

le décret précité et dans le tableau ci-dessus diffèrent légèrement, à des fins de clarification des activités qu'elles recouvrent.

Reste que **l'activité 5 soulève encore beaucoup de questionnements**. Telle qu'elle est formulée, elle pourrait en effet recouvrir les activités, en particulier de maintenance, des éditeurs de logiciels et fournisseurs de services de santé, même lorsqu'ils n'en assurent pas l'hébergement.
Saisi de cette problématique très impactante pour les acteurs du secteur, dès la parution du premier projet de décret, le ministère de la Santé a auditionné les industriels et devrait se positionner prochainement.

5 Certification et sous-traitance

A la lecture des dispositions du décret, la question se pose également de savoir s'il est possible pour un hébergeur certifié de recourir à des prestataires qui ne le sont pas pour tout ou partie de son service, et donc, pour un prestataire, de réaliser tout ou partie de l'une des activités visées par le texte sans être certifié, et ce en offrant ses services à un hébergeur certifié.
A cet égard, dès lors que le certificat de l'activité offerte est porté par un acteur de la chaîne, le schéma est valide.
En effet, **un hébergeur peut recourir à un sous-traitant non certifié** s'il respecte les exigences relatives à la gestion des relations avec les fournisseurs, prévues dans les normes[15], en particulier la 27001, étant toutefois précisé que, dans cette hypothèse, le changement de sous-traitant pourrait remettre en cause la certification de l'hébergeur ou, en tout état de cause, supposer un nouvel audit de l'organisme certificateur accrédité.

> « L'esprit du texte est d'assurer la sécurité des données compte tenu de leur sensibilité, peu importe la qualité des acteurs qui les traitent et les externalisent »

6 Limitation doctrinale du périmètre des acteurs concernés

D'après la lettre de l'article L1111-8 CSP, ainsi que précédemment développé, **c'est la nature des données qui conditionne l'applicabilité de ces dispositions**.
La problématique est donc celle de déterminer si les données objet de l'hébergement constituent des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social.
A cet égard, il convient de relever que l'esprit du texte est d'assurer la sécurité de ces données, compte tenu de leur sensibilité, peu importe la qualité des acteurs qui les traitent et les externalisent, étant rappelé que la Loi de modernisation avait justement supprimé les mentions permettant de les circonscrire aux seuls acteurs du secteur sanitaire.

Pourtant, **le champ d'application de ces dispositions a été circonscrit**, par la DSISS, dans une foire aux questions du 11 juillet dernier[16], aux seuls hébergeurs offrant leurs services à des acteurs du secteur sanitaire, social et médico-social, ou aux patients.
Seuls les « responsables de traitements de données de santé à caractère personnel ayant pour finalité la prévention, la prise en charge sanitaire (soins et diagnostic) ou la prise en charge sociale et médico-sociale de personnes », sont donc désormais tenus de recourir à un hébergeur certifié.
Cette doctrine vient limiter le périmètre des acteurs concernés par le cadre juridique relatif à l'hébergement de données de santé à caractère personnel.
Ainsi, en application de cette doctrine, peu importe que les données confiées à l'hébergement correspondent à celles directement visées par la lettre de l'article L1111-8, celui-ci ne s'applique pas à d'autres acteurs que ceux du secteur sanitaire, social et médico-social.
Des exemples *a contrario* excluent d'ailleurs du champ d'application de ces dispositions les organismes d'assurance maladie obligatoire et complémentaire, notamment, de même que les fabricants / fournisseurs / distributeurs de dispositifs médicaux, en dehors du cas où ils interviennent dans des activités de télésurveillance médicale (cette activité relevant du secteur sanitaire, social ou médico-social).

Cette toute nouvelle doctrine, qui bouleverse celle jusqu'alors en vigueur, tord le cou aux dispositions légales, et ce faisant, instaure **un régime « deux poids, deux mesures »** de l'hébergement des données de santé issues d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social.
Toutefois, les dispositions du RGPD imposent aux responsables de traitements de ces données de prendre les mesures techniques et organisationnelles appropriées pour assurer leur sécurité, c'est-à-dire respecter les référentiels sectoriels applicables, et donc finalement celui qui est applicable à l'hébergement des données de santé… Et la boucle est bouclée .

15 ASIP - FAQ HDS

16 DSSIS - FAQ HDS V. 12-07-2018 v0.10

ISO 27001, l'odyssée de la sécurité numérique

La certification ISO 27001, si elle ne constitue qu'une étape permettant de coller à la réalité des exigences (HDS, RGPD, …), est bien plus qu'un marqueur technique. Elle concrétise la coopération des professionnels au service de l'essentiel : soigner des patients dans les meilleures conditions d'efficacité et de sécurité possibles.

Un parcours varié (Industrie, Enseignement supérieur et Recherche, Santé), ainsi que des domaines d'activité balayant une grande diversité des métiers du SI (process industriel, développement, méthodes, formation) ont conduit **Philippe Tourron** vers la sécurité. Avec un fil rouge constant depuis 15 ans : la formation à la gestion des risques.
Après la mise en place de la PSSI à l'Université de la Méditerranée et la participation au déploiement national d'un kit PSSI pour les Universités, il s'est tourné vers un secteur où l'enjeu de sécurisation est vital. Après cinq ans à l'AP-HM (Assistance Publique Hôpitaux de Marseille), il peut faire état de trois agréments « Hébergeur de Données de Santé » et la certification ISO 27001 pour ce périmètre.

Convergence. C'est devenu une obsession dans beaucoup de domaines. Convergence des organisations avec les Groupements Hospitaliers de Territoire (GHT), convergence des systèmes d'information avec des schémas directeurs en cascade, convergence, voire hyper-convergence des technologies…
Mais on oublie parfois que la convergence nécessite une cible et une stratégie pour l'atteindre. En sécurité, comme ailleurs, on peut vite se perdre dans les méandres de solutions miraculeuses ou annoncées comme telles. Et si, finalement, tout convergeait vers un bon sens organisé ? C'est ce que propose l'ISO 27001 lorsque l'on sait lire entre ses lignes et en dégager l'esprit : connaître ses risques, les réduire à un niveau cohérent, se réévaluer pour s'améliorer.

Souci d'efficience, gage de validation externe

Pourquoi choisir une norme pour gérer la sécurité des systèmes d'information ? Avant tout, par souci d'efficience : éviter de refaire ce qui existe. Mais réutiliser, c'est aussi accepter et faire accepter que d'autres aient de bonnes idées, donc mettre l'ego de côté, ce qui est parfois difficile et peut être un frein à l'acceptation d'un cadre et de ses exigences, à l'acceptation du jugement des autres (obligation d'audit), mais aussi à l'obligation d'amélioration continue.
Préparez-vous donc à affronter tout ce qui amène un être humain à résister au changement.
Au-delà d'un modèle, pourquoi être certifié ? Avant tout, pour des raisons de survie face aux exigences (le cadre réglementaire d'Hébergement des Données de Santé par exemple), mais aussi parce que c'est le meilleur moyen de garder une dynamique avec des audits réguliers. C'est aussi le gage d'une validation externe et donc … incontestable, qui apporte la confiance et la satisfaction des gouvernances, des acteurs du SI et *in fine* des patients.

Le challenge d'une démarche ISO 27001 : un point d'équilibre à trouver entre les hommes, les organisations et la technique.

Ainsi adopter une norme et viser la certification est avant tout un travail sur les hommes qui décident, construisent et animent le SI pour qu'ils acceptent les changements indispensables à ce nouveau cadre dans lequel il ne suffit pas d'être professionnel mais aussi de le prouver.
L'ISO 27001 est une norme de management, comme l'ISO 9001. Elle conduit donc à accomplir aussi un travail sur l'organisation de la sécurité qu'il convient de prouver dans sa mise en place, son fonctionnement et son amélioration. Mais, contrairement à l'ISO 9001, la norme ISO 27001 intègre des exigences précises en termes de mesures à mettre en place et dont on ne peut déroger qu'avec un argumentaire en cohérence avec son analyse de risque (annexe A de la norme).

> « L'ISO 27001 est un accélérateur des grands chantiers SIH à venir »

Pourquoi mener cette démarche dans les structures de santé ?
On pense souvent que les normes sont réservées aux très grandes entreprises, aux industries, aux domaines où les enjeux sont avant tout financiers. Si je vous pose la question « *quel est le bien le plus précieux que vous souhaitez protéger par-dessus tout ?* », vous me direz … « *la santé* ». Alors oui, les systèmes d'information de santé valent la peine que l'on converge vers un cadre de gestion des risques comme nous avons su le faire depuis longtemps pour les risques sanitaires.
Une certification n'étant pas une fin en soi, la démarche d'amélioration continue qui l'accompagne est gage de confiance pour les patients, les professionnels de santé et les établissements de santé hébergés. Ainsi, tous les cadres réglementaires convergent aujourd'hui vers cette norme : HAS, certification des comptes, politiques de sécurité de l'Etat, du ministère chargé des Affaires sociales et de la Santé, de l'ASIP Santé, agrément HDS, RGS et RGPD. Par ailleurs, dans le contexte actuel de cybermenaces

permanentes, ciblant de plus en plus les données de santé et le développement de la e-santé, la norme permet de construire et de faire évoluer un modèle de sécurité adapté aux besoins des professionnels de santé et des patients.

Conduire un projet de certification ISO 27001 : Vision, Pédagogie, Pragmatisme et Agilité

Il faut avant tout convaincre les directions avec une **vision à trois-cinq ans**. Les enjeux sont nombreux : territoire, HDS, certification des comptes, GHT, Etat et ministère (LPM, directives DSSIS-309, NIS). La direction doit être sponsor et le leitmotiv doit être la confiance.

La stratégie SSI doit être comprise de la gouvernance, elle doit intégrer les enjeux (positionnement / territoire), valoriser l'établissement, garantir la conformité et permettre une maturité progressive.

Une organisation optimisée doit viser à s'appuyer sur tout ce qui existe pour démarrer (Commission, CoPil, certification HAS, …) pour montrer la plus-value d'une démarche qui n'ajoute pas de lourdeur administrative excessive

> « Adopter une norme est avant tout un travail sur les hommes pour qu'ils acceptent les changements indispensables à ce nouveau cadre dans lequel il ne suffit pas d'être professionnel mais de le prouver »

Quels impacts pouvez-vous espérer d'une certification ISO 27001 ?

L'ISO 27001 est un **accélérateur des grands chantiers SIH** à venir. La sécurité, souvent considérée comme une contrainte ou un centre de coût, est aujourd'hui une source d'opportunités, avec la mobilité, la dématérialisation, la signature électronique, l'accès des patients et des professionnels de santé au SI. Dans ce contexte d'ouverture, nous avons besoin d'une rigueur d'autant plus importante, permettant d'être éligible aux grands défis et aux exigences accrues concernant les données de santé (HDS et RGPD).

Enfin, le défi permanent qui fait la spécificité des établissements de santé est la diversité des applications et des éditeurs d'applications sur le périmètre du SIH « classique » mais aussi les périmètres concernant le biomédical ou la gestion technique.

Etendre progressivement le périmètre de la certification ISO 27001 et ses exigences est un **levier en termes d'organisation et de technique** pour amener nos applications, tous périmètres confondus, vers un niveau de sécurité cohérent avec la criticité de la santé des patients.

L'organisation induite par la certification ISO 27001 est aussi une **réponse au contexte actuel de cybermenaces** conduisant à gérer nos risques en temps réel avec une anticipation de type préventif et un entrainement nous permettant d'organiser la protection et la continuité des services en gestion de crise.

Réussir une certification ISO 27001 : une gestation en 9 étapes

- Etape 1 : Définir le **périmètre**, **structurer l'organisation** et motiver les acteurs. La communication et la pédagogie sont essentielles pour amener les acteurs à comprendre et accepter les changements. Les jeux de rôle sont un moyen efficace, sur des durées courtes, pour la compréhension des risques. Identifier des relais, des correspondants sécurité SI qui vous aideront à détecter des risques et à convaincre de l'application des mesures de sécurité.
- Etape 2 : Mettre en place une **gestion de crise** du système d'information car il y aura de plus en plus de situations complexes à gérer (cyberattaques, incidents sur les interdépendances des applications et des technologies, …). Le RSSI doit être le coach de ces moments pour entraîner les équipes à communiquer entre elles et avec les directions. L'entraînement à ces situations permettra de les anticiper en jouant des scénarios probables et garantira qu'au moment critique chacun sera conscient de son rôle.
- Etape 3 : **Analyser les risques** : c'est le point de départ de la cohérence des mesures à mettre en place pour garantir la sécurité. Une méthode pour être exhaustif et conforme ISO 27005 est indispensable : EBIOS est bien adaptée pour construire cette gestion des risques par agrégation de périmètre.
- Etape 4 : Intégrer le processus de gestion des risques dans la **pratique de la DSI** (cf. ITIL). Les processus de gestion des projets et des changements en amont, des incidents en aval, sont trois piliers permettant de garantir la pérennité du management de la sécurité dans les pratiques de la DSI.
- Etape 5 : Relier la **gestion de la sécurité à la réalité**. Associer toutes les procédures et les composants de sécurité à la Déclaration d'Applicabilité (DDA), corréler les mesures manquantes avec le plan de traitement des risques et construire la base de référence de questionnement pour l'audit interne.
- Etape 6 : Déployer **l'audit interne : former des auditeurs internes parmi les équipes de la DSI et de la Qualité.**
- Etape 7 : Prendre du recul : rédiger la **Politique de Sécurité de l'Information** (PSI). Elle doit formaliser les parties prenantes internes et externes, leurs exigences et leurs attentes et identifier les propriétaires des risques qui pourront décider de leur traitement.
- Etape 8 : Revenir à la réalité : rédiger les **politiques opérationnelles** correspondant aux périmètres techniques (postes de travail, serveurs, réseau, …) et/ou aux activités principales sur le SI (installer un serveur, déployer une application, fournir un téléphone portable, etc.).
- Etape 9 : Intégrer la gestion des risques dans le **schéma directeur** SI. Le traitement des risques devient une source d'orientation stratégique. La sécurité doit aussi être une valeur ajoutée : aujourd'hui elle est notamment le levier de la dématérialisation.

ISO 27001, de la difficulté présumée à l'utilité véritable

Il y a un réel retour sur investissement pour qui fait l'effort de connaître l'ISO 27001 et de s'y former. Sans nécessairement en devenir un spécialiste, disposer d'une vision générale et acquérir un vocabulaire commun seront des atouts indiscutables pour progresser individuellement ou au sein d'un groupement de territoire.

Ingénieur de formation, **Pascal Sabatier** participe aux nombreux projets de transformation du système d'information hospitalier. Depuis 2013, il est Responsable de la Sécurité des systèmes d'Information du Centre Hospitalier d'Aix-en-Provence et d'un groupement d'hôpitaux (Salon-de-Provence, Manosque et Digne). Depuis mai 2018, il assume également la fonction de Délégué à la protection des données.

Chacun a conscience du caractère stratégique du Système d'Information Hospitalier (SIH) et souhaite le protéger. Une intention louable mais qui peut s'évanouir face à la diversité des menaces relayées dans la presse spécialisée, au caractère pléthorique des référentiels sécurité ou encore à l'empathie bienveillante et intéressée des consultants certifiés.

Par où commencer ? La sécurité est une affaire de bon sens avant tout. Dès lors, une démarche logique conduit à sécuriser dans un premier temps ce qui apparaît comme le plus précieux. Une maison ne se protège pas de la même façon qu'il s'agisse du garage ou du cœur du foyer. L'analogie avec le SIH est possible à ceci près que vouloir sécuriser un SIH c'est vouloir sécuriser une auberge espagnole débordant de portes et de fenêtres.
Une méthode est nécessaire. La norme ISO 27001 en est une, incontournable. Elle est le socle commun de la PSSI de l'Etat, de la PGSSI-S, de la PSSI-MCAS.
L'idée selon laquelle cette norme ne serait applicable qu'à de grosses structures, et faite par des experts pour des experts, est une idée reçue dont il convient de s'affranchir.
Sa complexité est relative si vous l'abordez dans le cadre d'un projet précis et non avec l'ambition d'être conforme sur la totalité de la norme, ou d'être certifié.

Manager le risque ? Historiquement, la direction du système d'information (DSIO) prend en charge les risques liés à son domaine. Il est vrai que la DSIO est à même d'évaluer ce qui est critique en cas de d'indisponibilité ou de perte sur son périmètre.

La DSIO l'est un peu moins lorsqu'il s'agit d'évaluer les risques, les mesures de protection existantes et les mesures complémentaires pour l'ensemble du SIH, qui inclut les services biomédicaux, les services techniques, la recherche clinique, etc.
Encore moins s'il s'agit d'arbitrer des décisions sur des risques stratégiques relevant de la responsabilité du chef d'établissement.
C'est tout l'intérêt de cette norme qui spécifie les éléments nécessaires pour construire le système de management de la sécurité du SI (SMSI).

Une norme industrielle pour l'hôpital ? L'hôpital est un site industriel… qui ne se voit pas en tant que tel. Pourtant, un centre hospitalier est un site de production qui fonctionne 24h/24h, peuplé d'acteurs très différents, d'automates et de systèmes informatisés. Or la rigueur normative connue depuis longtemps dans les secteurs industriels de l'aviation ou de l'automobile peine à s'imposer en santé.
Ce constat peut s'étendre à l'ensemble des partenaires de l'hôpital, éditeurs et constructeurs, qui auraient pourtant stratégiquement tout à gagner (ou tout à perdre !) à intégrer et à appliquer les principes et mesures de ce référentiel.

Si les CHU sont déjà aguerris au SMSI de l'ISO 27001 (et ses dérivés, l'ISO 27002 pour les mesures et l'ISO 27005 pour l'analyse de risques), ils ne représentent qu'une petite minorité des structures qui composent le secteur médicosocial.
Or les enjeux sont les mêmes pour tous. La structuration en groupe hospitalier de territoire (GHT) va imposer une convergence. Cependant, l'attentisme optimiste qui compte sur la prise en charge de la problématique de la sécurité par l'établissement pivot du GHT est illusoire à court terme. Il est nécessaire que chacun se mette en marche, sur la base d'une méthode commune.
C'est dans ce contexte qu'être familier avec la norme prend tout son sens, quelle que soit la taille de l'établissement.

> « L'attentisme optimiste qui compte sur la prise en charge de la problématique de la sécurité par l'établissement pivot du GHT est illusoire à court terme. Il est nécessaire que chacun se mette en marche, sur la base d'une méthode commune »

ISO 27001, de la difficulté présumée à l'utilité véritable

Quels sont les intérêts de l'ISO 27001 ?

- Le gain de temps

La fourniture d'une méthode et d'une base documentaire structurée évite de se perdre et de réinventer ce que d'autres ont déjà pensé et formalisé. Le cycle PDCA (Plan, Do, Check, Act), aussi connu sous le nom de « roue de Deming », décrit toutes les étapes de planification, d'action, de contrôle et d'amélioration.
Il faut intégrer que gérer la sécurité du SI est un projet qui s'inscrit dans la durée et qu'au regard de l'échelle de temps, la première action à mettre en œuvre est la formation du pilote (RSSI) pour qu'il dispose de la vision globale de la norme.

- La visibilité

L'implication de la direction dans la gestion du risque SI est un principe fondamental de l'ISO 27001. Le modèle faisant reposer cette gestion sur les seules épaules de la DSIO disparait. La sécurité opérationnelle continue d'être gérée par la DSIO, mais les actions sont connues et arbitrées par un comité de pilotage présidé par le chef d'établissement.

- Le suivi des améliorations

Adosser les actions d'améliorations à un référentiel fini de mesures constitue un suivi mesurable de la progression. Il offre également la possibilité de se comparer en terme de maturité à d'autres établissements dans l'optique d'atteindre un niveau commun et de justifier l'allocation de ressources budgétaires.

- L'auditabilité

A l'heure du règlement général européen de protection des donnée, la capacité d'un établissement à produire des éléments de preuve sur sa sécurité est imposée.
Les processus d'audit interne et de gestion de la preuve font partie de la norme et structurent, de fait, l'auditabilité attendue par un auditeur (HAS, CAC, etc.)

> « La fourniture d'une méthode et d'une base documentaire structurée évite de se perdre et de réinventer ce que d'autres ont déjà pensé et formalisé »

Les 3 C de la sécurité des SI : conformité, communication, confiance

Comment garantir la confiance dans le système d'information alors que des changements majeurs s'annoncent, liés notamment aux enjeux territoriaux ? Les réponses tiennent en deux mots : conformité et communication.

Guillaume Jeunot, Responsable Sécurité du Système d'Information et Délégué à la Protection des Données du Groupement Hospitalier de Territoire 85, est également membre de la SOFGRES (Société Française de Gestion des Risques en Établissement de Santé). Il anime différents groupes de travail sur l'intelligence économique dans le secteur de la santé et sur l'évolution des enjeux Cyber dans l'administration pour diverses associations d'auditeurs de l'IHEDN (Institut des Hautes Etudes de Défense Nationale).

Nos systèmes d'information connaissent une profonde mutation qui passe par une évolution de la gouvernance de notre système de santé et des changements d'échelle de mise en œuvre des SI. Elle coïncide avec une prise de conscience collective de la valeur, et donc de l'intérêt, des données de santé, qu'elles soient ou non à caractère personnel. Dans le même temps, le nombre d'attaquants, la diversification de leurs profils, s'accroissent. Ils disposent de moyens et d'une technicité qui, pour certains, ne peuvent que nous laisser rêveurs. Alors quel est le devenir de la sécurité des SI (SSI) ? Quelle expression doit-elle prendre?

Faire accepter une évaluation du risque

Je me souviens d'une discussion, lors d'un de mes premiers projets d'informatisation de la prescription en hôpital, avec un médecin réfractaire à l'informatique. Aucun argument technique ne pouvait le convaincre que le niveau de sûreté que nous proposions était acceptable. A court d'arguments que j'estimais rationnels, j'ai décidé de m'absenter deux minutes afin d'illustrer un type d'acte malveillant. J'ai descendu un étage. Comme je m'y attendais, il y avait là un chariot, avec des dossiers patients, seul dans le couloir tandis que les soignants étaient entrés dans la chambre d'un patient. J'ai donc saisi un dossier que j'ai pu apporter à mon interlocuteur en l'invitant : « Faites de même sur mon système ! » Vous imaginez la suite...
Idéalement, nous serions garants de la mise en sûreté des informations de notre système, mais la sécurité, c'est-à-dire l'acceptation d'un certain niveau de risque, correspond mieux à la réalité. Avec ma petite histoire, je tenais à montrer la difficulté de faire accepter une évaluation du risque tant notre écosystème est complexe et tant nos interlocuteurs sont de profils différents. Alors qu'un ensemble de normes et de méthodes peut nous aider à qualifier ces évaluations (en particulier sous les angles de la disponibilité, de l'intégrité, de la confidentialité et de la traçabilité), nous restons face à des êtres humains avec leur histoire et leur part d'irrationnel. Dans le fond, qu'exigent-ils de nous ? Leur garantir la confiance dans le système d'information auxquels ils participent.
Comment faire émerger et maintenir cette confiance ? Comment faire en sorte que cette confiance irradie dans tout l'écosystème de nos établissements ? C'est bien LA question à laquelle doit répondre le RSSI.

De nouvelles échelles de définition des SI

Aujourd'hui nous entrons dans l'ère des SI que je qualifierais de troisième génération, du type « virtualisé ».

Selon ma classification, la première génération correspond au type « mainframe » qui permettait, avec une seule solution embarquant tout, de l'infrastructure au logiciel, de répondre à un besoin d'un service ou d'une fonction. La deuxième génération - je la qualifie de type « urbanisé » - que nous connaissons aujourd'hui et qui fait la part belle au progiciel, est établissement centré.

Cette période verra le développement des architectures orientées services ou ressources, la généralisation de l'externalisation type IaaS, PaaS et autres SaaS. Elle verra des changements majeurs dans l'organisation des DSI et bien entendu dans la manière d'aborder les questions en lien avec la sécurité. Les réponses aux enjeux de territoires de santé et de réseaux spécialisés de santé qui sont les nouvelles échelles de définition des SI, seront les espaces de confiance. Elles bousculeront dans leurs habitudes nombre d'acteurs qui avaient encore des difficultés à appréhender ce qu'est un système d'information. Ces nouveaux modèles ne sont pas intuitifs et s'ajoutent à la complexité existante (par exemple par l'apparition des mécanismes de blockchain et de modèles non prédictifs).
Nous connaissons également une accélération de la production du corpus réglementaire, sans pour autant voir l'augmentation de moyens nécessaires à son application. Cela nous amène à appréhender de manière différente la gouvernance de la SSI. Le RGPD, notamment, nous oriente vers des approches du type GRC (Gouvernance,

Les 3 C de la sécurité des SI : conformité, communication, confiance

Risque, Conformité). L'objectif, au-delà de la sécurité, est de permettre cette confiance « car il importe de susciter la confiance »[1].

Comme la sécurité incendie

Trop souvent perçues comme des contraintes, ces réglementations sont au contraire une chance. Une chance car elles nous imposent un cadre opposable. Qu'est ce qui est le plus rassurant pour un utilisateur ? Une présentation d'ingénieur expliquant la mise en place d'une PSSI pour les réseaux à base de pare feu et de règles de gestion des protocoles TCP-IP et de ports 443 ? Ou la présentation d'un rapport de conformité à la réglementation? Personnellement, je penche pour la deuxième réponse car les démarches qualité sont dorénavant bien admises dans nos établissements.

Avec l'accroissement de cette exigence de conformité, notre métier de RSSI pourrait se définir par : auditer et être audité. J'ajouterais que c'est également communiquer.

La SSI est un peu comme la sécurité incendie, elle doit être partout et qu'on ne la voit pas. Pourtant elle est essentielle. Les règles doivent être connues, les personnels doivent être formés, ou à minimum sensibilisés, les procédures éprouvées et les indicateurs monitorés. La SSI doit donc orchestrer des actions coordonnées d'experts de tout type. Mais elle est également l'affaire de tous et doit se faire au contact des autres pour répondre à la réalité de nos organisations. Elle doit être expliquée et comprise pour être acceptée car, comme la sécurité incendie, on n'en mesure tout l'intérêt que quand l'incident se produit.

En conclusion, vouloir garantir la sûreté reviendrait à ressembler à ces Danaïdes condamnées aux enfers à veiller sur un système d'information sans fond. Ce serait également s'astreindre à un zèle qu'aucune autorité crédible ne pourrait nous imposer. L'objectif rationnel est certes d'être en mesure d'assurer la conformité aux différentes réglementations mais il est surtout de veiller à l'amélioration continue de la sécurité au plus près des utilisateurs. L'enjeu est dans la communication par la sensibilisation et le partage d'indicateurs pertinents. Cette communication permet l'acceptation des vulnérabilités et donc de la confiance de nos utilisateurs (médecins ou agents), donneurs d'ordre et bénéficiaires. Cette confiance qui est essentielle à l'adhésion des projets, à rendre chacun, acteur de la sécurité. Elle permet alors l'acceptation des changements et de pouvoir relever les défis à venir.

Du latin confidere: cum, « avec » et fidere « fier », la confiance est l'acceptation des vulnérabiltés. La confiance renvoie à l'idée que l'on peut se fier au SI.

« Du latin confidere: cum, « avec » et fidere « fier », la confiance est l'acceptation des vulnérabiltés. La confiance renvoie à l'idée que l'on peut se fier au SI »

1 § 7 des considérations de la RGPD (https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679)

Une cartographie unifiée des SI ou comment maîtriser ses risques

La cartographie unifiée des systèmes d'information n'est plus une option, mais un point d'entrée indispensable à toutes les autres fonctions du SI. Sa compréhension et sa mise en œuvre s'organisent autour de cinq axes, détaillés par Didier Pescarmona.

Président de PREF-SI Conseil, consultant SSI et RGPD, Expert Ekialis Explore et Pilot, **Didier Pescarmona** est autodidacte. Il a réalisé son parcours professionnel au sein de la DSI de l'UNEDIC, Telindus, Capella Conseil et Cosialis Consulting. La création de PREF-SI Conseil, en 2017, s'appuie sur une conviction profonde : la nécessité d'apporter un conseil pragmatique, simple et efficace à ses clients. Il les accompagne dans leur transformation numérique sur quatre grands domaines : Protection du Patrimoine Informationnel et cybersécurité, RGPD, Gouvernance et Organisation. Expert en cartographie des SI depuis 10 ans, ses interventions permettent aux acteurs de la gouvernance d'obtenir une vision partagée des actifs de leur patrimoine informationnel et de ses données, contribuant à une amélioration permanente de la maîtrise des risques et des changements.

Les DSI, RSSI, DPO et leurs équipes sont confrontés à trois injonctions majeures : garantir la conformité légale et règlementaire (RGPD, HDS, Commissaire aux comptes, directive Network and Information Security, …), œuvrer à la convergence des SIS et rendre le service aux patients et aux utilisateurs dans les conditions de disponibilité et de sécurité attendues. La complexité des systèmes d'information de santé (SIS) rend cette tâche ardue. Dans ce contexte, une cartographie unifiée des SIS s'avère indispensable tant pour maîtriser les risques opérationnels que pour préparer les évolutions des architectures applicatives et techniques.

> « La cartographie offre une vision partagée et une connaissance dynamique du patrimoine informationnel et de ses données entre les acteurs de la gouvernance »

Quel état des lieux pouvons-nous dresser aujourd'hui des cartographies des SIS ? Dans la très grande majorité des cas, l'information est disséminée dans un nombre incalculable de fichiers Excel®, de schémas Visio®, de diaporamas, de documentations, sans oublier les connaissances propres à chaque acteur et non formalisées.

Cette atomisation des données ne permet pas de disposer d'une information globale à jour et fiable. Les conséquences de cette situation sont multiples : pas de vision exhaustive des actifs des SIS ; nécessité de consacrer beaucoup trop de temps à la recherche de l'information juste ; difficulté pour apporter les éléments de réponses probants aux autorités ; difficulté pour anticiper avec certitude les conséquences d'un changement ; incapacité à maitriser les impacts d'une défaillance pour décider et organiser la gestion de crise.

Le temps est venu de changer de paradigme : la cartographie unifiée des SIS n'est plus une option. Elle est un point d'entrée indispensable à toutes les autres fonctions du SI.
Sa compréhension et sa mise en œuvre s'organisent autour de cinq axes.

Axe 1 : Un référentiel unique des actifs du SIS

Il regroupe, par organisation, l'ensemble des actifs du SI qu'il est indispensable de connaître et de maîtriser : les applications, les flux de données, les données maitres, les composants d'infrastructure, de réseau et de sécurité, les sous-traitants, fournisseurs et partenaires, les traitements de données à caractère personnel, les certificats, les équipements biomédicaux, etc.

Axe 2 : Des actifs du SIS liés par des relations de dépendances

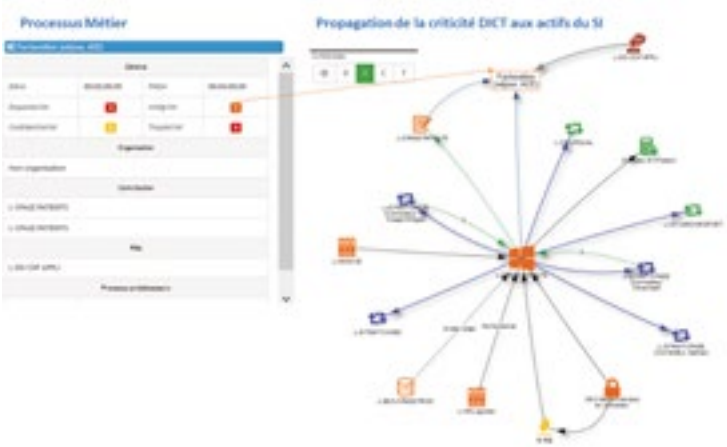
Les relations entre composants permettent de décrire et de visualiser leurs liens. Les analyses d'impact exploitent ces relations, par exemple, en préparation des changements ou en réponse à des incidents ou dysfonctionnements. Elles apportent une réponse opérationnelle à la maîtrise des risques.

Axe 3 : Un référentiel des processus métiers et de

Une cartographie unifiée des SI ou comment maîtriser ses risques

leurs besoins de sécurité DICT

Il contient les processus métiers en s'appuyant sur le référentiel de l'oSIS[1] qui constitue une excellente base de départ. La définition des besoins de sécurité DICT[2], en lien avec le référentiel des impacts et des conséquences de la PSSI-S, doit se faire au niveau du processus. Une contribution vers le ou les composants en contribution au fonctionnement du processus permet de propager ses besoins de sécurité DICT aux composants en relation avec les contributeurs. Cette fonction permet de s'assurer que les mesures de protection sont présentes sur tous les composants de la chaine des actifs : applications, flux, serveurs, bases de données, fournisseurs, sous-traitants, etc. Cette matérialisation du besoin de sécurité du processus via la propagation de la criticité DICT est un point d'entrée indispensable à toute analyse de risques pour aboutir à une classification juste des actifs.



Axe 4 : Un référentiel unique des documentations

La documentation constitue le socle de tous les systèmes qualité, dont le SMSI. Les documents de référence (fiches réflexes, dossiers de sécurité, dossiers d'architecture, cahiers de paramétrage, contrats,…) présents dans l'espace collaboratif et associés à chaque composant ou processus garantissent la présence et le partage de l'information.

Axe 5 : Un partage dynamique de l'information entre acteurs du SI

La cartographie offre une vision partagée et une connaissance dynamique du patrimoine informationnel et de ses données entre les acteurs de la gouvernance. Chaque acteur, selon son périmètre de responsabilité, enrichit le référentiel permettant aux différentes instances de gouvernance SSI, RGPD,… de disposer d'une aide à la décision, d'indicateurs et de tableaux de bord, reflets d'une réalité opérationnelle.

En conclusion, cette approche pragmatique de la cartographie des actifs et des processus permet de revenir au concept de base d'une cartographie à savoir: couvrir toute la chaine de l'information traitée en se concentrant sur ce que l'on utilise réellement !

1 Observatoire des systèmes d'information de santé
2 Disponibilité, Intégrité, Confidentialité, Traçabilité

(L'inévitable) guide d'hygiène de l'ANSSI

S'il est un sujet, en sécurité des SI, où l'on ne craint pas la pénurie, c'est bien celui des guides et référentiels. Mais s'il ne restait qu'un document à garder dans la masse documentaire qui s'accumule d'année en année, ce serait sans nul doute le guide d'hygiène de l'ANSSI[1] .

Cédric Cartau, RSSI et DPO du CHU de Nantes et du GHT44, est également chargé de cours à l'EHESP et à l'ESIEA. Il collabore régulièrement à la revue DSIH et a publié plusieurs ouvrages, notamment « La sécurité du système d'information des établissements de santé », seconde édition (Eyrolles, 2017).

Paru dans une première mouture en janvier 2013, le guide d'hygiène de l'ANSSI a détonné dans le paysage. Que l'on en juge : en seulement 40 mesures, pour la plupart simples, il prétendait guider les professionnels de la SSI dans les actions à mettre prioritairement en place. On y trouvait pêle-mêle des mesures organisationnelles (formation des acteurs), techniques (segmentation des réseaux), dédiées utilisateurs, ou dédiées aux administrateurs système, etc. Le guide a évolué en 2017 pour être entièrement revu, et comporte maintenant **42 mesures, réparties en 10 domaines et notées selon deux niveaux** (standard et avancé).

A la première lecture, tout Responsable Sécurité du SI (RSSI) sent le sol se dérober sous ses pieds : autant de mesures, pour la plupart simples, que l'on est incapable de mettre en œuvre dans nos établissements. Autant de mesures qui se situent dans ce qu'il est convenu d'appeler la zone d'humiliation : il s'agit de la zone dans laquelle, si un incident majeur survient, nous n'aurons que nos yeux pour pleurer tellement il était évident que telle ou telle mesure de protection devait être mise en œuvre… et pourtant on ne l'a pas fait. Quel établissement de santé impose à ses administrateurs système la séparation de son compte agent de celui de son compte admin ? Quels réseaux sont correctement segmentés pour isoler les équipements qui n'ont aucune protection antivirale ? Combien de salles informatiques sont localisées dans des locaux ouverts à tout le personnel, sans aucune habilitation d'accès ?

Le minimum syndical

Certes, on trouve aussi des mesures qui sont la plupart du temps mises en œuvre : sécurisation du Wi-Fi, déploiement d'un pare-feu, activation des journaux système, etc. Mais l'impression, à la fin de la première lecture, est que l'on dispose d'une grosse marge de progression, ce qui est peu dire.
Comment utiliser ce document, sans se noyer dans les détails ? La mauvaise stratégie consisterait à déposer le document sur le bureau du DSI en lui disant qu'il a trois mois pour tout mettre en œuvre : échec assuré. La bonne stratégie consiste à déterminer, de façon conjointe et avec les professionnels de la DSI, les cinq ou dix mesures – c'est selon – sur lesquelles il faut en priorité concentrer les efforts. Chacun fera son choix, mais sensibiliser (I-1), disposer d'une cartographie à jour (II-4), sécuriser les accès administrateur (III-8 et III-11), les postes de travail (IV-14) et segmenter le LAN semblent constituer le minimum syndical. Et surtout, surtout, faire rentrer ces points dans des revues régulières, courtes et maîtrisables pour s'assurer de leur progression.

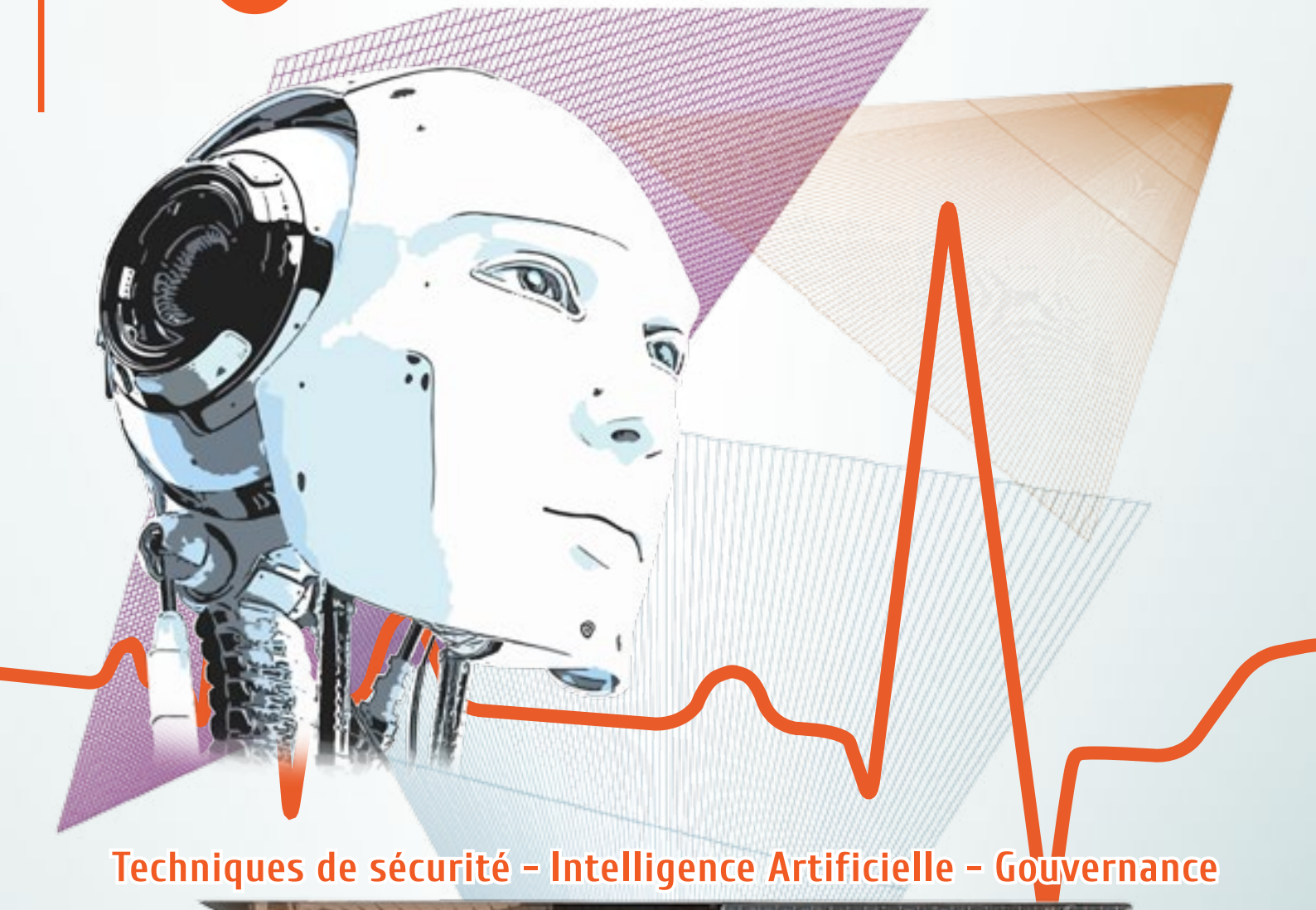
> « Avec le déferlement normatif, en SSI, que le monde de la santé vient de connaître, les établissements ne pourront plus dire qu'ils ne savaient pas »

L'autre levier pour le RSSI est de faire le lien avec des réglementations opposables. La récente directive NIS[2], qui va s'appliquer aux futurs Opérateurs de Services Essentiels (entre autres, à la plupart des établissements de santé qui disposent d'un service d'urgences) comporte des dispositions qui sont dans mentionnées dans le guide : obligation de tenir une cartographie à jour, de disposer d'une démarche SSI structurée, d'auditer, etc.

Alors le guide de l'ANSSI n'est clairement pas un guide de plus. S'il n'y en avait qu'un à retenir, ce serait celui-là. Avec le déferlement normatif, dans le domaine de la SSI, que le monde de la santé vient de connaître (pas moins de six textes majeurs depuis 2016), les établissements ne pourront plus dire qu'ils ne savaient pas.

1 Agence Nationale de la Sécurité des Systèmes d'Information. https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
2 https://www.ssi.gouv.fr/actualite/adoption-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la-transposition-en-france/

Le Mans - 2, 3 & 4 avril 2019



Techniques de sécurité - Intelligence Artificielle - Gouvernance

7ème Congrès National de la Sécurité des Systèmes d'Information de Santé

APSSIS

LE MANS DEVELOPPEMENT

0.2 GOUVERNANCE DE LA SSI SANTÉ

Direction du Système d'Information : cap sur l'océan du numérique, **Didier Bonnet** P. 23 & 24
Quand sécurité des SI, qualité et gestion des risques ne font qu'un, **Elodie Jamet** P. 25 & 26
Fonctions et priorités du RSSI, **Nour Kadi** P. 27
RSSI / chargé de sécurité : des liens étroits, **Stéphan Thamier** P. 28 & 29
Certification HAS : retour d'expérience, **Yohann Fourchon** P. 30 & 31
Une approche de la sécurité sous l'angle des projets, **Thierry Veauvy** P. 32
Sensibiliser, sans relâche, **Christophe Le Callonec** P. 33
La « gamification » ou « jeux sérieux » au service de la sensibilisation !, **Auriane Lemesle** P. 34 & 35
Le CHU de Rouen vise l'unité d'actions, **Jacques Ferrand et Cédric Hamelin** P. 36 & 37

Direction du Système d'Information : cap sur l'océan du numérique

Le poids des années présente des inconvénients, mais un avantage certain : celui de l'expérience. Je vais essayer de vous faire partager la mienne quant au rôle de la Direction du Système d'Information d'un groupe hospitalier public et de son pilote dans cet océan numérique où évoluent des professionnels, mais aussi des pirates et autres malfaisants, voire des inconscients, et où surviennent tempêtes, défaillances, fortunes de mer et autres difficultés qui peuvent mettre en péril la mission de nos institutions.

Après 15 ans au service de la Marine nationale (hydrographe puis informaticien), **Didier Bonnet** change de cap en 1990 et intègre une SSII comme Administrateur de projet, Ingénieur qualité (certification AFAQ), Responsable puis Directeur de projet et Responsable de pôle de compétences régional. Huit ans plus tard, il rejoint, en tant que Directeur de grands projets, le Syndicat Inter-hospitalier de Bretagne où il découvre le monde la santé. Il rejoint en 2001 le CH de Saint Brieuc comme Responsable SI. Il va y vivre quelques belles aventures (télédialyse, téléimagerie). En 2010, il prend la direction du Système d'Information des CH de Lannion et de Saint-Brieuc, par fusion des services informatiques, puis élabore (2014) le Schéma Directeur Communautaire du SI pour les cinq établissements qui vont constituer le Groupe Hospitalier d'Armor (Saint-Brieuc, Lannion, Guingamp, Paimpol, Tréguier). Il y crée la DSI commune, en mode centre de services.
Dans la région, il a été, en outre, Directeur Technique du GCS e-santé Bretagne, de 2007 à 2009.

Depuis quelques années maintenant, l'époque est définitivement révolue où les outils informatiques aidaient leurs utilisateurs dans des tâches annexes, relevant de l'accessoire. Nos hôpitaux n'ont pas échappé à cette révolution culturelle qui porte irrémédiablement l'accès à l'information numérique au même niveau que l'accès à l'eau, ou à l'électricité. Aujourd'hui, les professionnels de santé, comme nombre d'autres professionnels, ne peuvent plus exercer leur activité première sans accès à des données numériques et aux outils qui les véhiculent et ce, sans délai. En clair, la fiabilité, l'accessibilité et les performances de nos systèmes d'information et de leurs contenus influent directement sur la qualité de prise en charge du patient, y compris dans sa dimension vitale. La Direction du Système d'Information se voit ainsi investie d'un niveau de responsabilité sans commune mesure avec ce qu'elle assumait précédemment.

Dans une autre vie professionnelle, j'ai exercé le métier de marin. La mer est un environnement hostile pour ceux qui la pratiquent, peu stable, imprévisible et très versatile, ressemblant ainsi au monde numérique d'aujourd'hui. De cette expérience, j'ai acquis des réflexes basés sur la maîtrise des risques, quotidien d'un commandant de bateau et de son équipage, comparable à celui d'un Directeur du Système d'Information (DSI) et de ses équipes.

Le DSI, comme le commandant d'un navire, doit être le garant de la mission qui lui est confiée, à savoir dans le cas du DSI, celui de garantir - dans cet ordre - la disponibilité, la fiabilité, les performances ainsi que la confidentialité des outils et informations numériques nécessaires - toujours par ordre d'importance - à la prise en charge des patients (mission première de l'hôpital), à la gestion logistique et administrative. Tout comme un navire ravitailleur se doit d'être en mesure de délivrer du carburant, des munitions, de la nourriture, etc. à l'ensemble des navires de la flotte.

> « Le DSI, comme le commandant d'un navire, doit être le garant de la mission qui lui est confiée »

Systématiser l'analyse bénéfice/risque

Dans la liste des fondamentaux, l'approche par la maîtrise des risques rythme en permanence le quotidien du DSI qui se doit de l'insuffler au sein de son équipage et ce, au plus profond des activités. Dans ce domaine, je commencerai par la systématisation de l'analyse bénéfice/risque avant d'engager quelque action que ce soit, et accompagnée de quelques automatismes : à quel niveau d'implication l'action contribue-t-elle à la mission ? Quels sont les bénéfices attendus et à quelle échéance ? Quels sont les risques associés et leur niveau de probabilité ? Les indicateurs environnementaux sont-ils favorables ? A quel moment l'action est-elle pertinente ? Ai-je la puissance, la taille (en gros les moyens) ? Etc.
Systématiser cette approche permet d'objectiver les éléments et souvent l'analyse s'arrête dès les premières interrogations... La même approche appliquée aux actions récurrentes est aussi une manière de réinterroger la pertinence des processus de la DSI.
Je compléterai cette analyse bénéfice/risque par le principe de l'alternative ou de la continuité de service. Celui-ci consiste à garantir, autant que faire se peut, la mission en cas de défaillance totale ou partielle et ce en commençant par la notion de secours ultime, ou comment conserver un minimum de disponibilité d'information lorsque plus rien ne fonctionne (désastre majeur)... En clair : les radeaux de survie et les bouées couronnes.
Pour terminer, j'ajouterais la notion de « pied de pilote »[1] ou

1 La hauteur d'eau ajoutée pour une opération déterminée (entrée dans un port, pratique d'un chenal, passage d'un seuil, évitage, etc) qui constitue une marge de sécurité additionnelle.

Direction du Système d'Information : cap sur l'océan du numérique

de marges de manœuvre en cas d'événement ou d'incident. A savoir : quel est mon champ de latitude, ai-je les expertises, les ressources, sur tel ou tel sujet ? Puis-je reprendre la main en cas de défaillance de fournisseur ? Faire appel à un tiers de confiance ? Etc.

L'organisation et la formation de l'équipage à bord d'un navire sont également fondamentales et contribuent fortement non seulement à la réalisation de la mission mais également à la sécurité du bateau et de ses passagers. Chacun doit connaître parfaitement son poste et son rôle (les manœuvriers sur le pont, les mécanos à la machine...) et respecter les consignes à bord : je referme une porte étanche après mon passage, je n'engage pas une manœuvre tant que tout le monde n'est pas à son poste, etc. Pour les équipes d'une DSI, c'est la même chose. L'organisation doit être claire et adaptée à la cible.
Pour notre DSI, notre organisation différencie la délivrance des services numériques (le « run », qui est la mission première) de l'évolution des outils (le « build »). Les processus sont formalisés et chacun reçoit la formation qui lui permet non seulement d'assurer sa mission mais aussi de contribuer activement à la sécurisation commune du SI.

Concernant les passagers, nos utilisateurs, le DSI et ses équipes doivent impérativement faire preuve de pédagogie et leur faire percevoir, sans exagération mais avec précision, les possibilités, mais aussi les risques et les contraintes, de cet environnement qui devient de plus en plus exclusivement numérisé. Tous ont appris à l'école à lire dans des livres et à écrire sur du papier. Aujourd'hui ces supports disparaissent et les principes de la communication et du partage de l'information ont complètement évolué. Il est donc impératif de les accompagner dans l'appropriation de ce nouveau contexte, en attendant que l'éducation prenne le relais… mais il faudra un certain temps.

Le RSSI, en amont des prises de décision

Dans cette mission complexe, le DSI et ses équipes sont épaulés par le Responsable Sécurité du SI dont l'expertise, l'objectivité et la maîtrise des dispositions réglementaires et des principes à l'état de l'art offrent un angle de vue précieux. Dans notre organisation, ce dernier intervient dès les phases de conception et en amont des prises de décision. Les équipes de la DSI fonctionnent en transparence complète avec le RSSI, permettant d'insuffler son approche au plus près de l'action.

Pour terminer, le DSI et ses équipes se doivent de mettre à disposition leur expertise et leur savoir-faire pour permettre aux directions des établissements de bâtir leur stratégie en matière de patrimoine informationnel en conservant la maîtrise nécessaire pour l'accomplissement de leur mission de service public auprès de la population.

Il est difficile en si peu de mots de croquer le rôle de la DSI et de son manager car la mission revêt aujourd'hui un spectre particulièrement large et un niveau de responsabilité accru. La globalisation et l'externalisation croissante des outils et des informations renforcent la nécessité, pour les institutions comme les hôpitaux, de se doter d'une DSI de haut niveau d'expertise, notamment pour garantir la maîtrise complète du patrimoine informationnel relatif aux fonctions vitales nécessaires pour exercer leur mission première, à savoir soigner la population et ce dans n'importe quelles circonstances, y compris en temps de crise comme lors d'un événement climatique majeur ou d'un conflit.

> « Chacun doit connaître parfaitement son poste et son rôle et respecter les consignes à bord »

Quand sécurité des SI, qualité et gestion des risques ne font qu'un

Pourquoi confier la sécurité des systèmes d'information à un profil spécialiste de la gestion des risques ? Cette fonction, transversale, implique de côtoyer tous les acteurs de l'établissement et de développer une vision par « processus », points forts pour assurer les missions de RSSI.

Elodie Jamet est diplômée de l'Ecole Supérieure d'Ingénieurs en Agroalimentaire de Bretagne Atlantique (anciennement ESMISAB). Elle a occupé différents postes d'Ingénieur qualité et gestion des risques en établissements de santé, dans l'agro-alimentaires et le négoce. En 2017, elle a été recrutée par le Centre Hospitalier du Centre Bretagne, issu de la fusion des hôpitaux de Pontivy et de Plémet-Loudéac, établissement support du Groupement hospitalier de Territoire du Centre Bretagne.

La sécurité des systèmes d'information n'est pas un thème très évocateur pour bon nombre de nos concitoyens. Malgré une volonté à tous les niveaux dans notre vie courante de dématérialiser les supports d'information, beaucoup d'usagers sont encore néophytes et parfois très méfiants envers l'informatique par manque de connaissance des outils et surtout des aspects liés à leur sécurité. Le personnel hospitalier a un comportement semblable à celui d'une majorité des Français, dès lors qu'il utilise l'informatique dans son champ professionnel. L'informatisation est encore très couramment « subie » malgré les avantages indéniables qu'elle apporte dans l'amélioration de la prise en charge du patient par une meilleure traçabilité des soins, un meilleur suivi des séjours et des examens, la rapidité des échanges entre les professionnels… Dans les services de soins, l'informatisation débute généralement par le circuit du médicament puis s'étend aux autres activités de l'établissement de santé, en parallèle des applications utilisées par les services administratifs.

Des situations ubuesques

Il est très courant de voir un membre de l'équipe informatique désigné Responsable Sécurité du Système d'Information (RSSI) et rattaché au Directeur des Systèmes d'Information. Les applications, les infrastructures et les dispositifs techniques de sécurité ne sont-ils pas déployés par le service informatique ? L'informaticien n'est-il pas celui que l'on contacte lorsqu'une application ne fonctionne pas comme elle devrait ? Celui-ci fait alors de son mieux pour assurer la disponibilité des outils, n'anticipant pas suffisamment l'impact sur les organisations ou la survenue probable de défaillances. Le RSSI a dès lors un rôle important à jouer dans l'évaluation des risques qui découlent de l'utilisation de ces « nouveaux » outils.

Bon nombre de situations ont démontré que les dysfonctionnements proviennent du comportement des utilisateurs du système d'information et non des techniques. Il en découle des situations ubuesques dans lesquelles il est demandé aux directions des systèmes d'informations de mettre en place des dispositifs très coûteux alors qu'il serait plus judicieux d'agir sur les organisations et le comportement des utilisateurs. Mais agir sur le comportement de ses collègues peut se révéler difficile lorsqu'on est amené à travailler avec des machines en mode binaire…
C'est dans ce contexte que le centre hospitalier dans lequel j'exerce a préféré confier la sécurité des systèmes d'information à un profil spécialiste de la gestion des risques plutôt qu'à un expert technique : l'ingénieur qualité et gestion des risques.

Des compétences complémentaires

Titulaire d'un diplôme d'Ingénieur en qualité et gestion des risques, je ne m'attendais pas à me voir un jour attribuer cette mission exaltante et complexe. Après avoir fait part de mon étonnement lors de mon recrutement, je vois, en examinant de plus près les différentes missions du RSSI que la gestion du risque est prépondérante. En effet, l'informatisation supprime ou réduit certains facteurs de risques, mais elle en génère également, que ce soit au niveau du traitement des informations ou du comportement des utilisateurs… Mes compétences viennent donc en complémentarité de celles des informaticiens. J'apporte un œil externe, une vision basée sur l'évaluation des risques afin de définir un risque acceptable.

> « Bon nombre de situations ont démontré que les dysfonctionnements proviennent du comportement des utilisateurs du système d'information et non des techniques »

Ma formation initiale m'a permis de voir que les méthodes apprises dans la gestion des risques et la mise en œuvre ou le suivi de plans d'action, peuvent aisément être utilisées dans une multitude de secteurs dès lors qu'un climat de confiance se crée avec les experts métier et que ceux-ci acceptent de m'expliquer leur jargon ! Il est à noter que cet exercice constitue aussi pour eux un très bon entrainement. Mon collègue responsable du service informatique, auquel j'adresse un clin d'œil dans cet article, a donc bien voulu m'expliquer les différentes facettes du système d'information de l'établissement, les techniques utilisées, leurs principes et modes de fonctionnement …

Passée cette difficulté, j'ai découvert un domaine semblable à d'autres. Je m'étonne presque de ne pas voir plus de ges-

Quand sécurité des SI, qualité et gestion des risques ne font qu'un

tionnaires de risques assurer des fonctions de RSSI. Il est vrai que la mission est encore relativement récente, j'ose donc espérer que nous ouvrons la voie à de nouveaux profils ! Et si possible que ce domaine attire plus de profils féminins !

Et demain… DPO

Un autre avantage du cumul des deux fonctions d'Ingénieur qualité et gestion des risques et de RSSI porte sur le rôle transversal de ma première fonction dans ses missions. En effet, elle implique de côtoyer tous les secteurs et acteurs de l'établissement au travers des différents sujets traités, de comprendre les missions des uns et des autres, le fonctionnement des équipes, de faire du lien entre les différents services, ô combien cloisonnés. La curiosité devient donc une qualité et non plus un défaut! De plus, la démarche qualité et gestion des risques s'appuie sur le signalement d'évènements indésirables. L'analyse de ceux-ci exige de se renseigner auprès des différents intervenants impliqués dans la situation afin de conduire des comités de retour sur expérience pour comprendre la survenue de l'incident, trouver des actions d'amélioration pour éviter qu'il survienne à nouveau.

Je fais souvent le constat que cette vision par « processus» manque aux techniciens informatiques, malgré leur rôle également transversal, lorsque j'assiste à des congrès ou comités dédiés à la sécurité des systèmes d'information. Mes collègues se focalisent sur la technique, le côté opérationnel du dispositif ou de l'outil. Je vois que bon nombre d'entre eux ne sont pas suffisamment informés du fonctionnement des services. Cette situation n'est pas exclusivement de leur fait. La taille de l'équipe informatique peut en être la cause, la disponibilité des outils étant la priorité. De plus, il est malheureusement fréquent qu'ils ne soient contactés qu'une fois les projets validés, pour installer telle ou telle application…

Bref, la mission de RSSI ressemble à un puits sans cesse alimenté par une source de nouveaux risques et pleine de promesses en termes d'amélioration des pratiques. Elle me permet aussi une nouvelle fois d'assurer un rôle transversal dans l'établissement et tout naturellement de mieux comprendre comment les données sont protégées. Rien d'étonnant par conséquent, que tous les regards se soient portés sur moi lors de l'entrée en application du Règlement européen sur la protection des données…
Avec les compétences requises pour les missions citées précédemment, nul doute que beaucoup de RSSI, et peut-être de gestionnaires de risques, deviendront aussi des Délégués à la protection des données !

> « Les méthodes apprises en gestion des risques et mise en œuvre de plans d'action peuvent être utilisées dans une multitude de secteurs dès lors qu'un climat de confiance se crée avec les experts métier et qu'ils acceptent d'expliquer leur jargon »

Fonctions et priorités du RSSI

Le travail du RSSI consiste à protéger l'hôpital, ses patients et ses actifs numériques en aidant la direction à prendre les décisions les plus pertinentes et les moins risquées. Il présente aussi l'intérêt de faire progresser le sujet de la sécurité au sein des équipes.

Ingénieur en informatique et télécommunications, **Nour Kadi** a soutenu une thèse dans le domaine des réseaux sans fil dans le cadre du Laboratoire de Recherche en Informatique de l'Université Paris-Sud, à Orsay. Elle est actuellement Responsable de la Sécurité du Système d'Information au sein du Groupement Hospitalier de Territoire Orne-Perche-Saosnois, en Normandie.

Les besoins de partage de données ne cessent d'augmenter, entre patients et médecins, avec les agences gouvernementales, les laboratoires, les compagnies d'assurance... Par ailleurs, de plus en plus d'informations sensibles sont collectées et stockées par les établissements de santé, faisant de ces derniers une cible privilégiée pour les pirates. Améliorer et optimiser la sécurité informatique est donc devenu une priorité. Ce qui signifie qu'il faut identifier les risques et gérer les incidents lorsqu'ils se produisent afin d'assurer la continuité d'activité et de préserver la valeur de l'information.

En l'absence d'un RSSI, l'établissement de santé serait obligé de répartir cette responsabilité entre différents postes, ce qui aggraverait le risque de voir des problèmes prendre racine dans des zones non gérées. Un risque qu'aucune organisation de santé ne devrait accepter.

En nommant un RSSI, l'hôpital peut en revanche compter sur un spécialiste capable de faire progresser le sujet de la sécurité informatique.

Les cinq fonctions prioritaires du RSSI sont :

1. Développer des programmes de sécurité pour tout l'établissement

Protéger les actifs numériques de l'établissement est le travail le plus important du RSSI au quotidien. Gérer la cybersécurité et garder l'établissement à l'abri des cybermenaces n'est pas une tâche simple. C'est pour cela que la priorité de premier ordre consiste à protéger les portes d'entrée numériques.

2. Identifier, signaler et contrôler les incidents

Les incidents cybernétiques fusent de toutes parts et se produisent tout le temps. Quand ils arrivent, c'est le devoir du RSSI de les connaître et d'agir. Sa première tâche consiste à identifier qu'une tentative d'agression a lieu. Cela signifie avoir mis en œuvre les bons outils et services pour détecter et prévenir les menaces. Une fois le problème identifié, il doit être signalé. Le niveau de signalement devrait être défini par le niveau de menace ou de conséquence de l'attaque. Les intrusions quotidiennes, même lorsqu'elles sont stoppées, doivent être consignées et signalées à la communauté de sécurité afin que d'autres attaques puissent être évitées. Les menaces qui entraînent des violations ou vols de données doivent être signalées aux autorités compétentes. Au RSSI de préparer un plan afin d'identifier comment et à qui ces différents niveaux d'intrusion seront signalés.

3. Créer une culture de cybersécurité au travail

L'erreur humaine reste en effet la principale cause des violations de données, et ces violations causent aux organisations beaucoup de dommages financiers et entachent leur réputation. Pour cette raison, les employés doivent être formés régulièrement pour aider le RSSI à fournir une protection adéquate.

C'est le travail du RSSI d'informer l'ensemble du personnel sur les méthodes utilisées par les cybercriminels, de les former et de les éduquer collectivement.

En somme, de développer une culture de cybersécurité pour atteindre deux objectifs importants:

- mêler étroitement les pratiques de sécurité à l'exercice des différents métiers.
- démontrer que la sécurité n'est pas une fonction simplement reléguée au service informatique.

> « Développer une culture de la sécurité, c'est mêler étroitement les pratiques de sécurité à l'exercice des différents métiers »

4. Surveiller les menaces et prendre des mesures préventives

Les cyberattaques proviennent d'un ensemble de sources en nombre croissant. Le RSSI, partie intégrante de la communauté mondiale de la cybersécurité qui surveille et explore ces sources, permet le partage d'expériences et de connaissances avec d'autres experts et peut fournir des avertissements préalables concernant les menaces actuelles et futures.

5. Communiquer en continu

Le RSSI communique régulièrement avec la direction en lui transmettant des indicateurs exploitables. Il aide aussi les dirigeants à prendre des décisions efficaces qui permettent d'atteindre un équilibre entre les exigences opérationnelles et les exigences en matière de sécurité.

RSSI / chargé de sécurité : des liens étroits

Les missions du RSSI et du chargé de sécurité (incendie et sûreté) sont étroitement liées. Le plan de sécurisation des établissements (PSE) prévoit d'ailleurs des mesures concernant les SI. Rappel des principales dispositions.

Titulaire d'une licence en Gestion des risques et d'un master 2 en Sécurité intérieure, **Stéphan Thamier** est chargé de la sécurité (incendie et sûreté) du Centre Hospitalier de Montauban depuis 2002 et RSSI depuis 2017.

Le bon fonctionnement hospitalier est devenu dépendant du système d'information. La sécurité du système d'information (SSI) est un sujet stratégique dans le monde de la santé. L'importance prise par cette thématique résulte de l'informatisation croissante : dispositifs médicaux, dossiers patients, gestion administrative, gestion technique des bâtiments….
Le système d'information (SI) ne se réduit pas à l'informatique. Il regroupe l'ensemble des moyens humains, techniques et organisationnels visant à assurer le traitement, le stockage et l'échange d'informations nécessaires aux activités de l'établissement. La sécurité du système d'information permet de lutter contre les risques qui ont pour origine des défauts de conception, de développement, d'usage, ou la malveillance (vol d'information, usurpation d'identité, modification de configuration et diffusion d'informations confidentielles…) et la compromission via des virus.

PSSI et sécurité physique du SI

Dans le **Guide d'aide à l'élaboration d'un plan de sécurisation d'établissement** (PSE) d'avril 2017[1] (page 25), il est question des différentes mesures de sécurisation des SI à mettre en place. De plus une fiche conseil (n°4 en page 49) « Incident de sécurité sur un poste de travail informatique » est recommandée. L'instruction n° SG/HFDS/DGCS/2017/219 du 4 juillet 2017[2], relative aux mesures de sécurisation dans les établissements et services sociaux et médico-sociaux évoque également (partie 1-3) la prise en compte de la sécurité des SI.
Les éléments cités ci-dessus sont logiquement compris dans la politique de sécurité du système d'information (PSSI) de l'établissement, qui est obligatoire, et annexés au PSE.
Un des volets de la PSSI met en avant la sécurité physique du SI. C'est sur ce point que les objectifs sont communs. En effet, il faut protéger le SI comme tous les autres biens du centre hospitalier. Sauf que sa particularité est de toucher toutes les activités : soins, logistique, technique, administratif….

Mesures spécifiques

Les principaux objectifs sont :

- d'empêcher les accès physiques non autorisés (protéger les zones sensibles), les dommages et interférences vis-à-vis de l'information et des installations techniques ;
- d'empêcher la perte, l'endommagement, le vol ou la compromission du matériel et, surtout, d'éviter l'interruption des activités.

La protection contre les menaces physiques et environnementales est réalisée à partir d'une analyse de risques des zones sensibles ou locaux névralgiques (stockage contenant des informations confidentielles, salle serveur, de téléphonie, onduleur...) et des risques locaux.
Des mesures spécifiques assurent la sécurité du SI en protégeant les installations techniques et les zones sensibles afin de réduire les risques de menaces potentielles de type catastrophe naturelle ou d'origine humaine, attentat, vol, vandalisme, destruction humaine ou animale, incendie, fumée, explosion, fuite d'eau, inondation, poussière, vibrations, effets engendrés par les produits chimiques, chaleur ou froid, interférences avec le secteur électrique, interférences sur les lignes de télécommunication, rayonnements électromagnétiques…

> « Un contrôle des droits d'accès physiques aux zones sensibles doit être fait au moins une fois par an par le service sécurité avec le RSSI »

Les éléments à mettre en place

Quels sont les principaux éléments à retenir concernant **la sécurité physique du SI ?**

- les accès physiques aux zones sensibles et leur périmètre doivent être protégés par des mécanismes de contrôle (verrouillage des portes extérieures et fenêtres des bâtiments des zones sécurisées, fenêtres de rez-de-chaussée spécifiquement protégées) ;
- l'accès physique aux zones sensibles doit être limité au strict besoin des missions et les visiteurs doivent être signalés et accompagnés ;

1 https://solidarites-sante.gouv.fr/IMG/pdf/guide_d_aide_a_l_elaboration_du_pse_-_version_avril_2017.pdf
2 http://circulaires.legifrance.gouv.fr/pdf/2017/07/cir_42445.pdf

RSSI / chargé de sécurité : des liens étroits

• un contrôle des droits d'accès physiques aux zones sensibles (habilitation) doit être fait au moins une fois par an par le service sécurité avec le RSSI ;

• la signalétique des zones sensibles doit être discrète et fournir le minimum d'indications ;

• l'enregistrement vidéo, photo ou audio est interdit en zone sensible (hors la vidéo protection) ;

• des systèmes de détection d'intrusion doivent être installés. Ceux-ci doivent être activés en permanence lorsque les zones sensibles sont inoccupées. Il peut également être ajouté un système de vidéoprotection.

• des systèmes de détection et de protection incendies doivent être installés (les salles serveurs sont souvent protégées par une installation d'extinction automatique à gaz) ;

• la surveillance et la maintenance doivent être assurées sur : l'électricité, les télécommunications, l'alimentation en eau, le gaz, l'évacuation des eaux usées, la ventilation, la climatisation, la sécurité incendie, l'intrusion…

• la sécurité du câblage doit être prise en compte (type de câblage, séparation, enfouissement, marquage…) ;

• la sortie du matériel informatique doit être formalisée (autorisation…) ;

• la sécurité du matériel hors des locaux doit être respectée (pas de matériel sans surveillance, rédaction d'une charte) ;

• la mise au rebut et le recyclage sécurisé du matériel doivent être réalisés correctement (effacement, par qui et comment …) ;

• la politique de l'écran vide doit être généralisée (verrouillage de l'écran, gestion des identités et des accès, mots de passe robustes…).

En conclusion, la sécurité numérique est l'affaire de tous. Elle repose avant tout sur des mesures simples et des bonnes pratiques à adopter sans modération dans la sphère aussi bien privée que professionnelle, tout comme on adopte les consignes Vigipirate.

Certification HAS : retour d'expérience

Jusqu'à présent, la démarche d'amélioration continue que constitue la certification HAS était assez éloignée des préoccupations des directions de système d'information. Dans le contexte GHT, elle devient la doctrine principale d'une DSI qui souhaite se transformer en centre de services.

Yohann Fourchon est Responsable Sécurité du Système d'Information ainsi que Délégué à la Protection des Données au sein du Groupement Hospitalier d'Armor (Bretagne). Il fait partie de la DSI de GHT qui compte un peu plus de 50 personnes. Travaillant auparavant en milieu industriel, il a rejoint le secteur de la santé en 2002 sur des compétences qualité/gestion des risques en établissement de santé. En 2011, il s'oriente dans le domaine des systèmes d'information en qualité de référent sécurité du SI. Après l'obtention d'un master II en Management des Risques SI, il est nommé RSSI de la CHT d'Armor début 2016, devenue GHT d'Armor en juillet 2016.

Initiées en 2002, les visites de certification en sont à leur 4ème itération (V1, V2, V2010 et V2014), chacune de ces itérations présentant des changements, soit de périmètre, soit de référentiel. Dans la dernière version, la méthodologie a été remise à plat. Désormais, il convient que l'établissement réalise une analyse de risques (tiens, tiens !, c'est une notion qui rencontre un écho dans le domaine du système d'information), afin d'identifier les risques principaux sur le périmètre de la certification, de proposer, puis de suivre, des actions correctives, visant à réduire ces risques.

Un exercice périlleux

Ce retour d'expérience porte sur la 4ème itération (V2014) réalisée au sein de notre groupement hospitalier de territoire (GHT). **Premier groupement à réaliser une visite de certification sur un périmètre communautaire** (en 2016), notre GHT a fait le choix, après avoir bien pesé les bénéfices et les risques, de proposer la thématique « Gestion du Système d'Information », comme thématique communautaire investiguée par les experts-visiteurs. En effet, il s'agit d'un exercice périlleux, dans un contexte de mutualisation de la fonction SI, ce, au début de la transformation des DSI des cinq établissements en DSI communautaire (dans un mode centre de service). Cela signifie que le système d'information a été investigué individuellement dans chacun des cinq établissements membres du GHT mais il a aussi fait l'objet d'une évaluation à l'échelle du GHT. Il faut souligner que cette thématique est rarement investiguée par les équipes d'experts-visiteurs (seulement dans 6,6 % des visites de certification)[1].

> « Vous n'avez pas besoin de voir tout l'escalier, empruntez juste la première marche (Martin Luther King) »

Travaux préparatoires ?

Tout d'abord, il convient comme pour tout projet d'identifier un pilote (appelé « pilote de processus » dans le jargon) qui va coordonner la démarche pour cette thématique. Dans notre cas, le RSSI a assuré cette mission, sachant qu'il avait une bonne connaissance du processus de certification, ayant travaillé auparavant au sein de la cellule qualité/gestion des risques. A ce titre, il avait déjà eu l'occasion de coordonner la démarche dans sa globalité. Cela aide, mais après tout, le RSSI est le gestionnaire des risques spécialisé dans le domaine du système d'information.
De plus, c'est également le RSSI qui a assuré la responsabilité du suivi du programme Hôpital Numérique (HN). Et il se trouve que HN, qui a servi de tremplin pour la démarche de sécurité du système d'information (notamment pour sa démocratisation), constitue également un bon marchepied pour la certification HAS.
D'ailleurs, l'analyse de risques SI, réalisée quelques mois plus tôt afin de satisfaire aux prérequis HN, a été conçue de façon à pouvoir être réutilisée dans le cadre de la certification HAS. Toutefois, il a fallu collaborer avec les directions Qualité pour que la méthodologie (EBIOS) puisse s'intégrer dans les outils développés par les qualiticiens pour les autres thématiques.
Les fondations de la démarche étaient posées. Ensuite, comme dans toute démarche de certification, il faut être en capacité de justifier le respect des référentiels et de la bonne réalisation des engagements pris dans les politiques, par la production de documentation, la conservation d'éléments de traçabilité et le suivi d'un tableau de bord.

Harmoniser les pratiques dans les établissements du groupement

Tout l'intérêt, dans cette approche communautaire, c'est que la démarche mutualisée a permis d'harmoniser les pratiques dans les établissements du groupement, et éga-

1 HAS, *Certification HAS V2014 – Bilan à mi-parcours*, Mai 2017

lement de limiter le temps nécessaire à la préparation de ces visites.
Enfin, les cinq visites des experts-visiteurs se sont déroulées sur quatre mois. Dans chaque établissement, une rencontre de l'équipe SI et d'un expert-visiteur était organisée. Afin d'assurer la cohérence globale de la démarche, l'équipe SI était constituée du DSI de GHT, du RSSI de GHT et du RSI historique de l'établissement.
Dans leurs restitutions et leurs rapports de certification, les experts-visiteurs ont salué la démarche engagée sur la thématique SI (trois établissements évalués à 96,4 % et deux établissements évalués à 100%).
Si ces bons résultats constituent un satisfecit pour la démarche engagée, ils ont aussi permis de la crédibiliser auprès des directions d'établissement, ainsi que des professionnels de santé. Mais attention, il s'agit juste d'une photo à l'instant T, et la roue (de Deming) continue …
Loin de s'endormir sur ses lauriers, la DSI a souhaité transformer l'essai en s'engageant dans une **certification ISO 27001**, démarche similaire dédiée à la maitrise des risques des systèmes d'information. En effet, au sein des GHT, le système d'information constitue un moyen majeur de convergence, tandis que la maîtrise des risques du système d'information (SSI) constitue le gage de confiance. Il est donc primordial que la maîtrise du système d'information s'appuie sur la démarche d'amélioration continue pour conserver, et même accroître, la confiance des patients et des professionnels, surtout dans le cadre d'une transformation en centre de services.
Vous l'aurez compris, il est important de définir une stratégie claire et lisible en se fixant des objectifs et des échéances atteignables. En effet, l'escalier de la démarche d'amélioration continue est long et parfois sinueux. Il est primordial de le monter marche après marche, plutôt que de les monter quatre à quatre, au risque de trébucher ou de s'essouffler !

La démarche de certification

L'établissement transmet son auto-évaluation à la Haute autorité de santé afin que l'équipe d'experts-visiteurs en prenne connaissance. Ces derniers, professionnels exerçant dans le milieu sanitaire (médecin, directeur, personnel d'encadrement, qualiticien) se rendent dans l'établissement afin de vérifier que la philosophie de l'amélioration continue est bien ancrée dans les pratiques des professionnels rencontrés. Sur la base de leurs investigations, les experts-visiteurs produisent un rapport de visite, qui est transmis au collège de la certification. Ce dernier statue sur la décision de certification (A à E). Selon les résultats obtenus, soit l'établissement reçoit une nouvelle visite (dans les quatre à six ans), soit il doit produire un rapport complémentaire sous quelques mois, ou enfin, dans les situations les plus délicates, il doit organiser une nouvelle visite des experts dans des délais courts. Les résultats de la certification HAS sont rendus publics sur le site web de l'organisme.

> « Hôpital Numérique, qui a servi de tremplin pour la démarche de sécurité du système d'information, constitue également un bon marchepied pour la certification HAS »

Une approche de la sécurité sous l'angle des projets

L'intégration de la SSI à la racine des projets métiers constitue une méthode efficace d'adhésion aux principes de sécurité. Retour d'expérience et analyse de Thierry Veauvy, Responsable Sécurité des Systèmes d'Information et Référent Informatique et Libertés - CHU de Toulouse & Institut Universitaire du Cancer Toulouse – Oncopole.

Thierry Veauvy RSSI aux Hôpitaux de Toulouse depuis 2010, ancien consultant sécurité auprès de grands comptes français et internationaux.

Au CHU de Toulouse, le RSSI, Thierry Veauvy, est convaincu que la sécurité des SI nécessite une approche adaptée en regard du contexte de l'entreprise, de son activité, de sa culture, de sa maturité et de beaucoup d'autres paramètres. Le challenge du RSSI est d'atteindre les objectifs de sécurité en employant une méthode adaptée à cet « écosystème ». La voie royale du SMSI (ISO 27001) est bien sûr une piste évidente mais pas forcément accessible à tous. D'autres approches sont possibles.

> « La sécurité est un ensemble de contraintes qu'il faut idéalement transformer en réflexe »

La sécurité est souvent perçue comme génératrice de contraintes. Pour faire évoluer cette perception, le RSSI du CHU de Toulouse évoque une approche de la sécurité des SI sous l'angle des projets : « Dans mon ancienne vie de consultant, cette stratégie était mise en œuvre dans de grandes entreprises industrielles et tertiaires et cela fonctionne bien. En faisant abstraction du SMSI en cours de mise en place pour des contraintes spécifiques au sein du CHU, nous avons et continuons à mettre en place cette approche historique au CHU de Toulouse et les résultats sont très encourageants. »

Etre à l'écoute des métiers

L'idée simple et pragmatique est de ne rien imposer, mais d'accompagner et de faire découvrir les enjeux. « Certes, cela est consommateur, mais efficace ».
C'est ce qui explique d'ailleurs que le métier de RSSI requiert de nombreuses qualités, dont l'empathie, la communication et la pédagogie. Thierry Veauvy souligne l'importance de la compréhension du cœur de métier et du dialogue. « Il faut demander aux acteurs ce dont ils ont peur. Ces craintes sont faciles à recueillir, très bien connues des métiers, plus simples à exprimer qu'un risque… Aujourd'hui, il est nécessaire de faire de la sécurité par les risques mais il est souvent compliqué de traiter ces aspects par des méthodes complexes, le pragmatisme est très utile. »
« Imposer une PSSI de 100 pages en disant : voici le référentiel, voici le cadre à respecter, et l'imposer au chef de projet, ne fonctionne que rarement. Il faut construire un « référentiel projet », avec le métier et tous les acteurs, en échangeant. Ils vont ainsi s'approprier les enjeux, le contenu. Le RSSI, qui connait les « vrais » référentiels fera ensuite le lien et s'appuiera sur ce qu'il connait pour atteindre des objectifs partagés ».
« Il faut être à l'écoute des métiers de manière simple et modeste » …

Un RSSI «Yes, we can»

« Dans les projets, je me positionne toujours à la place du patient, de l'usager, de l'utilisateur. » Ainsi, par la compréhension des métiers au-delà de la technique, par la présentation et l'usage d'outils simples, par le fait d'insister sur ce que le métier connait et sur ce qu'il redoute, sans forcément exprimer un risque, le RSSI pourra aider à bâtir, dans le cadre du projet, un référentiel de sécurité compris, partagé et appliqué par tous. À l'usage et s'appropriant les enjeux, les métiers ne conçoivent plus les déploiements sans y inclure la sécurité en amont. « Et surprise ! … Les métiers deviennent sponsors, et redemandent de la sécurité. Elle n'est plus vue comme une contrainte mais comme faisant partie intégrante du processus. »
Un RSSI « Yes, we can », et non plus « Dr No » en quelque sorte.

Thierry Veauvy résume alors le challenge d'un RSSI : « La sécurité est un ensemble de contraintes qu'il faut idéalement transformer en réflexe. Pour que les gens aient ces réflexes, ils doivent comprendre pourquoi et s'approprier les pratiques ».

Labelliser ?

Les éditeurs et fournisseurs de produits et solutions doivent, eux aussi, progresser. « Dans la santé, la sécurité est trop souvent délaissée par les éditeurs », regrette Thierry Veauvy. « Trop souvent, la solution proposée répondra parfaitement aux besoins et aux exigences des soignants mais l'application pourra être truffée de vulnérabilités. Pourquoi pas un label ? Sujet difficile, mais à creuser … »

Sensibiliser, sans relâche

Malgré l'accélération de la dématérialisation, le personnel reste, dans le secteur santé, trop peu sensibilisé aux failles de sécurité. Au RSSI d'agir, dans la continuité, et en faisant preuve de créativité, face à des personnels qui se caractérisent par une grande diversité et, souvent, un fort turn over.

Christophe Le Callonec, RSSI et DPO auprès de la direction générale de Clinalliance/Repotel, est également responsable du suivi des projets de transformation numérique. Son parcours professionnel lui a permis d'évoluer des fonctions d'agent de service à aide-soignant, puis infirmier. A la sortie de l'école des cadres de santé, en 2007, il prend en charge un poste de directeur des soins et le projet d'informatisation du dossier patient. Son mémoire de Master 2 Management des établissements et organisations de santé porte sur « le coût humain de la dématérialisation du dossier patient : impact de l'informatisation sur le travail des soignants en soins de suite ».

Riche en interactions humaines, la santé draine une masse d'informations importante. En dix ans, ce secteur est passé du recueil sur supports papier, stockés dans une armoire de salle de soins, à une dématérialisation visant le zéro papier. Progressivement, et suite à différents projets de modernisation (Hôpital 2012, Hôpital numérique, et bientôt Hop'En), la transformation numérique modifie le paysage de la santé et, de ce fait, impacte les pratiques sous l'effet de la dématérialisation.

Si, auparavant, un déplacement était nécessaire pour consulter un dossier, dorénavant on accède à la donnée de toutes parts. Que ce soit horizontalement, dans un service de soins, verticalement d'un étage à l'autre, transversalement depuis un autre site, le décloisonnement est total, au point de donner naissance à des territoires de santé numériques.

L'acquisition ou le renouvellement des technologies s'inscrit comme une priorité dans les projets d'établissements. Les sites de groupements hospitaliers de territoire doivent communiquer facilement, rapidement, et de manière commune. Si les financements et investissements permettent l'accélération de cette dématérialisation, le personnel reste toutefois peu sensibilisé aux failles que présente cette facilitation d'accès à la donnée de santé.

Un personnel conquis mais néophyte

La progression fulgurante des technologies de l'information et de la communication au sein des établissements de santé embarque un personnel globalement conquis mais néanmoins néophyte.

De tous temps, le rapport avec le patient s'est joué sur le registre de la proximité. Si le personnel est soucieux de bien faire au chevet du patient, l'évolution dans un contexte virtuel multidimensionnel demeure récente.

A l'instar des responsables Qualité, le RSSI est en charge de mettre en œuvre le système de management de cette sécurité et de projeter les personnels dans un environnement où l'intrusion pourrait provoquer un incident grave sur le parcours du patient.

Le caractère multi disciplinaire des personnels - médicaux, paramédicaux et médico-techniques - vient complexifier cette tâche. En plus des supports ludiques, bien souvent la sensibilisation passe par une revue des textes législatifs qui entourent ces professions afin que l'impact soit plus fort (secret professionnel, etc.).

Faire preuve de créativité

Le turn-over important conduit le RSSI à dispenser cette sensibilisation le plus fréquemment possible et à faire preuve de créativité afin que sa réactualisation intéresse les nouveaux arrivants comme les anciens.

Sans oublier que d'autres catégories de personnels transversaux gravitent autour du patient : agents de service ou agents d'entretien, brancardiers, etc., disposent parfois de supports (tablettes ou autres) pour saisir diverses informations concernant leur activité.

Enfin, les activités nécessitant des connexions à distance exposent également la sécurité des systèmes d'information laissant l'utilisateur maitre du contenu auquel il accède ou qu'il embarque.

Des instructions ou règlements parus en 2016 dont l'application est effective en 2018 pointent cette obligation de sensibilisation des personnels. La HAS rappelle également cette nécessité dans la certification des établissements. Pour autant, le RSSI doit faire preuve de créativité pour donner de l'impact aux contenus qu'il dispense et les adapter en fonction des personnels qu'il accueille. Le facteur humain demeure essentiel dans la sécurité, sans distinction de fonctions et de tâches. La quantification par un indicateur, par catégorie d'acteurs, pourrait contribuer au suivi de cette sensibilisation à la sécurité des SI.

> « Le facteur humain demeure essentiel dans la sécurité, sans distinction de fonctions et de tâches »

La « gamification » ou « jeux sérieux » au service de la sensibilisation

Sensibiliser n'est pas chose aisée, surtout quand il s'agit de sujets perçus comme contraignants voire techniques... mais avec le jeu, rien d'impossible ! En 2018, à l'occasion du mois européen de la cybersécurité, l'ARS Pays de la Loire, le GCS e-santé Pays de la Loire et QualiREL Santé ont lancé un nouvel outil de sensibilisation pour les structures de santé de la région : l'escape game « Sant'escape, sécurité numérique ».

Groupe de travail coordonné par le GCS e-santé Pays de la Loire. De haut en bas et de gauche à droite :
Adrien Bourdon, technicien informatique, Association d'Hygiène Sociale de la Sarthe (AHSS)
Guillaume Jeunot, RSSI et DPO, GHT 85
Auriane Lemesle, Référente régionale Sécurité des SI, GCS e-santé Pays de la Loire
Marion Lucas, chargée de missions, QualiREL Santé
Anne-Laure Comtois, chargée de missions, QualiREL Santé
Gérard Gaston, RSSI et DPD, LNA-Santé
Nolwenn Renon, chargée de communication, GCS e-santé Pays de la Loire
Charlène Quentin, Responsable qualité et gestionnaire des risques, AHSS
Charlotte Hérique, Responsable Qualité - Gestion des Risques

La genèse du projet

Le nombre et la sophistication des menaces sur les systèmes numériques ne cessent d'augmenter de manière générale, mais également de manière plus ciblée sur le secteur de la santé / social. L'exploitation des vulnérabilités liées aux mauvaises pratiques des utilisateurs est également en constante augmentation. Partant de ces constats, au-delà de l'obligation de sensibilisation de l'ensemble des personnels, le rappel régulier des bonnes pratiques à mettre en œuvre et des règles à respecter en matière de sécurité numérique semble indispensable. Les traditionnelles formations nécessitent d'être complétées par d'autres modalités de formation impliquant davantage les apprenants.

Depuis plusieurs années, le GCS e-santé Pays de la Loire, missionné par l'Agence Régionale de Santé, s'applique à diversifier les outils de sensibilisation sur la sécurité numérique en santé. L'équipe souhaitait proposer un nouvel outil, moins formel, plus dynamique, où les personnes formées s'impliqueraient et deviendraient actives dans l'apprentissage. Le jeu dans les environnements de travail a plusieurs atouts et est apparu comme adapté aux objectifs : implication des apprenants grâce à l'aspect ludique et pragmatique, renforcement de l'esprit d'équipe, valorisation des compétences de chacun, réflexion logique et inventivité…

> « L'équipe souhaitait proposer un nouvel outil, moins formel, plus dynamique, où les personnes formées s'impliqueraient et deviendraient actives dans l'apprentissage »

Une collaboration régionale

Créé avec Orange Cyberdéfense, l'escape game est aussi le fruit d'une belle collaboration avec quatre structures régionales qui ont constitué le groupe de travail : l'Association

La « gamification » ou « jeux sérieux » au service de la sensibilisation

d'Hygiène Sociale de la Sarthe, LNA-Santé, le Groupement Hospitalier de Territoire 85 et QualiREL Santé. Il paraissait indispensable d'impliquer des acteurs de terrain pour vérifier la pertinence du scénario tant sur les aspects techniques, qu'organisationnels. La diversité des profils (sécurité des SI, qualité et gestion des risques, protection des données personnelles, communication) a été un véritable atout pour mener ce projet sur un temps très court, de juin à septembre ».

Un escape game qui sensibilise aux bonnes pratiques en matière de sécurité numérique

« Cinq journalistes peu scrupuleux s›introduisent dans une salle de réunion de l›Institut médical des étoiles des Pays de la Loire pour découvrir pourquoi Johnny Jackson a été pris en charge par cette structure. Les bonnes pratiques de base en matière de sécurité numérique ont-elles été bien suivies dans cet établissement ou seront-elles la clé d›accès aux informations de santé de l›inventeur du Lune Walk ? Ils ont 45 minutes pour trouver le scoop et rebooster les ventes du journal Ouest People ! » Voici le scénario de notre escape game ciblant la sensibilisation à la sécurité numérique.

Au terme des 45 minutes de jeu, une session de débriefing permet aux participants de partager leur ressenti, d'analyser ensemble les conséquences des mauvaises pratiques. Enfin, l'importance des actions individuelles au service d'une démarche collective est rappelée et des documents de sensibilisation sont remis à chaque participant.

Un outil fédérateur

Sant'escape Sécurité numérique est à la disposition des directions d'établissement désireuses de mettre en place un outil de team building pour renforcer l'esprit de collaboration et l'efficacité collective ; des gestionnaires de risques souhaitant mettre en place de nouvelles méthodes de diffusion des bonnes pratiques ; des référents ou responsables SSI et DPO pour sensibiliser et faire connaître leurs actions, parfois encore méconnues.

La diffusion de l'outil auprès des structures ligériennes s'effectue au travers d'une formation à la mise en œuvre et à l'animation de session de jeu. Un kit de ressources est remis aux participants afin d'organiser la communication dans l'établissement et de faciliter la mise en place.

Sant'escape : une offre régionale

L'ARS Pays de la Loire, soutient la structuration d'une offre régionale d'escapes games au sein d'une appellation unique: « Sant'escape ». L'outil de sensibilisation à la sécurité numérique est la première réalisation d'un catalogue amené à s'enrichir de nouvelles thématiques : qualité, sécurité des soins, e-santé...

> « Au terme des 45 minutes de jeu, une session de débriefing permet aux participants de partager leur ressenti, d'analyser ensemble les conséquences des mauvaises pratiques. »

Le CHU de Rouen vise l'unité d'actions

Le CHU de Rouen, établissement support du GHT Cœur de Seine, a mis en place, il y a trois ans, un Département « Méthode – Qualité – Sécurité – Contrôle Interne » au sein de la DSI. Un modèle de gouvernance qui a fait ses preuves. Retour d'expérience.

Référent Sécurité du Système d'Information depuis décembre 2015 au CHU de Rouen, **Cédric Hamelin** accompagne à la définition et à la mise en œuvre de la politique de sécurité du SI au sein de l'établissement ainsi que sur des actions de sensibilisations. Il a précédemment exercé des missions de prestations pour des clients Grands Comptes (Orange Labs, Completel, Bouygues Télécom, RTE, GRT GAZ…) et au sein de sociétés de services en qualité d'Ingénieur Développeur, puis Chef de projet.

Anciennement Responsable du Département des applications médicales et médicotechniques, puis responsable du Département Technique, **Jacques Ferrand** est Responsable du Département Méthode Qualité Sécurité et Contrôle Interne depuis octobre 2015 au sein de la DSI. Il assure également les fonctions de RSSI et de DPO.

Sous l'effet conjugué du renforcement des cadres légaux et règlementaires et de l'accroissement du risque numérique, les établissements de santé s'organisent et mettent en place des organisations permettant de répondre aux exigences de qualité et de sécurisation des systèmes d'information.

Le Responsable Sécurité du Système d'Information conseille, oriente les stratégies, prévient, contrôle, et sensibilise l'ensemble des acteurs, direction générale et utilisateurs. Divers schémas d'organisation le positionnent en rattachement auprès de la direction générale, d'une direction tierce, ou d'un directeur des systèmes d'information (DSI). La DSI apporte, par ailleurs, une contribution naturelle à des missions transversales de définition de processus ou de certifications, qui sont, en règle générale, portées par une direction Qualité.

1 La création du Département MQSCI

En 2015, à l'issue d'un audit de son SI, et sous l'autorité de son nouveau directeur, le Département « Méthode – Qualité – Sécurité – Contrôle Interne (DMQSCI) » a été créé au sein de la DSI, afin de répondre plus efficacement à l'ensemble de ces objectifs.

Ce département est une extension du Département Méthode et Qualité, créé en 2012. Celui-ci était alors principalement centré sur les volets processus, référentiels, cartographie, gestion de la documentation et communication. L'intégration des volets sécurité et contrôle interne lui a donné une nouvelle dimension. Par une meilleure unité d'actions, il permet également une meilleure compréhension des attentes et améliore l'imbrication des différentes thématiques.

Il accompagne la DSI dans sa démarche d'alignement et de respect de la conformité réglementaire et normative, basée sur les règles de l'art et les « best practices » exigées par les certifications européennes reconnues de type ISO.

Il soutient une acculturation de proximité aux normes, par une démarche de support et de contrôle.

2 Les missions du Département

Les fonctions du DMQSCI sont déclinées en **sept axes** pour un accompagnement large des départements techniques et fonctionnels de la DSI dans l'évolution de leurs pratiques.

- Un axe Qualité concernant la coordination et le suivi des certifications (Certification des Comptes, COFRAC, HAS, Programme Hôpital Numérique …), le respect des engagements institutionnels sur les dossiers stratégiques, la définition des indicateurs de performance interne et externe, ainsi que la mise en place des mesures de contrôle interne et l'animation de réunions Qualité.
- Un axe Sécurité, chargé de la sécurité, disponibilité et intégrité des données sur la base de normes et standards (ISO 20000, famille ISO 27000, …). Cela signifie la bonne maîtrise du corpus réglementaire associé, ainsi qu'une veille assidue concernant les évolutions des niveaux d'exigence (ANSSI, CNIL, RGPD, ministère, DGOS, ASIP Santé).
- Un axe Méthodes comprenant la définition des

usages, pratiques et processus (constitution et maîtrise des référentiels internes et externes, support méthodologique aux départements de la DSI).

• Un axe Audits avec la mesure du respect des usages et pratiques définis (audits techniques et organisationnels, pilotage et suivi des contrats de services, gestion de la relation « client – fournisseur » interne à l'Institution).

• Un axe Gestion documentaire pour la constitution de modèles de documents et le management de la base documentaire de la DSI.

• Un axe Communication pour porter la gestion du site Intranet de la DSI et la fabrication de supports de communications internes et externes.

• Un axe Ressources Humaines pour la gestion prévisionnelle des emplois et des compétences comprenant le processus de recrutement, le suivi du plan de formation de la DSI, des documents uniques et plans de prévention.

La diversité de l'équipe, composée de six personnes aux profils différents et aux expériences professionnelles variées (Architecture technique, Responsable de Centre d'appels, Chefs de projet, Développeur, référent CIL, Ingénieure Qualité ...) constitue une véritable richesse en raison des différents niveaux d'expertise qu'elle apporte.

Si l'organisation mise en place considère l'ensemble des exigences institutionnelles propres à l'établissement, elle intègre également les obligations induites par la mise en place du Groupement Hospitalier de Territoire, le GHT Cœur de Seine dont le CHU de Rouen est l'établissement support.

3 L'organisation de la SSI

Pour mener à bien les missions définies, la direction générale a validé la nomination du responsable de ce département en qualité de RSSI pour porter l'ensemble du volet SSI. Depuis l'entrée en vigueur du Règlement Général de Protection des Données, le RSSI a également pris en charge la fonction de Délégué à la Protection des Données.

Concernant la SSI, il est accompagné dans ses travaux par deux référents, ce qui permet d'éviter l'isolement de la fonction et d'améliorer collaboration et proximité :

• Un Référent SSI « Fonctionnel et Métier », garant du respect de la Politique de Sécurité des Systèmes d'Information de l'établissement. À ce titre, il assure la gouvernance et le pilotage de la sécurité à l'échelle du CHU de Rouen auprès des métiers et des équipes en charge des applications métiers.

• Un Référent SSI « Technique », affecté à l'ensemble du volet infrastructures. Il apporte support aux équipes techniques de la DSI, dans l'identification et la mise en œuvre des mesures de sécurité. Il les priorise par rapport aux moyens existants, et conseille sur les solutions à mettre en œuvre.

Ce trio peut s'appuyer sur l'apport de ressources complémentaires présentes au sein du département et en charge des autres axes, mais aussi sur le renfort de prestations extérieures dans le cadre de missions ponctuelles d'accompagnement (gouvernance, audits…).

S'il existe plusieurs stratégies de positionnement du RSSI au sein d'un établissement de santé, son intégration au sein de la DSI a permis d'accroître le niveau de maturité du service, par une prise assez directe sur le quotidien et plus de proximité auprès des équipes.

4 Les résultats

L'organisation mise en place a prouvé son efficacité sur de nombreux sujets. Elle s'est révélée être un atout important pour l'amélioration des pratiques, l'élévation du niveau de sécurisation des infrastructures et des applications ; elle a permis de répondre avec plus de réactivité et de pertinence aux dossiers de Certification.

Le département est aujourd'hui un organe structurant du service. Au regard de son large périmètre d'actions, de l'évolution constante du SI et des technologies numériques, de nombreux chantiers sont ouverts et mobiliseront les énergies sur le long terme.

> « La diversité de l'équipe de six personnes aux profils et aux expériences professionnelles variées constitue une véritable richesse »

0.3

TECHNOLOGIES DE SÉCURITÉ

Annuaire et IAM : les véritables enjeux, **Cédric Cartau** P. 39
Annuaire et IAM : retour d'expérience du CH Alpes-Isère, **Benjamin Delubac** P. 40 & 41
Simplifier la gestion des mots de passe, **Sébastien Wetter** P. 42
Sécuriser l'Active Directory de l'établissement de santé, **Christophe Jodry** P. 43 & 44
Les données de santé sensibles doivent être chiffrées et signées, **Gérard Peliks** P. 45 & 46
Un partenariat qui simplifie l'échange de données par MSSanté, **Sébastien Wetter** P. 47
Face au phishing : scoring et sensibilisation, **Michael Roman** P. 48 À 50
Et si le risque venait de l'intérieur ?, **William Culbert** P. 51
Tests d'intrusion et scans de vulnérabilité : in-dis-pen-sables, **Frédéric Cabon** P. 52 & 53
Scanners de vulnérabilités : connaître son SI pour mieux le protéger, **Charles Blanc-Rolin** P. 54 & 55
L'intérêt d'un cloud hybride, **Didier Verbeke** P. 56 & 57
Solution de prise en main à distance : un choix loin d'être anodin, **William Culbert** P. 58 & 59
Intelligence artificielle et outils de cyber-sécurité, **Loïc Guezo** P. 60 & 61

Annuaire et IAM : les véritables enjeux

Composants du socle applicatif, annuaires et IAM sont aux progiciels métiers ce que le réseau est à l'infrastructure technique : les rails sur lesquels circulent le train. Curieusement, ces composants, ou les projets de déploiements ad hoc, sont souvent mal positionnés dans les organisations, et abordés sous le seul angle technique. Quelle place leur donner dans le contexte GHT ?

Cédric Cartau, RSSI et DPO du CHU de Nantes et du GHT44, est également chargé de cours à l'EHESP et à l'ESIEA. Il collabore régulièrement à la revue DSIH et a publié plusieurs ouvrages, notamment « La sécurité du système d'information des établissements de santé », seconde édition (Eyrolles, 2017).

Un progiciel d'IAM est composé de **cinq modules principaux**. Le composant central est un méta annuaire : un annuaire technique qui n'est pas visible de l'utilisateur final mais qui agrège des données issues de différentes sources amont et alimente plusieurs sources aval.
Deuxième module : les sources d'alimentation amont des identités. On trouve bien entendu l'annuaire ressources humaines (RH), mais tout n'est pas dans cet annuaire (par exemple, les numéros de téléphone interne sont dans le PABX) et tous les individus ne sont pas forcément listés dans l'annuaire RH (par exemple les stagiaires non rémunérés, les personnels sous convention avec un laboratoire de recherche, etc.). Ces sources alimentent le méta annuaire et le peuplent d'identités qu'il faudra fusionner : un personnel peut passer du statut de stagiaire à celui d'employé recruté, et donc apparaître dans deux sources de données.
Troisième module : les cibles de provisionning aval. Avec les identités ainsi alimentées dans le méta annuaire, on crée plus ou moins automatiquement les comptes des utilisateurs dans les applications métiers avec les droits qui vont bien (calculés à partir de l'affectation de la personne, de son métier, grade, etc.).
Quatrième module : le SSO (Single Sign On). Stricto sensu, le SSO n'est pas totalement lié à l'IAM (on peut faire du SSO sans IAM et déployer un IAM sans SSO). Il faut voir ce module comme l'outil marketing qui permet d'améliorer l'ergonomie des utilisateurs qui n'ont plus à retenir qu'un seul mot de passe au lieu des 10 ou 15 habituels.
Cinquième module : un IAM qui est déployé en même temps que le SSO est souvent accolé à un déploiement de cartes à puces multiservice, il faut donc un outil de création des cartes : personnalisation graphique, génération des bi-clés, appariement avec les sous-systèmes self et locaux, etc.

Remise à plat du circuit des identités

Un projet d'IAM est tout sauf technique : le principal enjeu d'un tel projet est la remise à plat du circuit des identités au sein de l'établissement. Les dysfonctionnements dans ce circuit sont nombreux et à peu près partout les mêmes : annuaire RH non exhaustif, création des identités dans l'annuaire RH au moment de la paye des agents et non au moment de leur arrivée dans l'établissement, pas d'interconnexion entre cet annuaire et l'AD (ce qui empêche la suppression automatique des comptes au départ des agents), agents ayant plusieurs matricules (car ils ont eu plusieurs contrats), code de statut faisant référence à une sortie des effectifs pas listés ou pas exhaustifs, etc.
Déployer un IAM a beaucoup plus d'impact sur les DRH que sur les DSI - pour qui, somme toute, ce n'est qu'un logiciel de plus.
Il est crucial, au démarrage d'un tel projet, que le chef de projet fonctionnel soit le DRH : sans cet appui politique interne, les modifications de processus métier autour de la donnée Agent n'ont quasiment aucune chance d'aboutir.

> « Déployer un IAM a beaucoup plus d'impact sur les DRH que sur les DSI pour qui ce n'est qu'un logiciel de plus »

GHT : une combinatoire explosive

Les GHT ont d'abord été constitués autour de la notion de prise en charge régionale des patients. Conséquence logique : il sera nécessaire que des praticiens ou personnels soignants issus des différents établissements puissent accéder aux DPI de tous les établissements, dans l'attente d'un DPI unique - étape qui ne devrait pas arriver, selon toute vraisemblance, avant au bas mot 10 ans.
Mais comment donner un accès à un logiciel à une personne inconnue de l'annuaire RH, inconnue des autres sources d'annuaire ? Il faudra, à un moment donné, alimenter le méta annuaire d'un établissement avec les annuaires RH de tous les autres, ce qui fait une combinatoire explosive (c'est le problème bien connu des poignées de mains). Soit les annuaires RH fusionnent - ce qui suppose une gestion RH commune au sein du GHT, soit il faudra mettre en place des délégations d'annuaire, voire plutôt des fédérations d'annuaires et de méta annuaires. Il va falloir rejouer le film, mais à l'échelon au-dessus : obtenir un pilotage de ce macro projet par une DRH de territoire, uniformiser les processus sur toutes les DRH des établissements, etc.
Le chantier est énorme et les enjeux à la hauteur de celui des GHT.

Annuaire et IAM : retour d'expérience du CH Alpes-Isère

Un projet d'IAM[1] peut très vite devenir empirique et impactant institutionnellement pour peu que l'on pousse la réflexion au-delà de ce périmètre. Quelle place lui donner au sein d'un SI ? Quelle gouvernance et quel rôle au sein d'un GHT ? Voici quelques questions qu'un tel projet pourrait soulever et auxquelles je vais essayer de répondre avec ce retour d'expérience.

Benjamin Delubac, RSI et RSSI du Centre Hospitalier Alpes-Isère (38), est développeur de formation. Son entrée dans le monde hospitalier l'a rapidement conduit à s'intéresser à l'architecture et à la sécurisation des SI, avec un objectif d'efficience. Il est passionné par les technologies innovantes, la robotique, le big data, le machine learning, sujets qui font l'objet d'actions ou de projets dans son établissement.

De prime abord la tâche ne semblait pas si compliquée que cela. Après tout, qu'est-ce qui pourrait bien l'être dans la mise en place d'un annuaire ?

1 Un IAM pour les gouverner tous

Nous connaissons tous le leitmotiv de ce type de projet : reprendre la main sur la gestion des identités au sein de nos établissements. Alors, que ce soit par pur orgueil d'informaticien ou, plus prosaïquement, par une volonté de sécuriser et rationaliser la gestion des identités, ce projet prendra tout son sens lorsqu'il sera question de répondre aux nombreux audits/contrôles auxquels nous sommes assujettis : certification des comptes, certification HAS, Hôpital numérique, normes ISO, etc.

D'abord, une cartographie des applications à habilitations

La genèse de ce type de projet est donc d'en finir avec la création et la distribution sauvage d'habilitations au sein de nos SI. Pour ce faire, il est essentiel de procéder au préalable à une cartographie (voilà qui est original !) des applications à habilitations, et de prioriser ces dernières afin de concentrer les efforts sur les futurs connecteurs à forte valeur ajoutée. Il est important, au moment de ce travail, de ne pas perdre de vue les cibles potentielles des auditeurs, DPI, GAP, GEF, mais également EAI, AD, GRH et autres accès périmétriques. Et si au passage, vous pouvez à moindre coût gérer vos pools de véhicules et caisses de cafeteria, vos usagers n'en seront que plus ravis !

C'est là que le travail se gâte : exit les projets centrés sur la DSI, tout le monde doit s'y mettre ! De la réorganisation des processus d'arrivée et de départ des agents à la délégation de gestion des habilitations, en passant par la modification des exigences applicatives (lors de nouvelles acquisitions notamment), c'est l'institution dans son ensemble qui se voit impactée. Il est l'heure de travailler de concert !
Il vous faudra faire preuve de pragmatisme et de pédagogie, lorsqu'il sera question d'expliquer à votre service des ressources humaines, le rôle central de son application (et implication) et la rigueur que cela induit en terme de gestion des contrats de travail. C'est le point de départ, l'identité est essentiellement (mais pas exclusivement) créée et gérée ici.

2 Un IAM pour les piloter tous

Une fois la connexion fiabilisée avec les référentiels, agents et structures, votre IAM va donc devenir la pierre angulaire de votre SI. Il va très rapidement piloter l'identité dans vos Active Directory (ou équivalent), vos messageries, vous permettant d'automatiser la création et l'invalidation des comptes et d'y déverser automatiquement une mine d'informations issues de votre GRH, comme les informations de métier, de grade, d'unité(s) ou les numéros RPPS de vos praticiens (très utiles pour simplifier les accès aux plateformes régionales entre autres). Dès lors, commence à s'opérer une redistribution des responsabilités et les premiers effets vertueux se font sentir. « Vous n'arrivez pas à ouvrir votre session ? En effet, votre contrat n'a pas été renouvelé dans le logiciel RH, merci de vous rapprocher du *service ressources humaines* ».

Confort et réactivité

Tout nouveau connecteur mis en place dans votre SI par le biais de votre IAM apportera ainsi son lot de sécurisation, de confort et de réactivité.
Un nouvel agent prend ses fonctions ce matin : le service de gestion des badges est en capacité de produire le support d'authentification. Ses habilitations informatiques sont provisionnées, son poste informatique accessible par le biais de sa carte, ses accès aux bâtiments ouverts et il pourra badger au self à midi avant d'emprunter un véhicule du pool pour se rendre au domicile du patient. Il recevra sa carte CPS dans les prochains jours, commandée automatiquement auprès de l'ASIP Santé par votre système.
Au lancement du projet, en 2011, cette vision nous paraissait utopiste. Aujourd'hui c'est une réalité !

3 Un IAM pour les contenter tous

Au-delà du confort et de la sécurité que cela apporte au quotidien pour la gestion des identités dans nos établissements, l'IAM est un outil qui fait mouche lors des différents audits. Très souvent couplé à des solutions

1 Identity and Access Management ou GIA, en français pour gestion des identités et des accès

de CMS[2] et de SSO[3], vous obtiendrez là un triptyque de poids lorsqu'il sera question d'auditer vos habilitations.
Vous réduisez la présence de comptes génériques dans vos SI, et cela se répercute dans vos applications (reste *a minima* quelques comptes applicatifs, prestataires externes,...).
Les comptes toujours actifs de personnels ayant quitté l'institution tendent également à disparaître, ou dans le pire des cas à être invalidés par votre IAM pour ceux nécessitant une traçabilité dans le temps. Le tout étant calculé à chaque alimentation en fonction de critères divers et variés (unité fonctionnelle, métier, dates de présence ….) et tenant donc compte des modifications faites (en RH par exemple) entre chaque alimentation.

Décentraliser

Pour les plus téméraires, cela permettra de pousser jusqu'à la décentralisation de la gestion / délivrance des badges (à un PC sécurité par exemple), de déléguer tout ou partie de la gestion des populations étudiantes (IFSI par exemple), personnels externes, stagiaires (direction des soins par exemple), de déporter sur les responsables de données, la gestion des habilitations dans leurs applications respectives.

4 Dans l'inquiétude… les « plonger » tous !

Histoire de ne pas se faire l'évangéliste d'un tableau trop idéaliste, avouons que l'IAM induit un certain nombre de contraintes / risques, et non des moindres.
Il nécessite la mise en place de garde-fous afin de ne pas mettre à genou votre SI en cas de bug du moteur de calcul. Imaginez une invalidation complète des comptes informatiques, ou un mélange massif des attributs entre homonymes…
Il induit des coûts directs et indirects non négligeables, liés aux interfaces, au temps homme nécessaire à l'administration et à la surveillance de la solution, au temps organisationnel nécessaire entre les services de l'institution pour mettre en place les nouvelles organisations, aux projets connexes (SSO et lecteurs de badge par exemple).
Il va très rapidement introduire des calculs complexes d'attributs, afin de gérer toutes sortes d'exceptions, souvent liées à des métiers ou des types particuliers de personnes.
En conclusion, une mauvaise évaluation des contraintes peut rapidement rendre le projet titanesque et décourager les moins persévérants. Mais à l'aube du nouveau programme Hop'En et de la mise en place des systèmes d'information convergents, le pilotage nécessaire des identités entre les différentes entités juridiques place plus que jamais l'IAM comme le médiateur incontournable des systèmes d'informations territoriaux.

> « Il vous faudra faire preuve de pragmatisme et de pédagogie lorsqu'il sera question d'expliquer à votre RH le rôle central de son application (et implication) et la rigueur que cela induit en terme de gestion des contrats de travail »

2 Card Management System, application permettant entre autres la gestion du cycle de vie des cartes
3 Single-Sign-On, méthode permettant à un utilisateur d'accéder à plusieurs ressources informatiques en ne procédant qu'à une seule authentification.

Simplifier la gestion des mots de passe

Plus de neuf établissements de santé sur dix déclarent désormais avoir formalisé une politique de sécurité du système d'information[1]. Mais au-delà de cette formalisation, qu'en est-il des usages ? Comment simplifier les accès tout en sécurisant les données ? Réponse : le Single Sign-on, dont Enovacom vient de renouveler les interfaces et fonctionnalités.

Chef Produit / Gamme Sécurité chez Enovacom depuis 2012, **Sébastien Wetter** a d'abord travaillé en SSII, au service de diverses DSI, où il a consolidé ses compétences en système d'information, notamment en architecture et urbanisation. Il a ensuite découvert le secteur de la santé quand il a rejoint le cabinet Stream Consulting, en tant que consultant en systèmes d'informations. Il est en effet intervenu pour plusieurs ARS, GCS et établissements de santé, avant de se spécialiser dans le domaine décisionnel et l'interopérabilité, puis de manager une équipe de développement.

Les pirates ciblent de plus en plus les hôpitaux publics et structures de santé privées, sans surprise. Selon Websense, les intrusions dans les systèmes d'information de santé ont augmenté de 600% en 2016.
De nombreux exemples récents illustrent ce constat. A Singapour, l'infection d'un ordinateur a permis le vol des données d'1,5 million de patients ; l'institut de santé hawaïen a été victime d'un ransomware concernant 40 800 patients. La France n'est malheureusement pas épargnée : on se souvient du groupe de pirates Rex Mundi qui s'était attaqué, il y a quelques années, à un laboratoire d'analyses.
Pourquoi nos données de santé deviennent-elles la cible de toutes les attaques ? Principalement pour la valeur des informations récoltées. Elles se revendent très bien sur le marché noir : 30 à 200$ selon Vincent Trély, président de l'APSSIS. Les données **détenues par les hôpitaux (dossiers médicaux, numéros de sécurité sociale,** identité de la personne, etc) attirent donc les cybercriminels**.**
Mais, au-delà du piratage, nos données sont à la merci d'un autre problème : l'institut Ponemon révèle qu'une brèche de sécurité, directement liée à un employé malveillant, ou simplement négligent, facilité le plus souvent les attaques.

Comment se protéger de la faille humaine ?

Il devient nécessaire de rendre opérationnelle, simple et sécurisée la gestion des accès aux données sensibles.
Nos données de santé sont des informations sensibles. Leurs accès doivent être contrôlés, limités à la bonne personne, au bon moment, pour éviter tout risque de malveillance, ou simple oubli. Pour ce faire, au-delà d'une politique d'habilitations bien définie en amont, l'accès au dossier du patient doit être sécurisé.
Sécurisé, mais aussi simplifié. Pourquoi ? Car au-delà de prévenir les négligences dont nous pouvons faire preuve au quotidien, la technologie doit être au service des usages. Dans un hôpital, le soignant doit pouvoir accéder rapidement aux informations médicales de son patient pour être le plus réactif possible, ET de manière sécurisée. Mais il a en général des dizaines d'applications à gérer, avec autant de mots de passe différents. Guère étonnant, dès lors, s'il oublie le mot de passe renforcé avec la majuscule, le caractère spécial et les dix chiffres à intégrer… Son exercice quotidien est alourdi par cette contrainte, et le fameux post-it glissé sous le clavier tellement tentant !

> « Au-delà d'une politique de sécurité établie, il devient nécessaire de rendre opérationnelle, simple et sécurisée la gestion des accès aux données sensibles »

Un nouveau Single Sign-On 100% Santé

Fort de ses 16 ans d'expérience auprès des établissements de santé, Enovacom, a choisi de repenser la manière de sécuriser les données. Sa solution Single Sign-On (SSO)2 est dotée d'une nouvelle interface homme machine et de nouvelles fonctionnalités tirant profit des technologies les plus récentes. L'objectif ? Réussir à simplifier la sécurité des accès au système d'information hospitalier. Il n'est en effet plus nécessaire de se souvenir des mots de passe car la solution permet aux soignants de se connecter au dossier patient, et à toutes ses applications, avec le principe d'authentification unique par carte CPS par exemple.
Au-delà des fonctionnalités natives d'un SSO, elle a été conçue pour faciliter le quotidien, tant des utilisateurs que de l'équipe informatique. En plus d'être simple à déployer, c'est l'autonomie des utilisateurs qui a primé dans son développement : ils peuvent désormais gérer eux-mêmes leurs mots de passe et leurs moyens d'authentification. Le SSO répond ainsi aux différents cas d'usage rencontrés dans les établissements de santé. Il fait partie des briques logicielles essentielles pour garantir la confidentialité des données, tout en respectant la pratique quotidienne des utilisateurs.

1 Selon une étude du Clusif (Club de la sécurité de l'information français)
2 ENOVACOM Secure Login. Pour en savoir plus et découvrir la solution en vidéo : https://www.enovacom.fr/sso-sante.html

Sécuriser l'Active Directory de l'établissement de santé

Trois scénarii illustrent clairement les conséquences d'une absence de maîtrise et d'un manque d'expertise sur la technologie d'Active Directory, largement répandue dans les établissements de santé. Introduction à une lecture indispensable des guides et recommandations.

Christophe Jodry est le directeur des offres e-Santé et PCI-DSS chez Claranet France. Il démarre sa carrière comme ingénieur d'exploitation en société de service, puis chef de projet dans le monde de l'hébergement et de l'infogérance. Il bascule, à partir de 2010 dans le domaine de la sécurité informatique et devient le RSSI de Runiso, premier hébergeur PCI-DSS en France, également hébergeur agréé données de santé. Avant son arrivée chez Claranet, Christophe Jodry était en charge de la PGSSI-S à l'ASIP Santé.

L'Active Directory (AD) est une technologie de Microsoft qui comporte trois fonctions principales au sein d'un système d'information (SI) :

- base d'annuaire ;
- base de contrôle d'accès ;
- base de gestion de parc machines et serveurs.

C'est le composant du SI qui porte l'authentification et les autorisations d'accès de tous les utilisateurs, c'est pourquoi sa sécurisation est une nécessité absolue. Se rendre maître de l'Active Directory permet notamment l'obtention du droit total sur toutes les ressources et le droit sur tous les accès utilisateurs. En somme, la compromission de l'Active Directory signifie la compromission de tout le système d'information. Or, l'AD est une technologie très fréquente dans les établissements de santé français. Ceci est lié au fait que les DSI ont fait le choix de parcs de postes de travail essentiellement sous Windows.

Le fonctionnement de l'Active Directory

Impossible de le décrire de manière exhaustive dans le cadre de cet article. Rappelons simplement quelques notions essentielles (nous n'expliquerons pas par exemple les notions de forêt et de liens d'approbation).

La notion de domaine : un ensemble de machines et d'utilisateurs partageant le même annuaire Active Directory.

La notion de contrôleur de domaine : « *Un serveur hébergeant l'annuaire Active Directory est appelé « contrôleur de domaine ». Active Directory stocke ses informations et paramètres dans une base de données distribuée sur un ou plusieurs contrôleurs de domaine* » (source : Wikipédia)

Il existe plusieurs protocoles d'authentification. Du plus ancien au plus récent, citons : LM Hash, NTLM et Kerberos.

Focus sur le LM Hash

LM hash, ou **LAN Manager hash** est un format développé par Microsoft pour stocker les mots de passe utilisateurs qui ont moins de quinze caractères. Il est utilisé dans les premières versions d'Active Directory.
Le principe de fonctionnement est le suivant :

- Le mot de passe est séparé en deux éléments de 7 caractères.
- Si le mot de passe a une longueur inférieure à 14 caractères il est complété par des caractères nuls.
- Le hash de chaque élément est calculé séparément.
- Les deux hashs concaténés forment le hash LM.

Par ailleurs, le format LM ne gère pas la casse. Tous les caractères minuscules sont remplacés par des caractères majuscules.

➤Ce mode de fonctionnement a autorisé la mise en place d'attaques faciles et rendues triviales par des outils comme les Rainbow Tables. Les protocoles plus récents (type Kerberos) sont désormais fortement recommandés.

Analysons maintenant trois scénarii de risques autour de l'Active Directory.

Risque 1 : Rétrocompatibilité sur les domaines Windows

Microsoft autorise la rétrocompatibilité au sein d'un domaine Windows, ce qui permet par exemple d'héberger un serveur Windows 2003 dans un domaine Active Directory 2016. Cette rétrocompatibilité est très utile aux établissements de santé pour faire cohabiter des applications métiers de différents âges, s'appuyant parfois sur des OS obsolètes.

Sécuriser l'Active Directory de l'établissement de santé

Problème principal : il faut maintenir des protocoles anciens comme le LM hash pour les mots de passe. Or, comme nous l'avons vu plus haut, ce type de protocole est très vulnérable.

L'existence d'applications reposant sur des OS anciens est de ce fait clairement une menace pour le domaine Windows et donc tous les accès utilisateurs de l'établissement. Même si les critères métiers et fonctionnels restent prépondérants dans le choix d'une application, les éditeurs se doivent de prendre en compte cette menace et de proposer des spécificités techniques à jour.
Les DSI sont alors amenés à gérer une transition en douceur, en éliminant les applications obsolètes une par une. Mais, même une fois les OS en cohérence avec un niveau de domaine Active Directory récent, le protocole est mis à jour uniquement au changement du mot de passe. Ce qui veut dire qu'il leur faut renouveler tous les mots de passe créés en LM pour les voir utiliser un protocole plus récent et plus robuste. Cette opération est évidemment risquée sur les comptes de service des applications.
La rétrocompatibilité offerte par l'Active Directory est donc une arme à double tranchant pour les DSI des établissements de santé.

> « La compromission de l'Active Directory signifie la compromission de tout le système d'information. »

Risque 2 : l'administrateur du domaine

Le meilleur ennemi d'un domaine Windows est son administrateur. Ce type de compte a tous les droits sur le domaine : révocation et création d'utilisateur, changement possible de tous les mots de passe, etc. Alors que multiplier les comptes administrateurs du domaine et leur laisser la possibilité de se connecter sur n'importe quel poste de travail peut paraître pratique, c'est en fait un vecteur d'attaque idéal.

Mettons-nous en situation : un administrateur du domaine utilise son compte administrateur sur son poste de travail au quotidien. Pour réaliser ses gestes d'administration sur le domaine Active Directory… mais aussi pour ouvrir sa messagerie, naviguer sur internet, ouvrir des applications métiers, l'intranet etc. Un compte utilisateur simple, aux accès restreints pourrait suffire pour réaliser ces dernières tâches. Oui, mais cela nécessiterait que notre administrateur utilise deux comptes différents pour se connecter : un accès utilisateur et un accès administrateur. Pas pratique à gérer au quotidien !
Imaginons désormais le scénario catastrophe (et déjà vécu par des établissements de santé) : l'administrateur du domaine ouvre un cryptovirus via sa messagerie, avec ses accès et droits administrateur. Le cryptovirus se propage sur le poste de travail mais aussi sur tous les répertoires réseaux accessibles à l'administrateur, donc potentiellement toutes les ressources du domaine… dont l'AD même. C'est le système d'information entier qui va être bloqué et l'Active Directory complétement compromis. AD qu'il faudra reconstruire complétement. Ce qui signifie plusieurs jours d'indisponibilités garantis !

Des règles d'hygiène spécifiques aux administrateurs du domaine sont à respecter selon l'ANSSI.

Plus globalement, l'administrateur du domaine se doit d'être un utilisateur vigilant, formé et sensibilisé. A grand pouvoir, grandes responsabilités.

Risque 3 : le contrôleur de domaine

Même s'ils sont des serveurs sous Windows, les contrôleurs de domaine ne sont pas des serveurs comme les autres. Portant la base de données d'Active Directory et les fonctionnalités inhérentes, les accès doivent être limités et la surface d'attaque réduite au maximum.

En quelques lignes, voici les bases du durcissement d'un Active Directory. Pour plus de détails, nous vous renvoyons au document de l'ANSSI :

- segmentation réseau ;
- durcissement OS ;
- patch management ;
- réduction de la surface d'attaque : aucun autre logiciel autorisé.

« *Aucun autre logiciel autorisé* » … ce qui pose la question de l'antivirus : faut-il installer ce type d'outil sur un Active Directory ?
L'antivirus peut être perçu comme le dernier rempart face à un malware mais aussi un vecteur d'attaque supplémentaire. Ce n'est, après tout, qu'un logiciel, faillible comme les autres, avec ses erreurs de code. Combien de chevaux de Troie ont utilisé les failles d'un antivirus pour infiltrer un SI ? Un peu trop à notre goût…

Alors, *antimalware or not antimalware* ? Pour le RSSI, la réponse est dans le contexte de son SI. Les défenses périmétriques autour de l'AD sont-elles suffisantes ? Les accès sont-ils suffisamment restreints ? Les administrateurs du domaine sont-ils suffisamment vigilants et formés ? Y a-t-il déjà un passif avec les antivirus ? Le RSSI agira en gestionnaire du risque pour déterminer les meilleures mesures à prendre.
Les trois scénarii ci-dessus sont représentatifs des risques encourus. Les guides de l'ANSSI et de Microsoft constituent une lecture recommandée pour se poser les bonnes questions.

Les données de santé sensibles doivent être chiffrées et signées

La cryptographie apporte une réponse satisfaisante aux nécessaires fonctionnalités de confidentialité et d'intégrité des données numériques sensibles. Quels sont les mécanismes du chiffrement et de la signature électronique ? Explications.

Président de l'association CyberEdu (créée par l'ANSSI), président de l'atelier sécurité et vice-président de Forum ATENA, membre du Conseil d'Administration de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information (ARCSI), **Gérard Peliks**, ingénieur diplômé, est chargé de cours sur la cybercriminalité/cybersécurité pour des mastères et MBA d'écoles d'ingénieurs. Il écrit des articles de vulgarisation sur les dangers du cyberespace et les contre-mesures pour en diminuer les risques.

Si une donnée médicale est sensible, il est nécessaire de ne la rendre lisible et exploitable que par ceux qui sont autorisés à en prendre connaissance. Pour parler de manière plus technique, il est nécessaire d'assurer ses permissions en lecture, ce qui assure sa confidentialité. Mais ce n'est pas suffisant. Il faut aussi s'assurer que la donnée créée n'a pu être modifiée que par ceux qui sont autorisés à le faire. Il est ainsi nécessaire d'assurer ses permissions en écriture, ce qui assure son intégrité.

La confidentialité est implémentée par le chiffrement et le déchiffrement basés sur des algorithmes et des clés. **L'intégrité** est implémentée par la signature numérique, elle-même basée sur des algorithmes, sur des clés et sur des calculs d'empreintes. Nous allons voir quelles sont les réponses de la science des messages cachés, la cryptographie, et comment tout ceci se met en place.

Bien entendu, les algorithmes doivent être difficilement cassables et les clés utilisées suffisamment longues, sinon les cryptanalystes pourraient essayer de retrouver en clair les données chiffrées par d'autres moyens que ceux de la cryptographie, en essayant toutes les clés possibles ou en cherchant des failles dans l'implémentation des algorithmes. Ces cryptanalystes pourraient donc, alors qu'ils ne sont pas autorisés à le faire, non seulement lire les données chiffrées mais en outre, et c'est plus grave, les modifier.

1 Le chiffrement

Dans le mécanisme du chiffrement, un message en clair est traité par un algorithme, qui est un programme qui va effectuer des substitutions et des permutations sur chacun des caractères du message en fonction du contenu de la clé de chiffrement. Le message ainsi chiffré, passant par le même algorithme qui le traite en fonction du contenu d'une clé de déchiffrement, est remis en clair.

Si la clé de déchiffrement est la même que la clé de chiffrement, le chiffrement est dit symétrique. Si la clé de déchiffrement et celle de chiffrement sont différentes, le chiffrement est dit asymétrique.

Il semblerait que le chiffrement asymétrique doive s'imposer pour chiffrer les données médicales sensibles. Mais il présente des problèmes. Il est beaucoup plus lent que le chiffrement symétrique car il nécessite des calculs beaucoup plus complexes. L'autre problème est de prouver qu'une clé publique est bien celle qui est mathématiquement liée à la clé privée détenue par son propriétaire.

Le certificat numérique

Le problème de la preuve de la relation entre une clé publique et la clé privée correspondante est résolu par le certificat numérique dans lequel la clé publique se trouve. Ce certificat numérique contient non seulement la clé publique, les dates de validité de cette clé et l'identité de son propriétaire, mais il est signé numériquement, par un tiers de confiance. On ne peut modifier le certificat sans qu'on s'en aperçoive, donc l'appartenance de la clé publique est établie par la confiance portée à l'autorité qui a signé le certificat.

Pour chiffrer au moyen du chiffrement asymétrique, on demande son certificat numérique à celui à qui on veut transmettre un message chiffré. On extrait de ce certificat la clé publique qu'il contient et on chiffre le message avec cette clé publique. Seul le destinataire du message ainsi chiffré, propriétaire du certificat numérique qu'il a envoyé à l'émetteur du message chiffré, pourra déchiffrer ce message. En effet, seul le destinataire possède la clé privée correspondante à la clé publique qui a chiffré le message.
Mais ce chiffrement / déchiffrement est très lent. C'est pourquoi, dans les dispositifs de cryptographie, on utilise toujours le chiffrement symétrique pour chiffrer / déchiffrer les messages. Le chiffrement asymétrique est utilisé pour chiffrer / déchiffrer la clé de chiffrement symétrique qui sert à chiffrer / déchiffrer les messages.

Les données de santé sensibles doivent être chiffrées et signées

Symétrique versus asymétrique

Un chiffrement symétrique, tel que l'AES[1] , est très rapide est très sûr car il est basé sur le mécanisme mathématique du « OU exclusif » qui ne demande que peu de ressources. Le problème est que celui qui chiffre et celui qui déchiffre doivent posséder la même clé. Cela ne pose pas de problème quand ils sont à côté et peuvent s'échanger la clé de la main à la main, mais cela pose un très gros problème quand ils doivent s'échanger la clé à distance, par exemple par Internet, car les cyberprédateurs sont à l'écoute. De plus, la clé doit être modifiée fréquemment et générée par celui qui chiffre pour créer, dans l'idéal, une clé purement aléatoire. Elle doit être suffisamment longue pour ne pas être retrouvée par force brute, à partir du message chiffré. Ajoutons que, quand les utilisateurs sont nombreux à chiffrer / déchiffrer, le nombre de clés symétriques nécessaires, et qui doivent pourtant rester secrètes, croît très vite.
Le chiffrement asymétrique ne présente pas ces problèmes. Une paire de clés est mise en jeu : la clé de chiffrement et celle de déchiffrement. L'une des clés, dite clé privée, doit être conservée par son propriétaire, l'autre, dite clé publique, peut être donnée à tout le monde. Quand on chiffre avec l'une des clés, on ne peut déchiffrer qu'avec l'autre. Les deux clés sont mathématiquement liées et, à partir de la clé publique, il est mathématiquement très difficile de retrouver la clé privée correspondante. L'un des algorithmes, le RSA, acronyme formé des initiales des trois mathématiciens qui l'ont conçu[2], est basé sur la difficulté de factoriser un grand nombre qui est le produit de deux nombres premiers. En simplifiant à l'extrême, la clé publique pourrait alors être le grand nombre, et la clé privée les deux nombres premiers dont le produit donne le grand nombre. Car à partir du grand nombre, il est très difficile de retrouver ces deux nombres premiers.

2 La signature électronique

Nous avons ainsi le moyen d'assurer la confidentialité d'une donnée médicale sensible, reste à assurer son intégrité. C'est ici qu'intervient le mécanisme de la signature électronique, et tout d'abord pour l'implémenter, le mécanisme de calcul d'empreinte.

Une chaîne de caractères de longueur quelconque passant par une fonction de calcul d'empreintes, comme le SHA-2[3], donne une suite de bits de longueur fixe qui caractérise cette chaîne. On parle d'empreinte ou de *hash* en anglais, ou encore de condensat en bon français. Il n'est pas question de retrouver la chaine de caractères à partir de son empreinte, ce n'est pas le but. La fonction de calcul d'empreinte n'est pas une fonction de chiffrement mais une fonction dite « à sens unique ».

Le calcul d'empreinte

Pour prouver l'intégrité d'une donnée numérique, on calcule d'abord son empreinte. On chiffre cette empreinte avec sa clé privée qui intervient dans un chiffrement asymétrique. On transmet la donnée numérique accompagnée de son empreinte ainsi chiffrée. Celui qui veut s'assurer de l'intégrité du message extrait la clé publique du certificat, transmis par celui qui a chiffré l'empreinte, après avoir vérifié qui a signé le certificat (c'est l'autorité qui sera garante de la confiance accordée à la signature). Il déchiffre l'empreinte avec la clé publique de celui qui l'a chiffrée, et recalcule l'empreinte de la donnée numérique dont il veut s'assurer de l'intégrité du contenu et de l'autenthicité du signataire. Si l'empreinte recalculée est la même que l'empreinte déchiffrée, on est assuré de l'identité de celui qui a signé puisqu'elle est écrite dans son certificat numérique. On est assuré aussi que le message n'a pas été modifié depuis la signature, sinon les deux empreintes, déchiffrée et recalculée, auraient été différentes.

A noter que, pour le chiffrement, on chiffre une clé symétrique avec la clé asymétrique publique de celui à qui on veut transmettre le message. Ce message est chiffré avec la clé symétrique qu'on a générée. Pour la signature électronique, on chiffre l'empreinte du message avec sa clé asymétrique privée. On peut chiffrer un message ou simplement le signer ou faire les deux.

> « La sécurité du chiffrement ne repose pas sur le secret des algorithmes, qui doivent être de préférence publics et standards, mais sur celui des clés »

Le socle de la cybersécurité

Cet article décrit certains des mécanismes de cryptographie, mais l'utilisateur n'a pas besoin de connaître tous ces détails pour chiffrer, déchiffrer ou signer une donnée. Ce sont les solutions qu'il utilise qui s'en chargent avec des interfaces utilisateurs conviviales. Citons par exemple les logiciels libres PGP, GPG et Veracrypt. Citons aussi, pour ceux qui sont autorisés à l'utiliser, la solution de la Direction générale de l'armement, ACID. La sécurité du chiffrement ne repose pas sur le secret des algorithmes, qui doivent être de préférence publics et standards, mais sur celui des clés. Garantissant la confidentialité et l'intégrité des données numériques, les mécanismes de la cryptographie forment un socle sans lequel il n'y aurait pas de cybersécurité possible.

1 Advanced Encryption Standard
2 Rivest, Shamir, Adleman
3 Secure Hash Algorithm

Un partenariat qui simplifie l'échange de données par MSSanté

Enovacom et Microsoft ont travaillé ensemble afin que les établissements désireux d'utiliser Office 365 puissent assurer l'échange des données de santé en toute sécurité, grâce à la comptabilité MSSanté de la solution Enovacom. Explications.

Chef Produit / Gamme Sécurité chez Enovacom depuis 2012, **Sébastien Wetter** a d'abord travaillé en SSII, au service de diverses DSI, où il a consolidé ses compétences en système d'information, notamment en architecture et urbanisation. Il a ensuite découvert le secteur de la santé quand il a rejoint le cabinet Stream Consulting, en tant que consultant en systèmes d'informations. Il est en effet intervenu pour plusieurs ARS, GCS et établissements de santé, avant de se spécialiser dans le domaine décisionnel et l'interopérabilité, puis de manager une équipe de développement.

Enovacom et la messagerie sécurisée, c'est une longue histoire. Dès ses débuts, la société a accompagné les professionnels de santé dans la sécurisation de leurs échanges électroniques. Ce, avant même la naissance de la MSSanté, puisque nous avons mis sur le marché l'une des premières solutions homologuées GIP CPS[1] offrant messagerie sécurisée et authentification par carte CPS. Enovacom, qui se développe autour de deux gammes principales, l'interopérabilité et la sécurité des systèmes d'information, a d'ailleurs bâti une bonne part de sa notoriété sur l'offre Easycrypt, compatible S-Mime et Apicrypt. Nous étions en 2006. Autant dire le Moyen Age de la messagerie sécurisée en santé !

Présents dès le départ

On peut situer la Renaissance en 2012. A cette époque, le Conseil d'éthique et de déontologie auprès de l'ASIP Santé émet ses recommandations en matière de messagerie, puis une Journée nationale réunit, en fin d'année, tous les industriels concernés autour des objectifs affichés par les pouvoirs publics. Nous avons répondu présent dès le départ et régulièrement alimenté l'Asip Santé de nos commentaires lors des appels à concertation autour des diverses versions de spécifications fonctionnelles et techniques. Au printemps 2014, nous étions prêts pour les tests. Nous avons alors accompagné 11 des 15 établissements hospitaliers pilotes sélectionnés pour les premières expérimentations puisqu'ils étaient équipés de notre solution.
Cette phase a permis de valider avec l'ASIP Santé nos premiers proxys MSSanté et d'observer des cas d'usage différents. En fin d'année, une instruction DGOS demandait à tous les établissements de se mettre en conformité avant fin 2015[2].
Le déploiement se poursuit et nous pouvons déjà compter plus de 400 établissements équipés avec ENOVACOM Secure Messaging, sur un total de 1 113 établissements compatibles MSSanté (selon les derniers chiffres officiels de l'Asip Santé à mi-décembre 2018).

> « Le déploiement se poursuit et nous pouvons déjà compter plus de 400 établissements équipés avec Enovacom Secure Messaging »

Des réponses à la problématique de mutualisation

Le partenariat que nous avons noué avec Microsoft apporte un levier supplémentaire à cette dynamique. Alors que les établissements ont longtemps préféré maitriser leur service de messagerie en interne, ils s'intéressent désormais au cloud, devenu plus mature, et se sont mis à expérimenter Office 365. Mais ils devaient disposer d'un proxy compatible avec Office 365 s'ils ne voulaient pas être bloqués côté messagerie sécurisée. Face à cette demande, nous avons commencé à travailler avec les architectes de Microsoft ; cette collaboration nous permettant aussi d'apporter des réponses à la problématique de mutualisation des services de messagerie dans le contexte de mise en œuvre des groupements hospitaliers de territoire (GHT). Entre temps, Microsoft obtenait la certification Hébergeur de Données de Santé pour ses data centers localisés en France. Une conformité qui ne lui a pas posé de difficultés dans la mesure où la certification repose sur les normes ISO 27001 et 27018 que Microsoft respectait déjà.

Ces évolutions nous ont permis de faire aboutir notre partenariat sur une offre complète qui va faciliter les déploiements de la MSSanté, tout particulièrement dans le cas des GHT. Nous sommes, fin 2018, en phase pilote avec les premiers établissements désireux d'utiliser Office 365 et la MSSanté. Et nous prévoyons l'ouverture des premiers services début 2019. Nous sommes vraiment satisfaits de contribuer ainsi au développement de l'échange sécurisé de données. Nous savons que les usages sont là. Il restait à les simplifier.

1 Groupement d'Intérêt Public Carte de Professionnel de Santé, créé en 1993, dont les activités sont désormais assurées par l'Asip Santé

2 http://circulaire.legifrance.gouv.fr/pdf/2015/01/cir_39112.pdf

Face au phishing : scoring et sensibilisation

Comment évaluer la dangerosité potentielle d'une campagne de pishing, son impact à terme, et mettre en œuvre une campagne de sensibilisation efficace ? Michael Roman vous propose grilles de critères et conseils éprouvés.

Michael Roman, Responsable Sécurité du Système d'Information au CHU de Nîmes, est entré dans le monde hospitalier en 2013, après quelques années dans une petite multinationale du domaine des semi-conducteurs. « IT Security Specialist » au sein de l'équipe « Sécurité et Conformité », il apportait ses compétences pour les certifications Critères Communs et ISO 27001. Dans la santé, il découvre d'autres enjeux et des SI de plus en plus complexes.

Le secteur de la santé en France subit depuis le mois d'août, une campagne de phishing importante, avec une particularité : elle utilise des adresses email réelles en provenance d'établissements de santé ou de recherche.
Les protections face à ce type de campagne sont bien maigres : alimenter des listes noires, filtrer le contenu, bloquer des domaines…

L'efficacité, pour la majorité de ces mesures, dépend de la rapidité de réaction entre la détection et la configuration des équipements de sécurité. Une fois la configuration effectuée, on a tendance à attendre la prochaine vague. Mais on oublie souvent la vraie question : combien d'utilisateurs sont tombés dans le piège ? Combien d'adresses email sont maintenant potentiellement utilisables par un pirate? Combien d'utilisateurs ont cliqué sur le lien et rempli le formulaire ? Ou même seulement téléchargé la pièce jointe ? A quel point mon établissement est perméable au phishing[1] ? Au spearphishing[2] ? Voici une méthode simple pour maitriser une campagne de phishing, dont les résultats vous étonneront certainement.

Les critères de dangerosité d'une campagne de phishing

La réussite d'une campagne de phishing, qu'on soit RSSI ou pirate, repose sur quatre critères :

- Le niveau de renseignement (ciblage) plus ou moins précis sur les victimes,
- Les catégories de personnels ciblés,
- Le niveau de détectabilité, dépendant des techniques utilisées, plus ou moins complexes,
- Le niveau de valeur et de réutilisabilité des données récoltées.

Je propose d'établir une échelle de score pour chacun de ces quatre critères. La combinaison de ces scores permettra d'obtenir un scoring global de la dangerosité d'une campagne de phishing.

Echelle pour le niveau de ciblage de la campagne			
Niveau de ciblage	Techniques utilisées	Scénarios possibles	Note
Très ciblé	Spearphishing, renseignements poussés, email sur mesure avec infos réelles	Réponse à CV ou appel d'offre, ciblage du Directeur Financier / FOVI[3]	4
Ciblé	Usage d'un carnet d'adresses, usurpation d'identité	Phishing ciblé dans un domaine (santé), extorsions via usurpation d'email	3
Opportuniste, à scénario	Usurpation d'identité, email approximatif, menaces de piratage ou chantage de type « bluff »	Compte email désactivé, quota épuisé, faux chantage à la webcam (bluff), remboursement de trop perçu (impôts)	2
Généraliste	Publicités, spam	Loterie, gain quelconque	1

1 Hameçonnage
2 Hameçonnage ciblé. http://www.ssi.gouv.fr/particulier/principales-menaces/espionnage/attaque-par-hameconnage-cible-spearfishing/
3 Faux ordre de virement

Face au phishing : scoring et sensibilisation

Echelle pour les catégories de personnes ciblées			
Catégories	**Types de population**	**Exemples de populations**	**Note**
Peu sensibilisés	Personnels peu sensibilisés, peu concernés, non techniques, nouveaux arrivants	Personnels temporaires, internes, nouveaux arrivés	4
Métiers	Personnels sensibilisés, cœur de métiers	Cadres de santé, services critiques	3
Sensibles	Personnels très sensibilisés, susceptibles d'être ciblés, informés de ce fait, mais non techniques.	Directions sensibles (DRM[4], DRH, Finances), Financiers, Directeurs, DG, Secrétariats administratifs	2
Spécialistes	Personnel gérant l'informatique	RSSI, RSI, administrateurs systèmes et réseaux	1

Echelle pour le niveau de détectabilité (Techniques utilisées par le pirate, facilité de détection par l'utilisateur ou par un équipement de sécurité)			
Facilité de détection	**Techniques Site**	**Techniques Email**	**Note**
Difficile	Homoglyphie, usurpation de l'image de l'établissement ciblé, copie parfaite d'un site de l'établissement ciblé, non blacklisté	Adresse email piratée de l'établissement ou d'un établissement du même secteur	4
Possible	Nom de domaine approchant, ou sous-domaine approchant chez hébergeur, site sans fautes de langage et spécifique au domaine de l'établissement	Usurpation d'email d'un employé de l'établissement ou d'un établissement du même secteur	3
Facile	Nom de domaine générique (concours, admin, support…), site propre mais non spécifique	Email générique (concours, admin, support…), depuis un hébergeur classique (gmail, yahoo…)	2
Très facile	Adresse IP, nom de domaine sans rapport ou random, aucun soin au site	Email aléatoire, depuis un hébergeur classique ou sans confiance	1

Le score de dangerosité de la campagne de phishing se génère par l'addition de ces 3 premiers critères. Il est donc au minimum de 3 et au maximum de 12. Ce score suffit déjà à donner une bonne idée de la dangerosité d'une campagne, mais l'impact de cette campagne ne sera pas le même selon la valeur des données récupérées par le pirate. On doit donc prendre en compte ce dernier critère.

Echelle pour le niveau de valeur des données récupérées		
Type de donnée	**Traduction établissement**	**Note**
Permettant une intrusion immédiate	Identifiants de connexion VPN, compte administrateur d'une ressource accessible, accès distant	3
Permettant une seconde attaque	Compte email de l'établissement, identifiants d'un utilisateur	2
Faible valeur	Adresse email, liste de noms, données publiques, donnée à revente directe	1

4 Recherche médicale

Face au phishing : scoring et sensibilisation

Vous pouvez multiplier le score précédent par ce nouveau score ou bien considérer les deux parallèlement. Par exemple, une campagne de dangerosité 12/12 mais de valeur 1/3 est une campagne très ciblée, impossible à détecter pour la victime. Le pirate récoltera beaucoup d'adresses email, qu'il pourra revendre. Les conséquences restent faibles.

Lancer une campagne de phishing

L'excellent outil GoPhish permet de générer facilement des campagnes de phishing à des fins de sensibilisation et vous permet de connaître les résultats en temps réel : ouverture de l'email, clic sur le lien, envoi de données par la victime. Il s'installe et se configure sans difficulté.

Quelques conseils pour vos campagnes :

- toujours obtenir l'aval de votre hiérarchie, au plus haut niveau, avant toute campagne
- jouer sur les différents critères ci-dessus pour tester une population ou une technique particulière
- échelonner la campagne sur plusieurs semaines, voire plusieurs mois
- attention à la réaction potentiellement forte des utilisateurs : alerte importante, forte sollicitation du support informatique, escalade hiérarchique…
- il est intéressant d'utiliser les évènements comme sujets des emails piégés (news, jours fériés et fêtes, évènements sportifs…)
- il est intéressant d'explorer les travers humains : curiosité, cupidité…
- il faut veiller à ce que l'email de phishing ne soit pas bloqué par vos équipements !
- il est possible de tester la contamination par un virus en ajoutant le téléchargement automatique d'un fichier dès le chargement de la page, par exemple un fichier EICAR. Cela permet de tester vos équipements de sécurité (antivirus de flux, d'email, de serveur, de poste), et fournit des statistiques via la console de gestion de l'antivirus
- utilisez les méthodes d'un attaquant : appuyez-vous sur les informations publiques, avec un objectif (phishing de mot de passe, phishing de données confidentielles, pousser à l'installation d'un virus…)
- séparer les campagnes de sensibilisation immédiate (avec résultat affiché à l'utilisateur dès qu'il clique) et les campagnes de statistiques. Dans le premier cas, la rumeur du piège se propagera vite et faussera les statistiques (curiosité),
- pensez qu'il est assez simple de constituer une liste d'adresses email à partir de l'annuaire des praticiens de votre site web (format de l'adresse souvent en prenom.nom@domaine.fr).

> « On oublie souvent la vraie question : combien d'utilisateurs sont tombés dans le piège ? »

Et si le risque venait de l'intérieur ?

Le secteur médical se distingue par le fait que les menaces sur la sécurité viennent en majorité « de l'intérieur ». Un risque trop souvent sous-estimé dans les établissements de santé, mais qui peut être contré grâce à la gestion des privilèges sur le endpoint.

William Culbert est Directeur Europe du Sud chez BeyondTrust (autrefois Bomgar) depuis octobre 2017. Il a auparavant occupé le poste de Directeur Technique EMEA pendant plus de trois ans. Ses compétences IT portent notamment sur le devops, la sécurité, le cloud et la transformation numérique. Ses différentes expériences lui permettent d'accompagner ses clients, prospects et partenaires dans le secteur de la santé afin de les aider à se protéger des attaques constamment en mutation.

Ce que j'aime dans mon métier, c'est la possibilité d'accompagner les clients et prospects dans la mise en œuvre de leur stratégie de défense, de comprendre leurs éléments déclencheurs et leurs problématiques. Les situations sont variées et pourtant, je suis parfois surpris par certaines méthodologies qui me semblent naïves et, par déduction, risquées. Je m'explique : en cas d'attaques sur un système d'information et de fuites de données, je remarque souvent que l'on met en place une stratégie de repli en renforçant son périmètre de sécurité traditionnel pour se protéger de la menace extérieure. C'est un réflexe assez logique finalement, un peu comme si l'on cherchait à éviter la contagion. Mais comment faire si le risque vient de l'intérieur ?

Des droits admin complets

Le secteur médical est fortement impacté par les menaces liées aux erreurs d'utilisation des données et aux *malwares* (respectivement 27% et 24,6% des risques). C'est le seul secteur où les failles sont davantage causées par des employés que par des tiers : 56% des menaces viennent « de l'intérieur »[1]. Pourtant, je constate régulièrement qu'un grand nombre d'établissements hospitaliers accorde aux utilisateurs des droits *admin* complets : cela fait gagner du temps au service IT et aux utilisateurs puisque ces derniers sont indépendants et peuvent installer ou télécharger les pilotes ou applications de leur choix.

Mais avec un tel contrôle sur son poste de travail, l'utilisateur peut exécuter des processus et applications, installer (intentionnellement ou pas) des *malwares* exploitant les accès privilégiés, désactiver les paramètres système et sécurité, modifier des fichiers systèmes et ainsi lancer des *ransomwares*. Les *malwares* peuvent ensuite s'exécuter avec des privilèges élevés, les contrôles de sécurité sont contournés et les logiciels installés et lancés sans aucun contrôle ni visibilité.

Travailler efficacement et avec autonomie

Pour éviter que les cybercriminels n'exploitent les droits *admin* locaux pour obtenir des accès plus sensibles, aux domaines, applications, serveurs etc., de nombreux analystes, dont Gartner[2] , préconisent une gestion des privilèges sur le *endpoint*. Cela consiste en une combinaison intelligente de la gestion des privilèges (suppression, élévation ou limitation) et du contrôle des applications (liste blanche d'applications). Je trouve cette vision particulièrement pertinente car elle est compatible avec le besoin de productivité et de sécurité qu'ont les établissements de santé. Elle permet en outre de contrer les vecteurs d'attaques internes suivants :

- Installation de *spywares* et *adwares*
- Exposition des réseaux aux *malwares* et virus
- Accès aux données d'autres utilisateurs et fuite de données
- Désinstallation d'anti-virus
- Création ou modification de comptes utilisateurs, etc.

> « La gestion des privilèges sur le endpoint consiste en une combinaison intelligente de la gestion des privilèges et du contrôle des applications ; une vision pertinente car compatible avec le besoin de productivité et de sécurité des établissements de santé »

Ne sous-estimez pas le risque provenant de vos propres utilisateurs : la gestion des privilèges sur le *endpoint* leur permet d'avoir les niveaux de droits nécessaires pour lancer les applications dont ils ont besoin pour travailler efficacement et avec autonomie et de bénéficier d'élévations de privilèges sans mettre en danger les systèmes et données de l'hôpital et de ses patients. Le juste équilibre entre productivité et sécurité en somme.

1 Verizon, Data Breach Investigation Report Verizon, 2018

2 Gartner Inc., Reduce Access to Windows Local Administrator With endpoint privilege management, Robinson, Lori, October 20, 2017

Tests d'intrusion et scans de vulnérabilité : in-dis-pen-sables

Les prestations de tests d'intrusion et les campagnes de scans de vulnérabilités sont complémentaires et doivent s'inscrire dans une démarche globale de sécurisation des SI et de leur amélioration continue.

Frédéric Cabon a exercé des fonctions de Responsable informatique dans une société d'ingénierie navale. Passionné par l'informatique et la sécurité des systèmes numériques, il s'est notamment formé au CEH V9. Actuellement Responsable Sécurité des Systèmes d'Information au CHRU de Brest, il dispense des modules d'enseignement à l'Institut Supérieur de Formation (Service Santé Social du Groupe ISF).

Les systèmes d'information hospitaliers (SIH) sont devenus des cibles privilégiées des hackers. Cet été, pas moins de trois millions de dossiers patients se sont faits dérober (dans des hôpitaux à Singapour et à Hong Kong). Ces dossiers volés viendront rejoindre les nombreuses bases de données patients en vente sur le *dark Web*. La valeur de la donnée médicale ne cessant d'augmenter, il faut se préparer à une recrudescence des attaques informatiques des centres médicaux et hospitaliers.

Aujourd'hui, le CHRU de Brest intègre des tests d'intrusion périodiques et réalise des scans de vulnérabilités ponctuels de ses systèmes d'information. Ces dispositifs sont devenus des outils à part entière et viennent compléter les éléments de défense classiques : firewall, proxy, antivirus, sondes, etc.

1 Les tests d'intrusion

Les prestations de tests d'intrusion ont pour objectif principal de dresser un état des lieux de la sécurité d'un système d'information ou d'une application à un instant donné et de remonter les vulnérabilités de sécurité réellement exploitables. Les tests d'intrusion, autrement appelés *pentest* (pour *penetration test*), permettent de mesurer le risque associé aux systèmes d'information en simulant des conditions d'attaques réalistes. Les résultats de ces travaux viennent alimenter l'analyse de risque du SMSI (Système de Management de la Sécurité de l'Information) et un plan d'actions permettant de minimiser ces risques est défini, puis mis en œuvre.

A mon arrivée, en 2011, au poste de RSSI, je souhaitais avoir une première vision « réelle » de notre niveau de sécurité. Un regard externe sur la foi d'un *pentest* me paraissait alors pertinent. Il me semblait également indispensable d'inclure les membres de la DSI très tôt dans la démarche : ils ont notamment été associés au choix du périmètre audité et du prestataire retenu.

Un résultat édifiant

Le résultat du premier audit a été édifiant et a permis de mettre en avant un grand nombre de failles logicielles mais également structurelles.
Ces travaux m'ont donné des arguments, sur la base de cas concrets et tangibles, auprès de la direction générale et de la DSI, sur la nécessité de mettre en place une nouvelle politique de sécurité et de dégager des moyens complémentaires permettant l'application d'un plan d'actions conséquent afin de corriger les failles majeures relevées lors de l'audit. C'est à la suite de ce premier audit, par exemple, que nous avons durci notre politique de mots de passe, en passant d'une politique très souple (possibilité de mettre un mot de passe simple, voire à blanc) à une politique de mot de passe utilisateur complexe.

Cet exercice a également été bénéfique pour les équipes informatiques. Une seconde prestation ayant été très vite décidée, la motivation des équipes informatiques à appliquer les bonnes pratiques de sécurité et les règles définies dans la nouvelle PSSI n'en était que renforcée.

Tous les deux ans

Depuis, nous réalisons ce type de prestations tous les deux ans. Cette régularité nous permet d'obtenir des indicateurs de progression et de mettre à jour les plans d'actions en priorisant les nouveaux risques découverts.

> « Les audits de vulnérabilité sont systématiquement réalisés lors de la mise en production de nouveaux éléments numériques dans les SIH, avant ou lors de la recette »

Tests d'intrusion et scans de vulnérabilité : in-dis-pen-sables

Les phases généralement retenues lors de nos prestations de *pentest* sont les suivantes :

- Phase contractuelle : Un contrat entre les deux parties est rédigé. Celui-ci définit les responsabilités de chacun, le périmètre audité, le type d'attaques qui seront menées, ainsi que la liste des IP attaquantes.
- Phase de découverte :
  - Identification de l'architecture (routeurs, firewalls, machines) ;
  - Identification des systèmes (systèmes d'exploitation) ;
  - Identification des applications (noms et versions).
- Phase d'intrusion :
  - Recherche des vulnérabilités présentes (outils spécifiques) ;
  - Exploitation des vulnérabilités (utilisation de codes ou techniques d'exploitation) ;
  - Qualification des vulnérabilités.
- Analyse :
  - Études des risques encourus ;
  - Établissement des recommandations.

Le choix de la société de service spécialisée en *pentest* est essentiel. Au CHRU, nous nous appuyons sur la liste des prestataires qualifiés par l'ANSSI. Cela nous apporte des garanties sur les compétences des auditeurs en charge de l'audit et sur la méthodologie utilisée. De plus, un recours auprès de l'ANSSI est possible si la prestation réalisée s'avère non conforme au référentiel PASSI[1].

2 Le scan de vulnérabilité

Pour compléter les prestations de *pentest*, il me semble indispensable de mettre en place une politique continue d'audit de vulnérabilité interne permettant de corriger les failles dès l'installation d'un nouvel élément dans le SI.
En conformité avec sa politique de sécurité, le CHRU de Brest effectue régulièrement des scans de vulnérabilité sur son infrastructure et les applications métiers qu'elle héberge. Ces audits sont effectués avec des outils prévus à cet effet (Nessus, Nmap, OWASP Zap[2]…). Ils sont systématiquement réalisés lors de la mise en production de nouveaux éléments numériques dans les SIH (serveurs, middleware, bases de données, applications ….), avant ou lors de la recette. Cela pour deux raisons, la première étant que, lors de la recette d'une nouvelle application, le fournisseur à une obligation contractuelle de corriger les failles majeures mises en avant, la seconde étant qu'il est évidemment plus aisé d'effectuer ce type d'exercice alors que l'élément contrôlé n'est pas encore en production et donc soumis aux contraintes associées.

Lors de la rédaction des CCTP (Cahiers des Clauses Techniques Particulières), une clause spécifique d'auditabilité est incluse. Les serveurs, bases de données, middleware ou applications comportant des vulnérabilités CVE (*Common Vulnerabilities and Exposures*), ou du top 10 de l'OWASP, devront être corrigées par le fournisseur avant la mise en production. Concernant les éléments en production, le prestataire disposera d'un temps déterminé, lors de la rédaction du CCTP, pour corriger les failles dès lors que celles-ci auront été découvertes et notifiées au prestataire.
La manipulation de scanner de vulnérabilité doit être réalisée uniquement par une personne habilitée et formée à ces outils. En effet, lancer des scans de vulnérabilité sans maîtrise des outils peut s'avérer très risqué et peut compromettre l'intégrité des systèmes scannés.
Tout comme les résultats des prestations de *pentest*, les scans de vulnérabilité réalisés en interne permettent le suivi par tableaux de bord via des indicateurs factuels.

L'implication des responsables SI dans ces démarches est primordial. Il est en effet nécessaire de dédier du temps aux équipes de la DSI afin de leur permettre de corriger les failles mises en avant dès leur découverte. Or c'est souvent cela qui fait défaut.

> « La manipulation de scanner de vulnérabilité doit être réalisée uniquement par une personne habilitée et formée à ces outils »

1 Prestataires d'Audit de la SSI
2 Open Web Application Security Project

Scanners de vulnérabilités : connaître son SI pour mieux le protéger

Pour protéger son système d'information, il est indispensable de bien le connaître. Si la cartographie de l'ensemble des composants du SI apparaît comme LA base de la sécurité, le RSSI pourra se doter de différents outils permettant de prendre conscience des vulnérabilités. Tour d'horizon des solutions Open Source ou libres.

Administrateur systèmes et réseaux de formation, **Charles Blanc-Rolin** a intégré la DSI du Centre Hospitalier de Saint-Flour en 2008. Sur ces dix années, il a participé à de nombreuses étapes de la mutation numérique de l'établissement et continue d'y contribuer. Passionné par nature, toujours en quête de renouveau, il s'est rapidement épanoui dans le rôle de Référent des Systèmes d'Information, poste qu'il occupe officiellement depuis septembre 2015.

Comment fonctionne un scanner de vulnérabilités ?

Tests réseau. La première méthode d'analyse des vulnérabilités consiste à scanner les ports ouverts sur la machine cible, à la recherche d'informations relatives aux versions des logiciels utilisés ainsi qu'à leur configuration, afin de définir si ces logiciels utilisés disposent ou non des derniers correctifs de sécurité et si un mauvais paramétrage pourrait les rendre vulnérables.

Tests locaux. La deuxième méthode consiste à donner un accès « local » à la machine cible, via SSH par exemple, toujours dans le même but : savoir si les logiciels installés sont vulnérables.
Gratuits ou payants, ces outils permettent au RSSI d'établir l'état de santé de son système d'information grâce à des rapports et des graphiques notamment. Ils l'aident à planifier les actions correctives à engager grâce aux solutions d'atténuation proposées par l'outil, qui peuvent aller de l'application de correctifs de sécurité à un paramétrage plus fin des logiciels installés, en passant par le changement des mots de passe par défaut.

Si Nessus, proposé au départ sous licence GPL, devenu aujourd'hui un logiciel propriétaire, reste pour beaucoup le pionnier des scanners de vulnérabilités, son digne héritier OpenVas, toujours Open Source, malgré la forte implication d'un industriel dans le projet, fait le bonheur de nombreux utilisateurs, ainsi que les éditeurs qui ont construit leurs solutions sur ce désormais célèbre moteur d'analyse de vulnérabilités.

Pour aller plus loin…
Même si des scanners de vulnérabilités tels que Nessus ou OpenVas sont déjà extrêmement pointus de par les règles d'analyses qu'ils intègrent, certains outils réservés à des usages spécifiques peuvent permettre d'aller plus loin dans l'analyse.

Analyses Web. Auditer son site, portail ou application Web est loin d'être inutile. Point d'entrée dans le système d'information, source de fuite de données ou nuisance pour l'image de l'établissement, le Web présente de nombreux risques. Ce n'est pas l'OWASP (Open Web Application Security Project) qui dira le contraire. La célèbre fondation édite chaque année son célèbre Top 10 des vulnérabilités Web les plus critique[1], ainsi que des guides de recommandations. Elle référence également plusieurs outils d'analyse qui se basent sur ses recommandations[2] et propose plusieurs scanners de vulnérabilités Web comme Zap[3], WebMalwareScanner[4] ainsi que des scanners pour les très répandus CMS, Joomla et WordPress, avec JoomScan[5] et WordPress Scanner[6]. Pour les utilisateurs de CMS, d'autres outils s'offrent à eux comme CMSmap[7] ou WPScan[8]. À garder également dans sa caisse à outils : Grabber[9] de Romain Gaucher, disponible sur la distribution Kali qui permet de tester si une application Web est vulnérable aux attaques les plus répandues.

Auditer son Active Directory. L'Active Directory est, même si on l'oublie souvent, le maillon le plus sensible d'un système

> « Le scanner de vulnérabilités permet au RSSI de rendre des comptes à sa direction mais aussi de la solliciter pour obtenir des moyens. »

d'information basé sur une architecture Microsoft, soit plus de 99 % des SI et probablement 100 % des SIH français. C'est lui qui contient l'annuaire des utilisateurs du SI, leurs mots de passe et régit les droits d'accès aux informations, il est donc essentiel de bien le protéger. Active Directory est un outil pointu, complexe et parfois capricieux, et si tous les administrateurs systèmes savent l'installer et l'utiliser, rares sont les experts capables de le configurer proprement, ce qui en fait généralement un véritable talon d'Achille du SI, sans que personne ne s'en rende vraiment compte.
Forts de ce constat, deux anciens de l'ANSSI, Emmanuel Gras et Luc Delsalle ont fondé Alsid, une structure spécialisée dans l'audit et la sécurisation d'Active Directory[10].
Mais ils ne sont pas les seuls experts français à s'être penchés sur les faiblesses de l'Active Directory et l'authentification Windows. Citons aussi Benjamin Delpy (@gentilkiwi) et son

Scanners de vulnérabilités : connaître son SI pour mieux le protéger

célèbre outil Mimikatz[11] qu'il a déjà présenté aux quatre coins de la planète dans de nombreuses conférences, ainsi qu'aux ingénieurs de la société Microsoft chez qui il a été invité, sans oublier son désormais partenaire dans l'écriture de l'outil, Vincent Letoux qui propose de son côté PingCastle[12]. Cet outil gratuit (non Open Source) est extraordinaire de simplicité. Exécuté depuis une session utilisateur lambda ouverte sur un poste connecté au domaine, il donne très rapidement un état santé précis de son Active Directory et de précieux conseils pour corriger son mauvais paramétrage. Si vous ne le connaissez pas, attendez-vous à voir du rouge dans le cadran lors de sa première exécution ! À utiliser sans aucune modération !
Si vous souhaitez voir ce que peuvent donner la rencontre entre leurs deux cerveaux en ébullition, je vous recommande d'aller faire un tour la page dédiée à DCShadow[13].

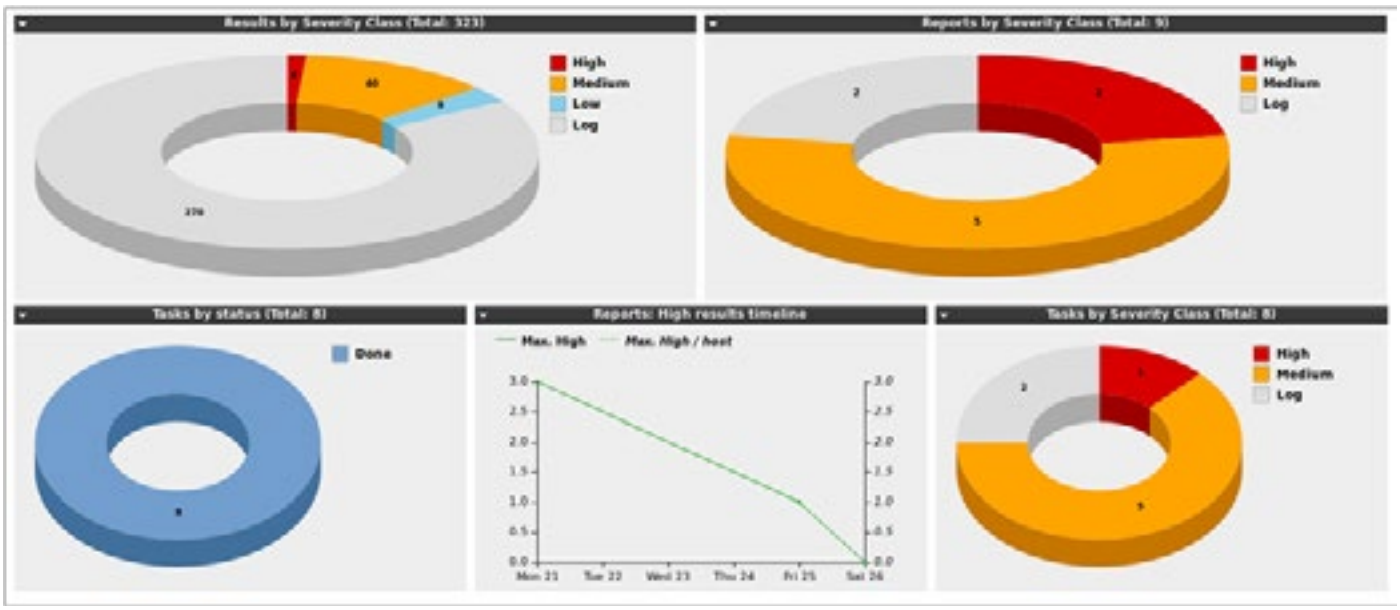
Les scanners de vulnérabilités « embarqués ». Aujourd'hui, certains pare-feu d'entreprise ou des solutions de protection « end point » embarquent des fonctionnalités de détection des vulnérabilités. Même si elles ne seront jamais aussi précises que des solutions dédiées, elles pourront s'avérer très utiles, voire complémentaires, notamment dans l'analyse des postes clients du parc, qui ne sont bien souvent pas dans le spectre des analyses que l'on met en place via les scanners de vulnérabilités.
Sans même le savoir, une solution que vous utilisez dispose peut-être d'une telle fonctionnalité. Renseignez-vous.

Le scanner de vulnérabilités permet au RSSI d'engager le dialogue avec la DSI, de guider les administrateurs, de rendre des comptes à sa direction mais aussi de la solliciter pour obtenir des moyens. En clair, un outil dont le RSSI ne pourra plus se passer.

Les références, en ligne

1 https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
2 https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools
3 https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
4 https://www.owasp.org/index.php/OWASP_Web_Malware_Scanner_Project
5 https://www.owasp.org/index.php/Category:OWASP_Joomla_Vulnerability_Scanner_Project
6 https://www.owasp.org/index.php/OWASP_Wordpress_Vulnerability_Scanner_Project
7 https://github.com/Dionach/CMSmap
8 https://wpscan.org/
9 http://rgaucher.info/beta/grabber/
10 https://www.alsid.it
11 http://blog.gentilkiwi.com/mimikatz
12 https://www.pingcastle.com
13 https://www.dcshadow.com/

Tableau de bord des résultats d'analyses réalisées avec OpenVAS



L'intérêt d'un cloud hybride : retour d'expérience

Le cloud hybride constitue une solution de synchronisation et de partage de fichiers capable de répondre aux attentes des utilisateurs métier tout en offrant de hauts niveaux de sécurité, de contrôle et de flexibilité. Retour d'expérience du GHT Psy Nord-Pas-de-Calais.

Mettre en musique la transformation numérique dans la santé, et surtout prendre en compte la démarche de cybersécurité dès le démarrage des projets, tels sont les principes d'action de **Didier Verbeke**. Après avoir été Directeur des Technologies et des Systèmes d'Information, et RSSI, de l'EPSM (Etablissement Public de Santé Mentale) des Flandres, il continue à propager son virus de bon sens en tant que RSSI et DPO du GHT Psy Nord-Pas-de-Calais, qui rassemble quatre EPSM.

Comme dans toutes les structures de santé, nos professionnels communiquent énormément. Mais, contrairement aux établissements MCO, ils œuvrent sur des lieux distincts et géographiquement dispersés : une cinquantaine de sites dans un cercle de 80 km de diamètre ! Les intervenants tiers (partenaires, fournisseurs, intérimaires, prestataires de services externes, sous-traitants) jouent un rôle croissant dans notre organisation et dans notre quotidien et les groupements hospitaliers de territoire (GHT) augmentent le nombre des professionnels impliqués. Nos professionnels et nos partenaires sont donc sans cesse en mouvement, avec un fort besoin de moyens de communications fiables, sécurisés et disponibles en permanence. Ils doivent également pouvoir partager facilement leurs fichiers avec les acteurs à l'intérieur ou à l'extérieur de nos réseaux, sans pour autant les exposer aux risques de sécurité.

Stop aux comptes personnels de partage et supports amovibles

De manière générale, pour être productifs, les employés ou agents sont dépendants des données de leur entreprise ou institution. Mais lorsqu'ils s'appuient sur leurs comptes personnels de partage en ligne de fichiers pour donner l'accès à leurs données, ils exposent celle-ci à des risques significatifs. Si la direction informatique se contente de bloquer ces comptes sans fournir une alternative autorisée, la productivité en souffrira. A l'opposé, laisser l'utilisation de ces comptes et supports amovibles se poursuivre est impensable. En fait, nous avions besoin d'une solution de synchronisation et de partage de fichiers bénéficiant des niveaux de sécurité, de contrôle et de flexibilité indispensables, mais également capable de garantir aux utilisateurs une expérience riche, de type grand public, garante d'une adoption rapide et complète.
Mon objectif étant de permettre une communication ouverte tout en respectant les principes fort de sécurité et les fondamentaux du RGPD (violation de données, traçabilité...), il a fallu réfléchir à la mise en œuvre d'outils facilitants et sécurisés.

Un cloud synchronisé pour un accès hors réseau

Nous avons mis en place un cloud hybride pour la portabilité et la confidentialité des données sensibles, en évitant particulièrement les supports mobiles trop à risque. Le cloud comprend une partie en interne confidentielle et sécurisée, et une partie externe pour tout ce qui est non confidentiel, avec des mécanismes de cryptage de bout en bout.
Il permet à tous les métiers (médecins, soignants, techniques, administratifs…) d'accéder en temps voulu à des informations sécurisées. Depuis 2015, il est utilisé par 1200 agents. Le retour est intéressant sur ce type d'outils et avec 200 comptes en ligne actuellement, nous avons du recul.
Un autre aspect important : ce cloud synchronisé pour un accès hors réseau permet de stocker en temps réel les procédures dégradées (prescriptions médicales, médicamenteuses, administratives et techniques) en cas de sinistre ou de perte de disponibilité du SI.
Enfin, point non négligeable : il répond aux attentes du RGPD sur la sécurité et sur la traçabilité de la donnée et de son cycle de vie.

> « Trop souvent, les métiers choisissent eux-mêmes les outils sans tenir compte des besoins en sécurité »

Une zone de stockage pour offrir l'accès à distance

Nous avons souhaité héberger nos propres données pour diverses raisons. Pour cela, nous avons créé ce que l'on appelle une zone de stockage dans notre centre de données. Cette zone de stockage est une fonctionnalité offrant un accès à distance aux utilisateurs. Elle peut également se connecter à d'autres applications grâce à des connecteurs spécifiques. Le stockage sur site me parait idéal lorsque la conformité des données est rigoureuse, car il limite l'accès des utilisateurs et garantit la sécurité des données par le chiffrement de fichiers.

L'intérêt d'un cloud hybride : retour d'expérience

L'accessibilité se fait par un « contrôleur de mise à disposition » avec les possibilités suivantes :

- Mise à disposition des applications auprès de tous les sites
- Redirection des utilisateurs de façon automatique et invisible vers un cloud ou un datacenter secondaire pendant la reprise automatique
- Garantie de haute disponibilité des services et des applications

La compréhension des besoins métier

Dans la maîtrise des risques liée à ce type de projet, il faut plutôt s'attarder sur les métiers que sur la technique pure. Nous savons que les métiers ont besoin d'outils permettant une meilleure accessibilité à l'information. La DSI a son rôle de maitrise d'œuvre, mais ce qui est important à mon sens, c'est de bien comprendre les besoins du métier. On constate trop souvent que les métiers choisissent eux-mêmes les outils sans tenir compte des besoins en sécurité. Certains choix proposés par des start-up offrent un réel apport fonctionnel, mais ils ne sont pas toujours très sécurisés et peuvent potentiellement entrainer des risques très élevés.
L'idéal serait que les métiers acquièrent en maturité sur les aspects SSI et aient le réflexe de frapper à mon bureau pour me dire: « *Monsieur le RSSI, venez voir, il y a quelque chose qui me chiffonne sur la sécurité de ce produit* ! »

Solution de prise en main à distance : un choix loin d'être anodin

La multiplication des logiciels, appareils et dispositifs médicaux utilisés dans les structures de soins accroît d'autant le nombre de fournisseurs intervenant pour les maintenir ou les dépanner, faisant de la prise en main à distance un point de plus en plus sensible en matière de sécurité.

William Culbert est directeur Europe du Sud chez BeyondTrust (autrefois Bomgar) depuis octobre 2017. Il a auparavant occupé le poste de directeur technique EMEA pendant plus de trois ans. Ses compétences IT portent notamment sur le devops, la sécurité, le cloud et la transformation numérique. Ses différentes expériences lui permettent d'accompagner ses clients, prospects et partenaires dans le secteur de la santé afin de les aider à se protéger des attaques constamment en mutation.

Ils débordent d'énergie, de passion, d'inventivité. Sans cesse à l'affût de nouvelles méthodes de travail, ils ne perdent jamais de vue leur objectif et font preuve d'une patience et d'une imagination sans faille. Pourtant, nous nous passerions volontiers de leur ferveur. Chaque semaine, les cybercriminels nous prouvent de quoi ils sont capables. Hélas, la liste (non exhaustive) est longue : ransomware avec Samsam, WannyCry, Petya, compromission de mots de passe admin par un employé avec des droits IT élevés, social engineering, etc.

De nombreux rapports, tels que le Global Security Report 2017 de Trustwave, révèlent que les chemins d'accès les plus utilisés par les cybercriminels pour s'infiltrer dans un réseau sont les solutions de prise en main à distance. L'informatique n'est pas le cœur de métier des établissements de santé. Pourtant, ils sont sous la pression de nombreuses contraintes imposées par leurs fournisseurs et, en parallèle, peinent à maintenir leur parc informatique à jour. Alors, évidemment, les établissements hospitaliers sont une cible de choix pour les personnes malveillantes et ce pour des raisons fonctionnelles et structurelles.

Quelles questions avant de choisir

Commençons par l'intensification de la télémédecine et de la mobilité du personnel : de nombreux collaborateurs doivent se connecter à un système à tout moment, de partout et depuis différentes plateformes. Sans compter qu'ils se voient régulièrement confier de nouveaux équipements, tels que des logiciels installés sur des tablettes, sans même avoir de formation à leur utilisation.
La mise en place de structures telles que les ARS ou les GHT implique également l'exploitation de systèmes mutualisés centralisés qui doivent être accessibles par du personnel dispersé géographiquement.
Enfin, la multiplication des logiciels, appareils et dispositifs médicaux utilisés dans les structures de soins - et donc des fournisseurs devant intervenir à distance pour les maintenir ou les dépanner - est certainement le point le plus sensible, surtout devant la nécessité évidente d'avoir des équipements opérationnels à tout moment.

Les solutions de prise en main à distance sont donc un élément fondamental pour tout établissement de santé. Toutes ne se valent pourtant pas en termes de fonctionnalités, et surtout de sécurité. Le choix d'une telle solution doit être considéré avec la plus grande attention et les questions sont nombreuses :

- Comment faire pour n'avoir qu'une seule solution qui assure le support de tous les systèmes et à tout moment ?
- Aurai-je de la visibilité et du contrôle sur les accès et les activités réalisées ?
- Comment faire pour qu'un accès ne soit accordé qu'à une personne définie, sur une plage horaire dédiée et pour intervenir sur un périmètre donné ?
- Comment garantir que le technicien qui viendra se connecter sur un poste de travail n'est pas malveillant et qu'il ne compromettra pas la confidentialité des données patients ?
- Chaque session ne peut-elle pas être enregistrée en cas d'erreurs ou de litiges ?

> « De nombreux rapports révèlent que les chemins d'accès les plus utilisés par les cybercriminels pour s'infiltrer dans un réseau sont les solutions de prise en main à distance »

Ce qu'il faut vérifier

Rares sont les solutions de prise en main à distance qui peuvent se vanter de conjuguer productivité, ergonomie, respect des règlementations et sécurité. Il est de la responsabilité des services informatiques de considérer tous ces aspects avant de choisir leur outil.
Le conseil que je donne souvent aux établissements de soins est de vérifier les points suivants :

Solution de prise en main à distance : un choix loin d'être anodin

• Compatibilité avec tous les OS (précédents et actuels), plateformes et systèmes
• Traçabilité, gestion simplifiée des audits et conformité avec les marquages
• Sécurité de l'architecture et des flux
• Respect des politiques de sécurité en place
• Possibilité de collaboration avec d'autres experts

Les outils de prise en main à distance ne doivent pas être une porte d'entrée vers les systèmes critiques, données patients, informations financières et bien d'autres informations. Une solution parfaitement sécurisée s'inscrira dans la stratégie de défense de l'établissement et sera un rempart puissant et efficace contre les menaces actuelles, internes ou externes.

> « Rares sont les solutions de prise en main à distance qui peuvent se vanter de conjuguer productivité, ergonomie, respect des règlementations et sécurité »

Intelligence Artificielle et cyber-sécurité

La prochaine vague de cyber-attaques mobilisera certainement les technologies d'IA. Présentes dans nos infrastructures depuis 2005, pour l'apprentissage anti-spam par exemple, ces technologies progressent en permanence et permettent déjà d'optimiser la protection des Systèmes d'Information.

Stratégiste Cyber-sécurité chez Trend Micro, **Loïc Guézo** supervise le développement stratégique de la société japonaise dans la zone Europe du Sud. Il a récemment été nommé réserviste citoyen de la Police nationale, auprès de la Sous-Direction de la Lutte contre la Cybercriminalité de la Direction Centrale de la Police Judiciaire (DCPJ), avec pour mission de participer à la sensibilisation du tissu économique local aux problématiques de cybercriminalité.
Il est par ailleurs membre de l'ARCSI (Association des Réservistes du Chiffre et de la Sécurité de l'Information) et administrateur du CLUSIF (Club de la Sécurité de l'Information Français).
Avant de rejoindre Trend Micro, il a occupé différentes fonctions dans le secteur informatique, chez Sagem Défense, au sein de l'Agence Française de Développement et chez IBM France.

L'avenir de la cyber-sécurité passe-t-il par l'Intelligence Artificielle ? Au-delà du buzzword, les technologies d'IA sont déjà une réalité dans ce domaine, et de longue date. Elles constituent certes une innovation, mais une innovation de continuité, une simple étape supplémentaire dans l'évolution permanente des solutions sur lesquelles portent nos efforts de recherche et développement. Trend Micro compte en effet déjà plus de 300 ingénieurs spécialisés en IA. L'IA constitue bien évidemment l'un des moyens à privilégier pour ne pas se laisser distancer dans la course entre le cybercriminel et le policier numérique. La prochaine vague de cyber-attaques utilisera sans aucun doute les technologies d'IA pour agresser et contourner les systèmes de sécurité.
Préparons-nous aux futures batailles d'IA ! C'est d'ailleurs ce que fait la DARPA (Defense Advanced Research Projects Agency, agence américaine chargée des projets de recherche avancée de défense), quand elle organise le défi Cyber Grand Challenge qui oppose des hackers cybernétiques, sans la moindre intervention humaine.

Des technologies présentes dans nos infrastructures depuis 2005

Afin d'accompagner au mieux les professionnels de santé, nous avons défini pour ce secteur une architecture de sécurité de référence, en adéquation avec des besoins génériques. Nous sommes également capables d'apporter des réponses spécifiques au domaine du biomédical notamment, connu pour sa complexité (cf encadré).
C'est dans ce cadre, et en fonction de l'évolution des menaces, que nous introduisons naturellement les technologies d'Intelligence Artificielle, selon les besoins et attentes des établissements de santé, en faisant preuve de souplesse. Présentes dans nos infrastructures depuis 2005, pour l'apprentissage anti-spam par exemple, les technologies d'IA progressent en permanence et permettent déjà d'optimiser la protection des systèmes.
Premier exemple : la détection d'e-mails frauduleux. Les attaques de type BEC (Business Email Compromise) qui consistent à se faire passer pour le décideur d'une organisation, avec demande urgente de virement bancaire ou de transmission de données sensibles, sont difficiles à détecter parce que les courriels n'ont généralement pas de pièce jointe ou de lien URL, qui sont le plus souvent reconnus comme suspects.

> « Préparons-nous aux futures batailles d'IA ! »

L'IA pour analyser le style d'écriture

Nous avons récemment introduit l'analyse du style d'écriture (Writing Style DNA). Il s'agit d'une nouvelle couche de protection contre ces attaques, qui utilise l'Intelligence Artificielle pour définir et reconnaître le style d'écriture d'un utilisateur, avec plus de 7 000 caractéristiques, à partir de ses messages antérieurs et par comparaison à des faux suspects. Lorsqu'un courriel est soupçonné d'usurper l'identité d'un utilisateur important, le style est comparé à ce modèle d'IA, un avertissement est envoyé à l'expéditeur impliqué, au destinataire et au service informatique. Cette technologie combine les connaissances d'un expert en sécurité et un modèle mathématique d'auto-apprentissage pour identifier les faux e-mails en examinant à la fois les facteurs comportementaux et l'intention d'un e-mail.
Elle intéresse le monde hospitalier, qui commence à connaitre ce type d'attaques, comme on peut le voir par exemple grâce au dispositif d'alertes du Portail d'Accompagnement Cybersécurité des Structures de Santé[1]. En avril 2018, plusieurs centres hospitaliers signalaient en effet une

1 https://www.cyberveille-sante.gouv.fr

tentative d'escroquerie, leurs directions financières ayant été contactées par mail au nom de la DGFIP (Direction Générale des Finances Publiques) par un individu souhaitant obtenir les références de comptes clients ainsi que des informations comptables confidentielles. « Les mails envoyés sont nominatifs, rédigés en bon français, et leur auteur emploie les tournures habituelles des courriers administratifs. Deux adresses émettrices ont été pour le moment utilisées », précisait l'alerte.

Deux approches du marché

Deuxième exemple : les technologies d'IA se démocratisent actuellement sur le poste de travail, grâce aux nouvelles capacités et puissances de calcul, avec la mise en œuvre de moteurs de Machine Learning avant et après exécution des logiciels et pièces jointes.
Si l'IA est désormais présente dans l'ensemble des offres de cyber-sécurité, on peut cependant distinguer deux approches du marché : les acteurs implantés de longue date (comme Trend Micro, créée en 1988), mais qui communiquent depuis peu sur ce thème, et les nouveaux entrants, qui font de l'IA un fer de lance et tentent de décrédibiliser les premiers. Problème de ces jeunes pousses : elles génèrent beaucoup de faux positifs car il leur manque l'expérience accumulée sur la base des anciennes technologies permettant de continuer à éliminer 95% des flux de malwares.
N'oublions pas que l'IA, c'est non seulement des algorithmes nouveaux nécessitant de la puissance de calcul, mais surtout la capacité d'apprendre sur une base de vastes jeux de données qualifiées.

Sécuriser le parcours de soins : une priorité !

Développement du programme Hôpital numérique, réorganisation du maillage territorial du secteur santé, entrée en vigueur du RGPD et gestion des données de santé : 2018 a été marquée par de profondes mutations. Il est aujourd'hui primordial de se prémunir contre des cyber-attaques capables de paralyser un système et d'entraver le bon fonctionnement d'un établissement.
Avec des établissements de santé de plus en plus connectés, et la multiplication exponentielle du nombre de points d'entrée possibles exploités par les cyber-assaillants (imagerie, matériel biomédical, pharmacie), la santé ne peut plus être conçue sans cyber-sécurité.
Dans ce contexte, la protection du système de santé et des environnements biomédicaux s'impose comme une priorité.
Fort de 30 ans d'innovation au service de ses clients, Trend Micro contribue à sécuriser le parcours de soin au sein des établissements de santé et met un point d'honneur à proposer à ces derniers des solutions de sécurité à la fois simples, efficaces et rapides.
Trend Micro travaille notamment sur une campagne de sensibilisation 2019 innovante, axée sur la protection des environnements biomédicaux, ciblant les GHT, les groupements privés et les institutionnels (ARS,GCS).

0.4

RGPD ET CYBERSÉCURITÉ

RGPD et contrats des fournisseurs IT Santé : peut mieux faire ?, **Me François Coupez** P. 63 À 65
Data Protection Officer : quel positionnement, quel périmètre, **Fabien Dachicourt** P. 66 & 67
Le point de vue d'un chargé de mission en ARS, **Guy Marty** P. 68 À 70
Comment faciliter la mise en œuvre du RGPD dans les laboratoires de biologie médicale, **Bruno Gauthier** P. 71 & 72
Ce qu'il faut savoir à propos du Privacy Impact Assessment, **Cédric Cartau** P. 73
ACSS : une réponse à la menace de cybersécurité dans le secteur santé, **ASIP Santé** P. 74 À 76

RGPD et contrats des fournisseurs IT Santé : peut mieux faire ?

La protection du SI des établissements de santé suppose que l'ensemble de ses éléments, ou des acteurs qui y interviennent, quand ils sont le fait de tiers, soient soumis à des engagements contractuels stricts. Malgré quelques progrès, grâce au RGPD, de nombreux points d'attention demeurent.

Maître François Coupez est avocat à la Cour, associé-gérant et fondateur du cabinet ATIPIC Avocat, classé en quelques années parmi les meilleurs cabinets d'avocats français spécialisés en nouvelles technologies et protection des données (par les Trophées du droit, Leaders League, Lawyer Monthly, etc.). Ancien responsable juridique d'entreprise, membre de l'AFCDP[1], il est également conférencier et formateur (à Paris II, au CELSA, à Dauphine, au CNAM, etc.). Il assiste depuis près de 20 ans les acteurs privés et publics en matière de sécurité des systèmes d'information, de protection des données à caractère personnel, de dématérialisation ou encore de contrats informatiques.

Depuis l'entrée en application du Règlement Général sur la Protection des Données (RGPD), le 25 mai 2018, il devient plus facile pour les entreprises clientes de prestations IT d'obtenir de leurs fournisseurs des engagements stricts, clairs et détaillés quant à la sécurité des prestations qu'ils fournissent.

En effet, pour autant que les prestations consistent dans le traitement de données à caractère personnel pour le compte d'un donneur d'ordre, celui-ci a l'obligation :

• de ne travailler qu'avec « des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée ». En d'autres termes et sous peine des sanctions prévues par le RGPD, ils ne doivent faire appel qu'à des prestataires qui peuvent notamment prouver que leurs produits ont été conçus « privacy by design » quand ils sont amenés à traiter des données à caractère personnel pour le compte de l'entité cliente ;

• de prévoir dans son contrat avec son sous-traitant une liste d'obligations spécifiques détaillées à l'article 28 du RGPD (vers lequel va renvoyer le nouvel article 60 de la loi du 6 janvier 1978 tel que modifié par l'ordonnance n°2018-1125 du 12 décembre 2018)[2], et notamment la mise en œuvre de solutions de sécurisation des données, l'interdiction d'usage tiers de celles-ci, un droit d'audit prouvant le respect des obligations, etc.

Des spécificités dans le monde de la santé ?

Si la prestation en question est effectuée pour le compte d'un établissement soumis au droit public et renvoie au Cahier des clauses administratives générales applicables aux Techniques de l'Information et de la Communication (CCAG-TIC), l'article 5.2.2 de ce document a prévu l'hypothèse de l'évolution de la législation sur la protection des données à caractère personnel en cours d'exécution du marché. Il énonce ainsi que « les modifications éventuelles, demandées par le pouvoir adjudicateur afin de se conformer aux règles nouvelles, donnent lieu à la signature d'un avenant par les parties au marché », ce qui a permis aux établissements de santé concernés par l'établissement de ce texte de « mettre à jour » leurs contrats pour intégrer ces nouvelles obligations et enfin réussir à imposer à leurs prestataires, dans certains cas, le respect de règles de base en matière de sécurité.

Surtout, dans le domaine de la santé, un cadre contractuel supplémentaire est susceptible de compléter l'obligation générale de l'article 28 du RGPD. Ainsi, si la prestation en question, effectuée en qualité de sous-traitant, consiste en l'hébergement de données de santé « à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social »[3], l'article R. 111-11 du Code de la santé publique détaille en 14 points les clauses que doit prévoir, au minimum, le contrat d'hébergement (indication des lieux d'hébergement, mesures mises en œuvre pour garantir le respect des droits des personnes concernées par les données de santé, indicateurs de qualité et de performance permettant la vérification du niveau de service annoncé, le niveau garanti, la périodicité de leur mesure, ainsi que l'existence ou l'absence de pénalités applicables au non-respect de ceux-ci ; garanties et procédures mises en place par l'hébergeur permettant de couvrir toute défaillance éventuelle de sa part ; etc.).

1 Association Française des Correspondants à la protection des Données à caractère Personnel

2 Conformément à l'article 29 de l'ordonnance n° 2018-1125 du 12 décembre 2018, ces dispositions entrent en vigueur en même temps que le décret modifiant le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction résultant de l'ordonnance précitée, et au plus tard le 1er juin 2019.

3 Nous renvoyons le lecteur intéressé par la notion d' « activité d'hébergement de données de santé à caractère personnel sur support numérique » aux article R. 1111-8-8 et R. 1111-9 du Code de la santé publique.

RGPD et contrats des fournisseurs IT Santé : peut mieux faire ?

> « Si nombre de prestataires n'avaient pas pour habitude de détailler dans le contrat le respect des règles de base d'hygiène informatique ou des principes de privacy by design, on aurait pu penser que le RGPD avait mis fin à ces pratiques »

Un RGPD contourné et mal interprété ?

Si nombre de prestataires n'avaient pas pour habitude de détailler dans le contrat le respect des règles de base d'hygiène informatique ou des principes de privacy by design, on aurait pu penser que le RGPD avait mis fin à ces pratiques et que, désormais, la prise de conscience des prestataires (et les fortes sanctions du texte s'appliquant aussi à eux dans certaines conditions) allaient amener le couple établissements de santé / fournisseurs de solutions IT à envisager ensemble une vie meilleure.

Plusieurs exemples auxquels nous avons pu être confrontés en pratique démontrent que, malheureusement, certaines réticences existent toujours et que la situation est encore loin d'être idyllique :

• Tout d'abord, que ce soit pour les fournisseurs de matériels avec logiciels embarqués ou pour les développeurs de solutions logicielles, il est parfois encore difficile de leur faire comprendre l'importance cruciale des engagements contractuels liés à la sécurisation de leurs produits à partir du moment où ceux-ci ne traitent pas de données à caractère personnel (et donc ne sont pas soumis au RGPD). Pourtant, un développement logiciel spécifique servant de brique à une solution de traitement des données des patients sera tout simplement nocif pour la sécurité ainsi que pour la conformité RGPD de l'ensemble du traitement de l'établissement s'il n'a pas été conçu « security / privacy by design ». **Qu'importe pour l'établissement de santé que le prestataire ne traite pas lui-même des données personnelles, le fait est que, dans cette hypothèse, ce sont les produits du sous-traitant qui servent de briques de base à sa propre conformité. Il faut donc prévoir – et imposer – contractuellement les clauses strictes qui en découlent !**

• On aurait pu croire que l'article 28 du RGPD était très détaillé et encadrait parfaitement le sujet, donnant naissance à la rédaction de clauses très détaillées avoisinant de façon habituelle la dizaine de pages. **La pratique démontre pourtant que si les sous-traitants proposent des clauses contractuelles respectant de plus en plus les textes, ils jouent aussi sur les silences dudit article** : ils profitent ainsi de la préexistence dans un grand nombre de contrats de limitations strictes de la responsabilité financière du prestataire pour l'appliquer aux manquements en matière de protection des données… La chose est d'autant plus aisée que ce type de clause étant rédigé de façon générale, il suffit de ne pas prévoir d'exclusion en la matière pour que la clause s'applique aussi à cette situation. Par ailleurs, ces clauses de limitation de responsabilité se trouvent souvent à plusieurs articles de distance dans le contrat, ce qui impose non seulement d'avoir une vision transversale du contrat pour permettre une négociation efficace, mais également de prévoir un accompagnement pendant toute la phase de négociation et jusqu'à sa conclusion (afin d'éviter que cette question ne soit sacrifiée in fine sur l'autel d'une signature rapide sans en avoir pesé les impacts) ;

• Même si l'esprit du texte est foulé aux pieds, limiter sa responsabilité en la matière est une pratique qui n'est interdite ni par le droit administratif, ni même par l'article 1111-11 précité concernant les contrats des hébergeurs de données de santé. Si le principe d'une limitation peut s'entendre, un montant de quelques milliers, voire dizaines de milliers d'euros au maximum, comme on le retrouve souvent, peut sembler choquant au vu de l'importance pour l'établissement de santé des obligations en matière de sécurité des données. L'existence de telles limitations, souvent éloignées du discours commercial, conduit surtout à diminuer fortement la confiance que les établissements de santé peuvent avoir dans les engagements du prestataire ;

• On aurait pu croire également que, depuis que le texte du règlement a été définitivement adopté (27 avril 2016), ses principes auraient été compris et mis en œuvre par l'ensemble des personnes amenées à le faire appliquer. Toutefois, trop souvent les qualifications de « responsable de traitement », de « sous-traitant » ou de « responsables conjoints » sont plaquées artificiellement dans un contrat, sans analyse réelle des flux de données et des opérations effectuées. La vague d'envoi « d'avenants de sous-traitance» par les entreprises responsables de traitement à l'orée du 25 mai 2018, indépendamment du rôle exact du partenaire amené à traiter des données personnelles, en a été un parfait exemple, reléguant la « conformité RGPD » à la simple validation formelle d'une liste de mesures à adopter, idéalement effectuée le plus vite possible .
Autre exemple, plus récent et beaucoup plus préoccupant à notre sens, montrant que la qualification des acteurs au sens du RGPD, pourtant essentielle, n'est pas claire, même pour ceux qui sont censés évangéliser : ainsi, en matière de marchés publics, la direction des affaires juridiques du ministère de l'Economie et des Finances a publié le 25 octobre 2018 une fiche technique sur « l'impact du RGPD sur le droit de la commande publique ». **Or, dans cette note de trois pages traduisant la terminologie du RGPD « en vocable marchés publics », ou encore traitant de « L'impact du RGPD sur les marchés publics en cours d'exécution et ceux à conclure», à aucun moment n'est évoqué le cas où le titulaire du marché public serait responsable conjoint avec l'acheteur**. Ainsi, dans le paragraphe sur la « termi-

RGPD et contrats des fournisseurs IT Santé : peut mieux faire ?

nologie du RGPD traduite en vocable marchés publics », la fiche ne prévoit qu'un seul responsable de traitement au sens du RGPD : l'entité cliente. On ne peut que déplorer la nécessité d'une future mise à jour de la fiche pour prendre en compte la réalité des situations, beaucoup plus complexe, même dans le cas d'un marché de commande publique. En effet, comment faire rentrer dans le schéma décrit par cette fiche une prestation du type de celle qui serait offerte par une plateforme de réservation de rendez-vous avec les patients qui utiliserait la plateforme préexistante du titulaire du marché (qui est donc, par hypothèse, déjà responsable du traitement) ?

Ils vécurent heureux et assurèrent de concert la SSI des établissements de santé ?

Le constat est malheureusement clair : en matière de sécurité des SI des établissements de santé et au-delà de la sensibilisation des personnels internes, il reste encore du travail à faire au plan contractuel pour s'assurer du niveau de sécurisation apporté par les prestataires et co-contractants. Certes, les progrès sont tangibles, mais les mauvaises habitudes ont la vie dure !

Et pourtant, la sécurité des développements informatiques, des prestations effectuées ou encore de l'hébergement des données est la pierre angulaire d'une approche privacy by design et donc la base d'une conformité RGPD des établissements de santé. Sécurisation et conformité qu'il conviendra de démontrer, le jour venu, aux régulateurs ou aux personnes concernées. La bataille sur les contrats, qui permettent d'encadrer le niveau de sécurisation et de sanctionner les manquements, n'est plus perdue d'avance mais, pour certains, elle ne fait que commencer…

> « Trop souvent, les qualifications de « responsable de traitement », de « sous-traitant » ou de « responsables conjoints » sont plaquées artificiellement dans un contrat, sans analyse réelle des flux de données et des opérations effectuées »

DPO : quel positionnement, quel périmètre

Le RGPD impose aux établissements de santé la nomination d'un DPO[1]. Qu'il soit mutualisé, interne ou externe, la question du positionnement et du périmètre de ce DPO dans les établissements de santé mérite la plus grande attention.

Diplômé de l'IMT Lille-Douai en 2000, **Fabien Dachicourt** rejoint la même année Pictime Groupe. Aujourd'hui Directeur Normes et Certifications, il a mené avec succès la demande d'agrément pour l'hébergement de données de santé pour la division Coreye ainsi que la certification ISO 27001.
DPO pour Pictime Groupe, Fabien intervient également sur tous les aspects réglementaires pour l'ensemble des activités du groupe.

Pour couvrir correctement son périmètre, il n'est pas indispensable que le Data Protection Officer (DPO) soit un juriste. Cependant, des connaissances de base en droit, la compréhension des opérations de traitement, des technologies de l'information et de la sécurité des données semblent nécessaires.

Promouvoir la protection des données au sein de l'établissement et ses bénéfices sont des points essentiels. Le DPO doit bénéficier du soutien actif de la direction générale et surtout disposer du temps suffisant pour remplir ses fonctions. Il doit être connu de tous et il doit avoir accès à tous les services (DIM, biomédical, recherche, SI, RH, juridique, etc.) afin de recueillir les informations essentielles dont il a besoin. En effet, le DPO doit être associé à toutes les questions relatives à la protection des données à caractère personnel (et pas uniquement les données de santé des patients). Il a aussi dans son périmètre la relation avec les personnes concernées (majoritairement les patients et le personnel).

Des missions larges et variées

Ses missions consistent à :

- informer et conseiller sur les obligations du RGPD et des autres dispositions du droit en matière de protection des données
- contrôler le respect du RGPD
- dispenser des conseils sur l'analyse d'impact
- coopérer avec l'autorité de contrôle et être son point de contact.

Dans la réalité, selon la taille de l'établissement, il va aussi rassembler et maintenir à jour la documentation et les preuves, tenir le registre des activités de traitement, s'assurer des engagements contractuels de ses sous-traitants sur la protection des données, notifier les violations de données personnelles à la CNIL, s'assurer de la communication aux personnes concernées, et enfin réaliser et vérifier l'exécution des analyses d'impact.

Le périmètre étant assez large, s'il exerce dans un établissement de taille importante, le DPO va devoir s'appuyer sur des Relais Informatiques et Libertés afin de collecter et transmettre les informations pertinentes au personnel.

Liberté organisationnelle et décisionnelle

L'indépendance professionnelle du DPO (article 38 §3 du RGPD) s'oppose à ce qu'il puisse être dirigé sur la manière de traiter une question dans l'accomplissement de ses missions. Il n'a aucun compte à rendre à un supérieur hiérarchique et il dispose d'une liberté organisationnelle et décisionnelle dans le cadre de sa mission. Pour autant, il n'agit pas seul et sans concertation puisqu'il peut consulter la CNIL ou tout autre sachant.

Enfin, le DPO fait directement son rapport au niveau le plus élevé de la direction du responsable du traitement tant et si bien que, si le responsable du traitement prend des décisions incompatibles avec le RGPD et les conseils du DPO, ce dernier doit avoir la possibilité de rendre une opinion dissidente directement au niveau le plus élevé de la direction. Notez que le DPO n'est pas personnellement responsable.

> « Le DPO va devoir s'appuyer sur des Relais Informatiques et Libertés afin de collecter et transmettre les informations pertinentes au personnel »

Les risques de conflits d'intérêts

Le RGPD a pris en compte les risques de conflits d'intérêts (art. 38 § 6). Selon le G29[2], cela concerne les postes de cadres supérieurs ou de direction (comme le Directeur Général, le DAF, le médecin-chef, le directeur des affaires médicales, le

1 DPO : Data Protection Officer

2 Groupe de travail Article 29 sur la protection des données formé par l'ensemble des CNIL européennes

DPO : quel positionnement, quel périmètre

DRH, le DSI, etc.), mais aussi des rôles qui conduisent à la détermination des finalités et des moyens de traitements de données personnelles.

Selon la taille de la structure, il n'est pas rare que le DPO soit aussi le RSSI, avec un rattachement à la DSI. Dans ce cas, il y a un risque de conflit d'intérêts à étudier au cas par cas. Le G29 souligne : « L'absence de conflit d'intérêts est étroitement liée à l'obligation d'agir en toute indépendance ». Le positionnement du DPO est donc une affaire subtile. Un rattachement à un secrétariat général ou à un département juridique sont des pistes à étudier.

En conclusion, le positionnement et le périmètre d'actions du DPO doivent s'inscrire dans la démarche globale de gestion des risques portée par l'établissement pour améliorer la qualité et la sécurité des soins, et tout particulièrement dans le cadre de la gestion des risques de sécurité du système d'information de l'établissement.

> « Le DPO doit être associé à toutes les questions relatives à la protection des données à caractère personnel, reporter au plus haut niveau sans être en conflits d'intérêt »

Le point de vue d'un chargé de mission en ARS

Le secteur de la santé était plutôt bien préparé à l'arrivée du RGPD, en raison de la sensibilité particulière des données qui y sont traitées et de la richesse du cadre réglementaire pré existant. Si l'on estime que ce texte correspond à 80% de la loi précédente, l'effort nécessaire à la mise en conformité n'est pas si énorme… à moins de n'avoir pas été conforme à la législation en vigueur !

Guy Marty, Docteur en informatique, est chargé de mission systèmes d'information de santé de l'ARS Occitanie, une fonction qu'il exerce depuis 2003 au fil de la transformation de l'ancienne ARH, puis ARS Midi-Pyrénées. Chargé du suivi des SIH, il a instruit les dossiers de financement du programme Hôpital numérique pour la région. Il est aussi responsable des problématiques transverses telles que la sécurité des SI de santé et les programmes nationaux d'échange et de partage (DMP et MSSanté). Ses débuts dans les SI en santé remontrent à 1995 : ingénieur normalisation au GIE Sesam-Vitale, il représentait la France dans les instances internationales de normalisation CEN et ISO.

La première fois que je me suis intéressé au RGPD, c'était par hasard, à l'automne 2016, alerté par un prestataire : « *Cette législation est énorme. Qu'allez-vous faire pour les établissements de santé* ? *Ils risquent d'être en grande difficulté* ? ». Je me suis renseigné, j'ai lu, observé et écouté pour déterminer quelles actions mener et conseiller aux établissements. A l'automne 2017, quand le sujet est devenu d'actualité, j'étais prêt à construire un discours qui dédramatise cette évolution réglementaire.

Cet article est un format rédigé du diaporama sur le RGPD que je présente, depuis le printemps 2018, aux acteurs de santé de la région Occitanie, en général des établissements de santé, des non spécialistes de la SSI. L'Occitanie compte plus de 300 établissements de santé d'une grande disparité de dimensions, où travaillent de moins de 10 à plus de 10 000 personnes. Cette présentation est donc généraliste ; elle sert aussi d'introduction à la présentation des actions nationales en matière de SSI dans la santé.

> « Quand on se regarde, on se désole, quand on se compare, on se console »

Moins compliqué qu'on ne l'entend dire

Ne pas s'affoler! C'est ce qu'expriment les représentants de la CNIL à propos du RGPD**.** Personne ne sera conforme à 100% **:** il ne faut ne pas céder aux sirènes de la conformité « clef en main »[1].

L'objectif de la CNILn'est pas la sanction, mais la conformité. C'est un processus opérationnel d'amélioration continue, il sera essentiel pour prouver votre bonne foi en cas de problème.

Le RGDP correspond à 80% de la loi précédente. Autrement dit, si l'effort pour vous mettre en conformité est trop important, c'est que vous n'étiez pas conforme à la législation en vigueur !

Il existe beaucoup de ressources disponibles en ligne, préparées par la CNIL ou sectorielles (ASIP Santé).
L'écosystème du numérique à Toulouse est très actif. J'ai ainsi pu entendre beaucoup d'acteurs, partager les expériences sur la sécurité des SI et le RGPD en dehors du secteur de la santé.

Un régime de déclaration

Premier constat : le secteur de la santé, malgré ses données sensibles (selon la définition du RGPD), était plutôt mieux préparé que d'autres secteurs économiques.
Un des principes du RGPD est la licéité du traitement et la législation sur les données de santé est riche : consentement, collecte, conservation ; il n'y a pas besoin de définir de règles des traitements des données de santé. Par exemple, le droit à l'oubli est défini par la durée légale de conservation du dossier médical.

Les données de santé passent d'un régime d'autorisation à un régime de déclaration : révisez les demandes d'autorisation et utilisez-les comme éléments du registre des traitements.
Il existe des outils nationaux et régionaux pour l'échange et le partage sécurisé de données de santé. Utilisez-les, ils contribueront à votre conformité pour ces actions. « Hackez » ces outils, inventez des usages complémentaires : le DMP peut servir de voie retour pour la communication électronique sécurisée avec les patients.

Certains reprochent au secteur de la santé d'être fortement administré. Pour la conformité au RGPD, l'existence de lois, d'une PSSI, de plusieurs circulaires et instructions est plutôt une chance, et beaucoup aimeraient avoir été guidés ainsi (cf le tableau).

1 https://www.CNIL.fr/fr/pratiques-abusives-mise-en-conformite-RGPD-CNIL-DGCCRF

Le point de vue d'un chargé de mission en ARS

Texte réglementaire	Acteurs de santé concernés
Prérequis Hôpital Numérique (2012, IFAQ depuis 2015)	Établissements de santé, production de soins
Arrêté du 1er octobre 2015 portant approbation de la PSSI pour les ministères chargés des affaires sociales	Ministère, ARS, établissements placés sous leurs tutelles et contractants
Instruction N°SG/DSSIS/2016/309 du 14 octobre 2016 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information (« Plan d'action SSI ») dans les établissements et services concernés	Établissements de santé Laboratoires de biologie médicale Centres de radiothérapie Centres d'imagerie et de radiologie
Instruction N° SG/HFDS/DGCS/2017/219 du 4 juillet 2017 relative aux mesures de sécurisation dans les établissements et services sociaux et médico-sociaux	Établissements et services sociaux et médico-sociaux
Cybersécurité – Mémento à l'usage du directeur d'établissement de santé – Connaître vos risques pour mieux y faire face – édition 2017[2]	Établissements de santé
Article L. 1111-8-2 du code de la santé publique[3] (« Signalement ») décrets et arrêtés associés[4]	Établissements de santé dont hôpitaux des armées Laboratoires de biologie médicale Centres de radiothérapie
Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (« Loi NIS »), décret et arrêtés associés	Prestataires fournissant un service d'aide médicale d'urgence : Réception et régulation des appels, Service mobile d'urgence et réanimation Grossistes répartiteurs pharmaceutiques : distribution pharmaceutique

Toutes les données nominatives sont concernées

Pour le secteur de la santé, le RGPD n'est pas un début mais une continuation. Il peut être vu comme une extension de la SSI : c'est un projet de la direction. Dans un établissement de santé ou médico-social, il n'y a pas que des données de santé. Avec le RGPD, toutes les données nominatives sont concernées, même les identités professionnelles de vos correspondants. Vous avez plusieurs années de bonnes pratiques pour les données de santé, appliquez-les à toutes les autres données.

Pour cela, je propose une mappemonde des données personnelles dans un établissement de santé, composée de continents de finalités, avec des territoires de catégories de données.

On retrouve le grand continent monolithique des soins et le continent éclaté des ressources humaines avec ses données sensibles (instances représentatives du personnel…) normalement déjà défrichés et balisés.

Il existe des continents qui étaient moins sensibilisés à la protection des données personnelles, car essentiellement consacrés à des données professionnelles comme les partenaires extérieurs (prestataires, administrations), la communication ou les instances dirigeantes.

Il faut aussi prendre garde au continent « froid » souvent oublié des traces informatiques qui peut contenir beaucoup de données sensibles.

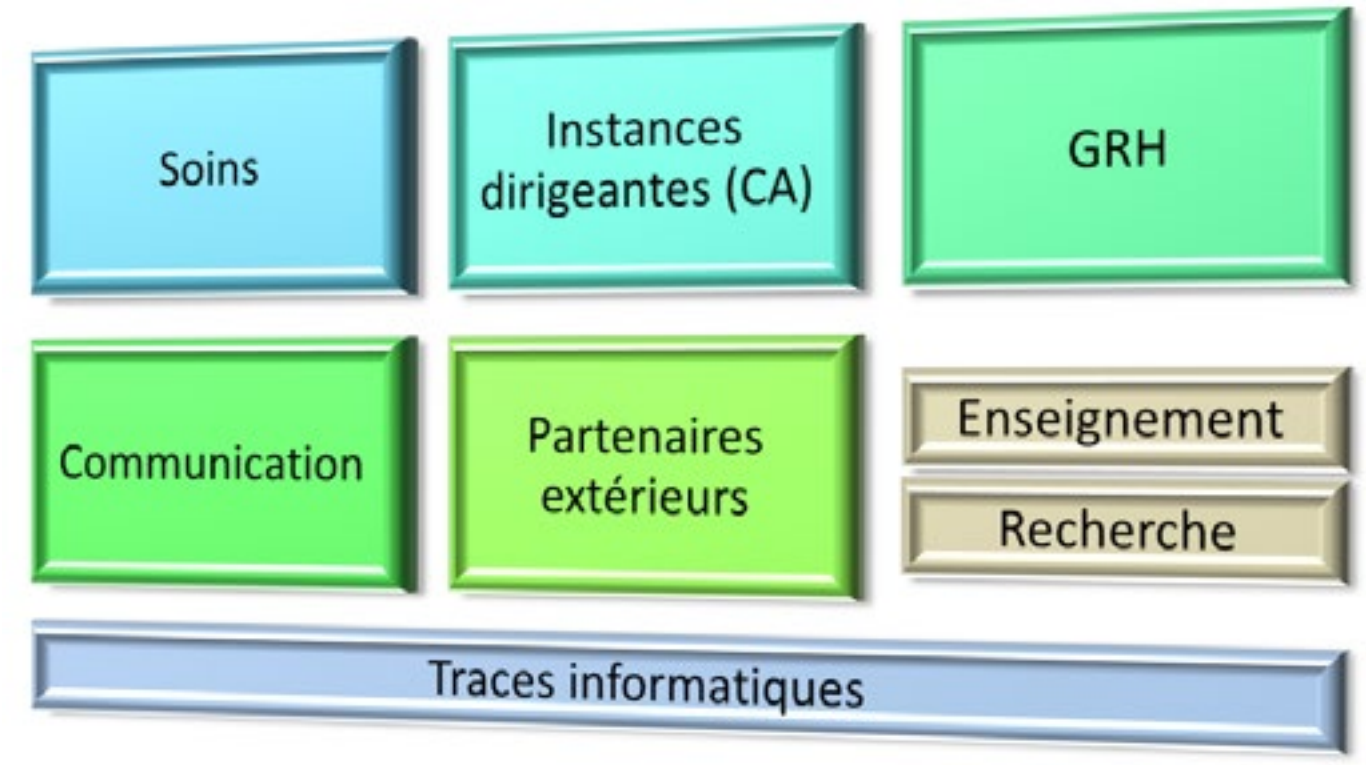
Enfin, les continents de l'enseignement et de la recherche que l'on rencontre moins fréquemment dans les établissements de santé mais très importants pour ceux qui sont concernés.

2 https://solidarites-sante.gouv.fr/IMG/pdf/dgos_memento_ssi_131117.pdf

3 Ne pas oublier de déclarer à la CNIL quand il y a atteinte aux données de santé à caractère personnel

4 https://signalement.social-sante.gouv.fr

Le point de vue d'un chargé de mission en ARS



Retour d'expérience

J'ai instruit les dossiers du programme Hôpital numérique de la région Occitanie, participé aux inspections et contrôles, et j'en ai tiré quelques enseignements.

La confidentialité doit être expliquée et appliquée à tous les prestataires, même s'il n'y a pas d'accès au SI[5]. La confidentialité est le quotidien des professionnels d'un établissement de santé. Mais ce qui est naturel pour eux[6] - ne pas parler à l'extérieur de ce qui a été vu à l'intérieur - ne l'est pas pour un artisan qui vient repeindre les couloirs[7].

Trop souvent, les dossiers de demande de financement Hôpital numérique contenaient des documents rédigés spécialement pour chaque indicateur. Alors qu'il vaudrait mieux utiliser ces obligations pour être conforme au RGPD et au plan d'action SSI.

Les prérequis Hôpital numérique imposent d'établir une cartographie applicative de tout le SIH par fonctionnalités et de maintenir à jour un fichier structure avec révision annuelle. Des indicateurs des domaines fonctionnels prioritaires exigent un taux de déploiement par service. En croisant ces obligations (pour chaque service, connaître les fonctionnalités déployées), on obtient un premier niveau d'habilitation : une personne n'a accès qu'aux applications déployées dans les services où elle travaille. La révision annuelle du fichier structure ainsi construit conduit forcément à la révision annuelle des habilitations.

5 Les indicateurs Hôpital numérique limitaient la confidentialité aux données de santé à caractère personnel.

6 Néanmoins, il arrive que la tentation soit trop forte : https://www.ouest-france.fr/bretagne/saint-brieuc-22000/saint-brieuc-le-secret-medical-mis-mal-l-hopital-yves-le-foll-4701457

7 J'en ai croisé régulièrement lors de mes visites aux établissements de santé.

Comment faciliter la mise en œuvre du RGPD dans les laboratoires de biologie médicale

La Société française d'informatique de laboratoire a décidé, en accord avec la CNIL, de produire un code de conduite. Etat des lieux des travaux en cours.

Bruno Gauthier, biologiste à Poitiers dans la SELAS BIO86, est trésorier de la Société française d'informatique de laboratoire (SFIL), président d'Armoris (fédération de biologistes) et vice-président du SDB (Syndicat des biologistes). Il coordonne, depuis Juin 2017, le groupe de travail sur la mise en œuvre du RGPD.

La loi 2016-41 de modernisation de notre santé du 26 Janvier 2016 a modifié le régime d'échange et de partage des données en l'étendant sous certaines conditions à d'autres professionnels, lorsque ceux-ci participent à la prise en charge du patient et que les informations transmises sont strictement nécessaires à la coordination ou à la continuité de soins, à la prévention ou au suivi médico-social et social. Cette même loi impose l'utilisation du cadre d'interopérabilité des systèmes d'information de santé (CI-SIS) pour toutes les transmissions de données de santé, et relance le DMP (Dossier médical qui passe de « personnel » à « partagé ») en confiant sa gestion à l'Assurance maladie. Elle change également les conditions pour être hébergeur de données de santé en substituant un processus de certification à l'agrément ministériel antérieurement requis. D'autre part, elle rend opposable la PGSSI-S.

Le décret 2016-46 relatif à la biologie médicale institue le compte rendu dématérialisé d'examen de biologie médicale, conformément au CI-SIS, en tant que document de référence.

Parallèlement à cette incitation à la dématérialisation et à l'échange ou au partage de données de santé, la pression réglementaire sur la protection des données s'accentue :

• Arrêté du 10 juin 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Produits de santé »,

• Décret 2016-1214 du 12 septembre 2016 relatif aux conditions selon lesquelles sont signalés les incidents graves de sécurité des systèmes d'information,

• Instruction N°SG/DSSIS/2016/309 du 14 octobre 2016 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information (« Plan d'action SSI ») dans les établissements et services concernés ; elle impose notamment la nomination d'un RSSI (responsable de la sécurité des systèmes d'information) dans les établissements de santé et les laboratoires de biologie médicale,

• Décret 2018-137 du 26 février 2018 définissant les modalités pour être hébergeur de données de santé,

• Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique

• Publication de la loi informatique et liberté modifiée et de son décret d'application le 3 août 2018 mettant en conformité le droit national avec le cadre juridique européen.

Au niveau européen, l'entrée en vigueur le 27 avril 2016 du règlement général sur la protection des données (RGPD), applicable le 25 mai 2018, renforce le droit des personnes et responsabilise les responsables de traitement.

> « L'objectif visé est qu'une conformité au code de conduite dispense le labotatoire d'être audité par le COFRAC sur son système d'information »

Focus sur les données à caractère personnel des patients

Les laboratoires de biologie médicale manipulent des données de santé à grande échelle et pour être conformes au RGPD, ils doivent désigner un délégué à la protection des données (DPO, *Data Protection Officer*), tenir un registre des traitements et mettre en œuvre une étude d'impact sur la vie privée (PIA, *Privacy Impact Assessment*).

C'est dans cet environnement très contraint (le défaut de PIA ou de DPO est passible d'une sanction s'élevant au montant le plus élevé entre la somme de 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial) que la Société française d'Informatique de Laboratoire (SFIL) a décidé, en accord avec la CNIL, d'élaborer un code de conduite appliqué à la biologie.

Dans ce code de conduite, la SFIL a pris l'option de faire un focus sur les données à caractère personnel des patients et d'exclure les données à caractère personnel des fonctions supports communes à l'ensemble des entreprises (Ressources Humaines, comptabilité ….).

Comment faciliter la mise en œuvre du RGPD dans les laboratoires de biologie médicale

Recenser les exigences réglementaires et normatives

En juin 2017, la SFIL a constitué un groupe de travail composé de biologistes du secteur privé et public, d'éditeurs de logiciels, de fournisseurs de DM-DIV[1], de représentants de la CNIL et de représentants de la SFIL. L'animation est assurée par la société Provadys, spécialisée en sécurité informatique, et le cabinet Lexing, spécialisé en droit du numérique.

Le premier travail de ce groupe a été de recenser de manière exhaustive les exigences réglementaires et normatives qui s'appliquent aux professionnels de santé et plus particulièrement aux laboratoires de biologie médicale. Dans un document de près de 200 pages, ces exigences ont été contextualisées et des recommandations de mise en œuvre ont été proposées en s'appuyant sur les différentes recommandations de bonnes pratiques proposées par la PGSSI, l'Anssi et la CNIL. Ce groupe de travail pragmatique a décliné les exigences spécifiques (réglementaires, ordinales, normatives) au contexte métier de manière opérationnelle pour l'ensemble des typologies de laboratoire. Cependant de nombreuses questions attendent des réponses de nos autorités de tutelles et de la CNIL (lire en encadré).

Contrôle et certification

Dans un deuxième temps, **nous allons produire un code de conduite associé à un modèle de PIA, permettant au laboratoire d'évaluer sa conformité et de générer un plan d'action.**
Pour être approuvé par la CNIL, ce code de conduite doit prévoir un mécanisme de contrôle. Les modalités de ce contrôle ne sont pas encore déterminées mais l'objectif visé est qu'une conformité au code de conduite dispense le labotatoire d'être audité par le COFRAC[2] sur son système d'information.

La mise en conformité au RGPD est importante. En effet, avec la révolution numérique, le monde est entré dans l'ère de l'échange et du partage de l'information, et la santé n'y échappe pas, d'autant qu'elle connait depuis peu une réelle volonté politique de favoriser ces développements. Les objectifs sont louables : optimisation et fluidification des parcours de soins, optimisation de la prise en charge du patient, réduction des coûts notamment en réduisant les redondances, développement de la médecine personnalisée et prédictive facilité par l'explosion des objets connectés permettant une médecine participative.
Mais le risque d'une utilisation détournée ou malveillante de ces données est proportionnel à l'augmentation des flux. Ce risque est d'autant plus important que les laboratoires et les établissements concentrent de plus en plus leur activité augmentant ainsi les surfaces d'attaques. La mise en œuvre du RGDP au sein des laboratoires est donc un formidable outil pour les accompagner dans leur révolution numérique en replaçant le patient, le secret professionnel et la confiance au cœur des préoccupations.

1 Dispositifs médicaux et dispositifs médicaux de diagnostic in vitro
2 Comité Français d'Accréditation

De nombreuses questions

• Dans le cadre de la télémaintenance, un fournisseur de DM-DIV et/ou de logiciel de laboratoire doit-il être considéré comme un hébergeur de données de santé s'il a accès à des données sensibles ?

• Un éditeur de SGL (système de gestion de laboratoire) qui propose une plateforme de dépannage à distance est-il soumis à la certification HDS à partir du moment où cette plateforme héberge des données de santé ?

• De la même manière, un laboratoire indépendant de l'établissement de santé avec lequel il travaille, recevant l'ensemble des mouvements des patients, doit-il être hébergeur de données de santé ?

• L'utilisation des fonds de tubes par un laboratoire sous-traitant pour son propre compte est-il soumis au recueil du consentement des patients ?

• Un laboratoire exploitant ces fonds de tubes pour valider ses méthodes est-il soumis à la règlementation sur la recherche ?

Ce qu'il faut savoir à propos du Privacy Impact Assessment

Document central, à dérouler pour chaque traitement sensible, le PIA (Privacy Impact Assessment) comprend en annexe l'appréciation des risques. Il correspond à une forme d'homologation et s'articule autour de quatre thèmes. Explications.

Cédric Cartau, RSSI et DPO du CHU de Nantes et du GHT44, est également chargé de cours à l'EHESP et à l'ESIEA. Il collabore régulièrement à la revue DSIH et a publié plusieurs ouvrages, notamment « La sécurité du système d'information des établissements de santé », seconde édition (Eyrolles, 2017).

Le RGPD introduit un changement majeur de paradigme dans la protection des traitements de données personnelles, puisque l'on passe d'une logique administrative à une approche par le risque, et surtout à une inversion de la charge de la preuve : il appartenait à la CNIL de démontrer qu'un traitement était non conforme, alors qu'avec le RGPD il appartient au responsable de traitement de démontrer qu'il a correctement évalué les risques et pris les bonnes mesures. Pour autant, la mise en conformité s'articule autour de plusieurs axes majeurs, dont le PIA.

1 Le fond

Sans rentrer dans les détails de toute la mise en conformité, l'ensemble de la démarche se décline en plusieurs axes : le socle commun, le volet contractuel, le PIA. Dans le socle commun, on trouve les mentions d'affichage, le recueil du consentement, les processus de signalement des incidents et de réponses aux demandes d'accès, etc. Le volet contractuel concerne la modification par avenant des marchés pour la prise en compte des spécificités du RGPD, notamment la répartition des responsabilités entre le client et le fournisseur dans les traitements mis en œuvre. Le PIA est le document central, à dérouler pour chaque traitement sensible, et qui comprend en annexe l'appréciation des risques.

Le PIA est une forme d'homologation, qui peut se résumer en une phrase : il n'est pas possible de mettre en œuvre un traitement sensible sans se poser un minimum de questions et faire acter par l'institution des risques que l'on fait encourir aux personnes dont on traite les données, des mesures que l'on a prises pour réduire ces risques, et des risques résiduels acceptés. Dans l'esprit, le RGS, qui s'applique aux téléservices, procède de la même logique, à savoir l'homologation préalable à toute mise en production, homologation articulée autour de l'appréciation des risques. Un PIA est articulé autour de quatre thèmes :

- la description des caractéristiques du traitement: description du traitement, identification du responsable de traitement, de la typologie de données traitées, des destinataires des données, etc.
- la description des principes fondamentaux: information des personnes, recueil du consentement, légitimité du traitement, etc.
- les mesures de protection en place : chiffrement, sauvegardes, etc.
- l'appréciation des risques formalisée.

Le PIA devrait être signé par le DPO (qui émet un avis non suspensif) mais aussi et surtout par le responsable de traitement, qui valide les mesures de protection mises en place et l'appréciation des risques formalisée.

> « Le PIA et l'analyse des risques sont réalisés par le responsable de traitement »

2 La forme

La CNIL fournit des modèles très complets sur son site, et la plupart des prestataires de services vous proposeront aussi des modèles qui rassemblent plus ou moins les mêmes items. Malheureusement, ces modèles ont souvent le même travers, à savoir la répétition ad nauseam, à la fin de chaque chapitre ou paragraphe, des éléments traités dans ledit chapitre. Par exemple, dans le modèle de la CNIL, on trouve une synthèse de tout ce qui a été traité plus haut dans le document : la recopie étant source d'erreur et rendant un document non maintenable dans le temps, on se demande bien pourquoi perdre son temps à cela. D'autant qu'en cas de contrôle de la CNIL, le document contient les informations exigibles.

De la même manière, mettre un tableau d'analyse de risques dans un document Word est, selon nous, fortement déconseillé. Un tableau, cela se saisit dans un tableur, qui devient ainsi une annexe du PIA.

Dernier détail : ce n'est pas le DPO qui réalise le PIA. L'article 35 du RGPD stipule que le PIA et l'analyse des risques sont réalisés par le responsable de traitement. Le DPO a un rôle de conseil et d'alerte, sa signature n'est pas requise stricto sensu, même s'il est fortement suggéré de prévoir cette étape dans le processus. Dans le cas, par exemple, où un responsable de traitement sous-estimerait volontairement les risques sans que le document soit visé par le DPO, et sans qu'il soit tenu compte de ses remarques, ce dernier aura cependant intérêt à consigner le fait que ses conseils n'ont pas été suivis.

ACSS : une réponse à la menace de cybersécurité dans le secteur santé

La cellule Accompagnement Cybersécurité des Structures de Santé (ou ACSS) correspond à un dispositif qui va au-delà du seul traitement des signalements d'incidents. Elle offre un véritable service d'appui, avec un accompagnement dans la phase post-incident d'amélioration des mesures de sécurité.

asipsanté L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

La cybercriminalité est aujourd'hui une menace prépondérante pour les structures de santé : cryptovirus, hameçonnage pouvant aboutir à des demandes de rançons, mais surtout à une indisponibilité d'une partie ou de tout le système d'information de l'établissement, avec un risque de mise en danger réel du parcours de soins des patients.

Face à ces risques, il était important de proposer un accompagnement et un appui aux structures de santé dans la gestion des actes de cybermalveillance et de mettre en place une cellule dédiée.

La cellule Accompagnement Cybersécurité des Structures de Santé (ACSS) a été créée en application de l'article L. 1111-8-2 du Code de la santé publique. La déclaration des incidents pour les établissements de santé, les hôpitaux des armées, les centres de radiothérapie et les laboratoires de biologie médicale devient obligatoire. Le ministère des Solidarités et de la Santé a mis en place un dispositif qui va au-delà du seul traitement des signalements pour répondre aux nouveaux enjeux liés à la menace de cybersécurité pesant sur les acteurs de santé.

> « Le signalement des incidents de sécurité des systèmes d'information des structures de santé est obligatoire depuis le 1er octobre 2017 »

Un dispositif autour de trois grandes missions

1. Le traitement des signalements des incidents SI permet de renforcer le suivi des incidents des structures concernées au sein du secteur santé ;
2. La veille sur l'actualité de la sécurité des SI et sur les menaces propres au secteur de la santé consiste à alerter et informer l'ensemble des acteurs de la sphère santé dans le cas d'une menace pouvant avoir un impact sur le secteur ;
3. L'animation de la communauté invite à partager des bonnes pratiques concernant les actions de prévention ainsi que les réponses à apporter aux incidents, afin de réduire les impacts et de mieux protéger les systèmes.

Dans le cadre de ce dispositif, le ministère propose un véritable service d'appui. Sous sa responsabilité, la cellule ACSS se positionne comme partenaire et conseiller des structures de santé. Elle apporte ainsi son appui aux structures dans le cadre de la mise en place de mesures d'urgence en :

- orientant vers un prestataire de proximité référencé par le GIP cybermalveillance.gouv.fr dans le cas d'une demande d'intervention sur site ;
- communicant une fiche réflexe (ex : phishing, cryptovirus, code malveillant ou défiguration de site Web) et des recommandations visant à confiner l'incident (ex : changements de mots de passe, mise en liste noire d'adresses de messagerie, blocage de protocoles, etc…).

La cellule ACSS propose aussi un accompagnement dans la phase post-incident d'amélioration des mesures de sécurité. Elle peut effectuer une évaluation technique des plans d'action sécurité et apporter des propositions d'amélioration de la sécurité du SI (par exemple, l'utilisation d'une application pour l'administration locale ou pour limiter l'exploitation de vulnérabilités). Elle est souvent amenée à faire connaitre les bonnes pratiques d'administration et de développement (ex : promotion des règles de l'ANSSI sur la configuration sécurisée d'un domaine Active Directory[1] ou la conception d'application web).

> « Un an après, ACSS a permis de remonter et traiter de nombreux incidents »

1 Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows.

ACSS : une réponse à la menace de cybersécurité dans le secteur santé

La messagerie électronique reste le vecteur le plus important de la menace de cybersécurité dans les structures de santé. Le manque de vigilance ou la méconnaissance des techniques d'attaque permettent à des pirates de récupérer des identifiants de comptes de messagerie ou de déployer des rançongiciels au sein des systèmes d'information des structures de santé. La mise en œuvre de ce type d'attaque a provoqué un grand nombre d'incidents au cours de l'été 2018. Ciblant particulièrement les structures de santé, les pirates ont exploité la compromission de comptes de messagerie de salariés de structures de santé, usurpant leur identité, pour attaquer d'autres structures de santé.

Au cours de cette première année d'activité, plus de 300 incidents dont 86% au sein des établissements de santé, ont été remontés au ministère et 41 demandes d'accompagnements ont été formulées. Les deux mois les plus significatifs en matière de cyber malveillance ont été juillet et août 2018, car de très nombreux établissements de santé ont été touchés par plusieurs campagnes d'hameçonnage menées à l'échelle nationale.

> « ACSS est un dispositif ancré dans un cercle de confiance dont les informations restent totalement confidentielles »

Préserver en confidentialité l'origine des signalements et des données relatives aux incidents est la garantie d'obtenir la confiance des déclarants dans le dispositif. Seuls le fonctionnaire de la sécurité des systèmes d'information(FSSI) et des personnels dûment habilités de l'ASIP Santé ont accès à l'ensemble des informations concernant les incidents. La cellule ACSS reçoit les informations, contacte la structure concernée pour qualifier l'incident et c'est seulement en cas de risque d'impacts sanitaire ou majeur que les informations sont transmises aux organismes dédiés.

> « L'échange et le partage de bonnes pratiques, la remontée des incidents permettent de prévenir les risques et de trouver les meilleures solutions dans les meilleurs délais. »

La cellule ACSS cherche à favoriser les échanges avec les structures de santé et ainsi créer un lien privilégié, non seulement dans le cadre du traitement des incidents, mais aussi plus globalement en vue de les aider à améliorer leur capacité à se protéger contre les menaces de cybersécurité.

Dans le cadre de la prévention des incidents, le portail cyberveille-santé, dédié à la sécurité numérique dans le secteur santé, joue un rôle central dans l'information des acteurs opérationnels de la sécurité : il publie quotidiennement des informations sur les vulnérabilités présentes au sein des systèmes d'information et diffuse régulièrement des alertes sur des menaces sectorielles.

ACSS : une réponse à la menace de cybersécurité dans le secteur santé

Pour en savoir plus

Le portail d'Accompagnement Cybersécurité des Structures de Santé : https://www.cyberveille-sante.gouv.fr/
Le portail de signalement des incidents de sécurité des systèmes d'information : https://signalement.social-sante.gouv.fr/

En proposant un espace sécurisé, le portail cyberveille-santé est le moyen privilégié pour échanger : il favorise la coopération et l'entraide entre les acteurs (ministère, ARS et structures de santé), afin de mieux faire connaitre les impacts des différentes menaces de cybersécurité à l'ensemble du secteur et permettre aux structures les plus vulnérables d'améliorer leur résilience aux incidents de sécurité.

La campagne portant sur les messages indésirables, durant l'été 2018, est un bon exemple de coopération entre les structures de santé et la cellule ACSS : plusieurs structures ont signalé les messages d'hameçonnage qu'elles recevaient et qui étaient émises par des structures dont certains comptes de messageries avaient été compromis. La cellule ACSS a informé l'ensemble des acteurs du secteur en publiant un bulletin d'alerte sur le site cyberveille-santé. Les structures « compromises » ont alors été informées des mesures de remédiation.

L'implication de l'ensemble des acteurs du secteur dans ce dispositif est essentielle : elle contribue à améliorer les actions d'accompagnement et de sensibilisation de la cellule ACSS. Les structures encore réticentes ne doivent plus hésiter à déclarer leurs incidents de sécurité. Il n'y a ni gêne, ni doute à émettre : les informations restent totalement confidentielles et ne serviront qu'à aider l'ensemble de la communauté.

L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

ACCOMPAGNEMENT CYBERSÉCURITÉ DES STRUCTURES DE SANTÉ (ACSS)

EN BREF

CRÉATION DE LA CELLULE ACCOMPAGNEMENT CYBERSÉCURITÉ DES STRUCTURES DE SANTÉ

C'EST UN DISPOSITIF DE PRÉVENTION, DE TRAITEMENT DES SIGNALEMENTS DES INCIDENTS DE SÉCURITÉ ET DE VEILLE SECTORIELLE AU PROFIT DES ACTEURS DE SANTÉ.

En application de l'article L. 1111-8-2 du code de la santé publique, les établissements de santé, les hôpitaux des armées, les centres de radiothérapie et les laboratoires de biologie médicale **doivent déclarer leurs incidents de sécurité des systèmes d'information depuis le 1er octobre 2017.**

LES 3 MISSIONS D'ACSS

1. **LE TRAITEMENT DES SIGNALEMENTS DES INCIDENTS SI**
2. **LA VEILLE SUR L'ACTUALITÉ** de la sécurité des SI et sur les menaces propres au secteur de la santé
3. **L'ANIMATION DE LA COMMUNAUTÉ** cyberveille-sante.gouv.fr

LES 6 CHIFFRES CLÉS

319 INCIDENTS DÉCLARÉS sur le portail des signalements

41 DEMANDES D'ACCOMPAGNEMENT

6 INCIDENTS SIGNIFICATIFS ont fait l'objet d'un suivi particulier de la part du FSSI

3 INCIDENTS ONT ÉTÉ PRIS EN CHARGE par l'Agence Nationale de la Sécurité des Système d'Information (ANSSI)

13 INCIDENTS ONT ÉTÉ COMMUNIQUÉS à l'Agence Nationale de la Sécurité du Médicament et des produits de santé (ANSM)

3 INCIDENTS AYANT EU UN IMPACT SANITAIRE

Contacter la cellule ACSS : cyberveille@sante.gouv.fr - Contacter le FSSI : ssi@sg.social.gouv.fr - Octobre 2018

0.5

0.5 PROCESSUS ET PROCÉDURES

L'appui et les solutions de l'ASIP Santé, **Alain Espinoux** P. 79 À 81
Connectivité et vulnérabilités, **Gérard Gaston** P. 82 & 83
Les cinq temps de la gestion des incidents SSI, **Cédric Cartau** P. 84 & 85
Outiller le processus de gestion des changements, **Stéphane Moneger** P. 86 & 87
L'enjeu de la gestion contractuelle dans l'atteinte de la conformité des SI en santé, **Pauline Berry et Isabelle Zablit** P. 88 & 89

PROCESSUS ET PROCÉDURES

L'appui et les solutions de l'ASIP Santé

Pour aider l'écosystème du secteur santé et médico-social dans la prise en compte de la sécurité des SI, l'ASIP Santé propose des dispositifs variés : publication de guides et référentiels, mise à disposition de produits et services pour identifier et authentifier les professionnels, accompagnement opérationnel et gestion de l'espace des messageries sécurisées de santé.

Alain Espinoux est directeur adjoint du Pôle Urbanisation et Services de Confiance, RSSI délégué et responsable de l'équipe SSI à l'ASIP Santé. L'activité SSI de l'ASIP Santé couvre d'une part la sécurité des systèmes d'information gérés par l'ASIP Santé (analyse de risques, tests d'intrusion, plan de continuité d'activité, …) et d'autre part l'élaboration de la PGSSI-S, le suivi des incidents de sécurité déclarés auprès de la cellule ACSS (voir page nn), les activités de cyberveille santé et de cybersurveillance dont bénéficient les acteurs de santé.

Le développement du numérique dans le secteur santé et médico-social s'accélère. Les professionnels utilisent désormais tous les jours les outils digitaux, notamment pour conserver les informations concernant les patients qu'ils prennent en charge. Ces systèmes sont de plus en plus communicants pour faciliter la coordination entre professionnels tout au long du parcours de santé du patient ; et l'usage de médias s'est diversifié : ordinateur PC, tablette, smartphone.

Nous sommes tous convaincus que le numérique améliore le quotidien des professionnels et des patients. Il favorise la qualité et la sécurité des soins et améliore l'efficience de notre système de santé. Cependant **les données de santé à caractère personnel sont très sensibles et nécessitent donc une forte protection**. Les risques sont multiples : incidents techniques, actes malveillants (*ransomware* par exemple) ou encore mésusages.

1 Une large palette de dispositifs

Pour aider l'écosystème du secteur santé et médico-social dans la prise en compte de cet enjeu, l'ASIP Santé propose des dispositifs variés : publication de guides et référentiels de sécurité, mise à disposition de produits et services utiles pour identifier et authentifier les professionnels, sans oublier une activité d'accompagnement en sécurité opérationnelle, et la gestion de l'espace des messageries sécurisées de santé.

1.1 La mise à disposition de guides et de référentiels de sécurité

La Politique générale de sécurité des systèmes d'information de santé (PGSSI-S) contient des référentiels et des guides destinés aux acteurs du secteur santé et médico-social pour les aider à protéger les données de santé des usagers.
Structurants pour le développement de la e-santé en toute confiance, les référentiels portent sur l'identification et l'authentification des acteurs de santé, ainsi que la force probante des documents de santé (qu'ils soient nativement numériques, dématérialisés ou rematérialisés).

1.2 La mise en place d'un processus de certification pour l'hébergement des données de santé

Compte tenu de la sensibilité des données de santé à caractère personnel, l'activité d'hébergement de ces données sur support numérique est encadrée. Soumise auparavant à une procédure d'agrément, elle nécessite désormais une évaluation de conformité à un référentiel de certification, délivrée par un organisme de certification accrédité par le COFRAC.

1.3 La publication des données d'identification des professionnels de santé, certifiées au niveau national

Les données d'identification des professionnels de santé inscrits dans les répertoires nationaux RPPS et ADELI sont publiées sur le portail https://annuaire.sante.fr et par web-services.
Ce répertoire permet à un établissement de santé de vérifier les identités et qualifications d'un professionnel de santé, de peupler son annuaire d'établissement avec les identifiants nationaux RPPS (ou ADELI) par exemple pour le suivi des prescriptions exécutées en ville, d'associer un numéro de carte CPS à un identifiant RPPS/ADELI pour faciliter l'enrôlement (SSO), ou d'obtenir les adresses des correspondants de ville.

1.4 La fourniture de dispositifs d'authentification, de signature et de chiffrement destinés aux acteurs de santé et médico-sociaux

L'ASIP Santé gère l'infrastructure de gestion de clés (IGC) dédiée au secteur santé et délivre à ce titre des certificats d'authentification, de signature et de chiffrement pour les professionnels et les structures de santé. Ces certificats sont fournis à l'état logiciel ou confinés dans les cartes de la famille CPS. L'ASIP Santé explore un dispositif d'authentification sur smartphone, le CPS wallet, associé, dans une première phase, à un enrôlement initial par carte CPS.

1.5 Des informations sur l'identifiant national de santé (INS)

La qualité de l'identification du patient repose sur sa bonne identification par le biais de procédures d'identito-vigilance

rigoureuses, et le bon référencement de ses données de santé en utilisant l'INS en tant qu'identifiant unique et pérenne à compter du 1er janvier 2020.
Le référentiel INS, mis en concertation en 2018, devrait être publié début 2019.

1.6 Un dispositif de déclaration et de suivi des incidents de sécurité et un service de cyberveille santé

Depuis octobre 2017, tous les établissements de santé, laboratoires de biologie médicale, centres de radiothérapie ont **l'obligation de signaler leurs incidents de sécurité de système d'information** via le portail signalement.social-sante.gouv.fr. Un suivi et un accompagnement sont assurés en toute confidentialité par la cellule accompagnement cybersécurité des structures de santé (ACSS).

Les **informations pratiques diffusées via le portail** https://www.cyberveille-sante.gouv.fr vous aident par ailleurs à vous prémunir des risques de sécurité des systèmes d'information : alertes de sécurité, bulletins de sécurité sur des technologies standards et dédiées au secteur santé, fiches réflexes apportant un appui dans la gestion des incidents. La communauté des correspondants cyberveille-santé dispose d'un espace de discussion favorisant ainsi partage et échange de bonnes pratiques.

1.7 Un service de cybersurveillance

Conçue initialement pour ses besoins internes, l'ASIP Santé a développé une **plateforme de cyber-surveillance**. Cet outil recherche et détecte de façon préventive les vulnérabilités sur les domaines exposés sur Internet des structures de santé. La plateforme permet la collecte, l'analyse et la restitution (sous forme de rapport automatisé) d'informations récupérées à partir de sources ouvertes et de techniques non intrusives.

1.8 Des modules de formation

La plateforme de formation https://esante-formation.fr met à disposition, en accès libre, des **modules de formation relatifs à la sécurité des systèmes d'information** : sur la sécurité et la robustesse des mots de passe, la gestion des courriels, la PGSSI-S, l'INS, l'hébergement des données de santé …

> « Le référentiel INS (Identifiant National de Santé), mis en concertation en 2018, devrait être publié début 2019 »

1.9 Un espace de confiance de messagerie sécurisée de santé (MSSanté)

L'espace de confiance des messageries sécurisées de santé permet aux professionnels d'échanger les données de santé de leurs patients en toute confiance.

2 Des enjeux nationaux dans une logique d'urbanisation sectorielle

La loi de modernisation de notre système de santé publiée en janvier 2016 a modifié les conditions d'échange et de partage des données de santé, dans le respect du secret professionnel, pour tenir compte de l'évolution des pratiques professionnelles nécessaires à la prise en charge du patient tout au long de son parcours de santé. Ceci a pour conséquence d'étendre les principes d'identification et d'authentification à tout professionnel concerné, qu'il exerce dans le secteur sanitaire ou médico-social, voire social.

Dans le contexte actuel caractérisé à la fois par la volonté de développement de la e-santé et des orientations prises pour accélérer le virage numérique dans la stratégie de transformation du système de santé (Ma Santé 2022), l'apparition de nouveaux usages (mobilité, terminaux partagés, objets connectés, …) et le renforcement de la règlementation (RGPD, eIDAS[1], force probante des documents de santé…), il apparaît nécessaire de mieux encadrer les pratiques par la définition d'une **stratégie globale d'identification et d'authentification des acteurs**.

Les objectifs en matière d'identification et d'authentification sont :

- d'attribuer à tous les acteurs impliqués une identité numérique ;
- de proposer des solutions d'authentification adaptées au contexte d'utilisation (poste de travail personnel ou partagé, dispositif mobile…) ;
- de garantir un niveau de sécurité en adéquation avec la sensibilité des données accédées.

La carte CPS constitue la solution historique principale pour l'authentification des acteurs de la sphère médico-sociale. Malgré ses qualités de sécurité jamais mises en défaut, elle présente certaines limites. Le support carte à puce génère des coûts de production, de maintenance et d'adoption (mise en œuvre d'un lecteur), et n'est pas adapté à un usage en mobilité.

Des solutions complémentaires ont été mises en place, aussi bien au niveau national que local, mais elles souffrent d'un manque d'homogénéité dans leurs usages et d'un coût relativement important, surtout lorsque l'on considère la redondance des investissements dans les différentes structures.
Il apparaît ainsi nécessaire de définir une nouvelle stratégie nationale pour rationaliser l'approche de l'identification et de l'authentification.

1 eIDAS, ou electronic IDentification, Authentication and trust Services est la première brique d'un socle commun en matière de confiance numérique entre les 28 pays de l'Union européenne, entrée en vigueur en septembre 2014. Pour en savoir plus : https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/

L’appui et les solutions de l’ASIP Santé

Pour pouvoir faire des choix pérennes, plusieurs points de doctrine doivent être tranchés au préalable :

- Quels niveaux de sécurité exiger pour l’identification et l’authentification selon les cas d’usage ?
- Quel positionnement adopter vis-à-vis du règlement eIDAS ?
- Quelle cohérence imposer entre solutions locales et nationales en matière d’authentification ?
- Quels choix réaliser en matière de logique économique ?

Ces choix d’identification et d’authentification sont des prérequis à **la mise en place du contrôle d’accès aux applications de santé, première brique indispensable à la protection de nos données de santé**. Le compromis trouvé entre le contrôle d’accès a priori et le contrôle a posteriori dépend des choix métier.

Les dispositifs de cybersurveillance permettent d’aller plus loin avec une analyse en profondeur du degré d’exposition des données de santé, pour faire face aux vulnérabilités qui évoluent tous les jours, et arriver à maintenir des systèmes d’information sécurisés dans le temps.

> « Le compromis entre le contrôle d’accès *a priori* aux applications de santé et le contrôle *a posteriori* dépend des choix métier »

Connectivité et vulnérabilités

Une bonne hygiène de son système d'information passe par une parfaite gestion des mises à jour de sécurité des systèmes d'exploitation et par la connaissance exhaustive de ses équipements, qui représentent autant de points d'entrée – et de vulnérabilité.

Gérard Gaston, de formation scientifique, est passionné par les nouvelles technologies et très impliqué, depuis 15 ans, dans la sécurité qui les entoure. Réserviste cyberdéfense depuis 2016, il a rejoint, la même année, LNA-Santé où il est Responsable de la sécurité des systèmes d'information et désormais Délégué à la protection des données. Il a, auparavant, exercé comme RSSI dans le milieu industriel pendant huit ans.

Après une décennie passée à sécuriser les systèmes d'information et à sensibiliser les utilisateurs, je souhaite partager avec vous mon regard sur la sécurité des établissements « connectés ». Nous sommes en 2018. Posséder un antivirus à jour sur l'ensemble de son parc informatique est devenu un standard et ce n'est plus un sujet pour un RSSI. Je sais que certains d'entre vous esquisseront un sourire en pensant à ce poste fourni par un prestataire et qui ne tolère toujours pas l'installation d'un antivirus en 2018. Je ne peux que vous conseiller de prendre vos dispositions pour isoler complètement cet équipement du reste de votre réseau informatique. Le fait est qu'en matière de sécurité, il est indispensable d'avoir un antivirus à jour, mais ce n'est pas une garantie suffisante. La correction des vulnérabilités est tout autant importante et encore trop souvent négligée.

Vulnérabilités par défaut de mise à jour

A mes débuts, j'ai eu l'occasion de côtoyer de très près le malware Conficker. Ce dernier se propageait à travers les réseaux à une vitesse impressionnante. C'est sûrement, de mémoire de RSSI, le ver qui a infecté le plus de machines dans les années 2000. Au moment où j'écris ces lignes, je n'ai pas été surpris d'apprendre qu'un établissement de santé avait récemment trouvé des traces de ce ver sur son réseau. Ce malware exploitait une vulnérabilité du système d'exploitation corrigée peu de temps avant par l'éditeur. Oui, mais voilà, fallait-il encore avoir déployé correctement les mises à jour sur son parc informatique !

A l'époque, Conficker engorgeait les réseaux, ce qui était déjà très problématique, mais sans détruire la donnée présente sur le poste infecté. D'ailleurs, le plus souvent, les petites structures équipées de peu de postes ne se rendaient même pas compte qu'elles étaient infectées. Il aura, cependant, fallu plusieurs mois, pour ne pas dire années, dans les grands groupes pour totalement s'en débarrasser.

Il y a maintenant un an, débarquait un ransomware du nom de Wannacry. Ce dernier a infecté beaucoup moins de postes que Conficker mais il a causé des dégâts beaucoup plus visibles, ce qui lui a valu d'être largement connu. Mon constat est qu'une fois de plus le non-déploiement d'une mise à jour de sécurité, publiée elle aussi quelques mois plus tôt, est à l'origine du problème. La propagation de ce malware a aussi été facilitée par la présence en (encore) trop grand nombre dans les entreprises de systèmes d'exploitation qui ne sont plus supportés par l'éditeur et qui ne bénéficient plus des correctifs de vulnérabilités. Quand je parle de Windows NT ou de Windows 98, la plupart me répondront en souriant « Quoi ! On en trouve encore !? ». Mais si je parle de Windows 2003 et de Windows XP, c'est une toute autre histoire : on commence le plus souvent à m'expliquer que c'est à cause d'un constructeur, d'un éditeur… Une décennie s'est écoulée entre ces deux attaques, mais ce sont bien les mêmes causes qui ont permis à ces deux malwares de faire leur renommée.

> « Un site comme Shodan référence l'ensemble des équipements connectés visibles sur Internet et il y a vraiment de quoi attraper le vertige quand on y lance une recherche »

Les équipements auxquels on ne pense pas

Et là, je vous parle uniquement des vulnérabilités sur un système d'exploitation très répandu. Qu'en est-il des routeurs, des pare feux, des GTB (Gestion Technique de Bâtiment)… ou encore de la machine à café (les derniers modèles nécessitent une connexion à Internet pour valider le solde de votre carte) ? Tous ces équipements embarquent des mini-systèmes d'exploitation et, avec eux, leurs lots de vulnérabilités, qu'il sera nécessaire de corriger au fil des diffusions des alertes.

Et puis, il y a tous ces équipements auxquels on ne pense pas toujours et qui nécessitent, eux aussi, une connexion sur le réseau de l'établissement, le plus souvent pour permettre le pilotage d'un appareil distant. Dernière-

ment, un casino en a fait les frais : l'attaquant s'est introduit dans le réseau informatique en passant par le thermomètre connecté de l'aquarium ce qui, par rebond, lui a permis d'accéder au système d'information. Nous n'en sommes qu'au début de l'ère du « tout connecté », la multiplication de tels équipements va aller croissant et malheureusement pour le RSSI, il ne sera pas toujours possible de refuser leur déploiement.

Des proies faciles

Un site comme Shodan (*www.shodan.io)* référence l'ensemble des équipements connectés visibles sur Internet et il y a vraiment de quoi attraper le vertige quand on y lance une recherche. Tous ces équipements sont autant de points d'entrée dans les structures. Il faut se rendre à l'évidence qu'avec de tels outils, un routeur dont la faille de sécurité n'est pas rapidement corrigée devient alors une proie facile pour l'attaquant.

N'imaginez pas non plus que, parce que votre système d'information n'a que peu d'équipements visibles sur Internet, vous serez moins sujet aux attaques. Le plus souvent, ces dernières sont réalisées par campagnes de mails ou au travers de la navigation Internet, les attaquants ayant au préalable infecté un site Internet légitime (attaque de type « point d'eau »).

Un attaquant dispose aujourd'hui d'un arsenal d'outils impressionnant et régulièrement mis à jour lui permettant le plus souvent d'exploiter automatiquement les dernières vulnérabilités avec très peu de connaissances techniques.

Le pot de miel

Entre l'annonce d'une vulnérabilité et le moment où il devient possible de l'exploiter, les délais pour appliquer les correctifs sont de plus en plus courts (quelques jours à peine, voire quelques heures). A une époque il était courant de dire qu'il fallait moins de 10 minutes pour qu'un poste dépourvu d'un antivirus et connecté à Internet se retrouve infecté. En ce qui concerne les vulnérabilités, c'est la même histoire ! Il existe des outils appelés « Honeypot » (pot de miel) dont les failles ne sont pas corrigées mais surveillées afin de comprendre comment un attaquant opère pour les exploiter ou pour identifier une tentative d'attaque. Il est alors possible de constater la vitesse fulgurante avec laquelle ces machines font l'objet d'attaques.

Je pourrais aussi vous parler des sites Internet et des outils de gestion (CMS) qui souvent les accompagnent, mais vous l'aurez compris: une bonne hygiène de son système d'information passe par la connaissance exhaustive de ses équipements et une parfaite gestion de leurs mises à jour. Je sais pertinemment que l'application des mises à jour peut apporter son lot de problèmes, le fait qu'il faille les planifier pour ne pas interrompre l'activité, etc. La tâche est loin d'être simple, mais au regard de la multiplication des d'équipements connectés, il est impératif de lancer des actions si l'on ne veut pas refaire le même constat dans dix ans.

Les cinq temps de la gestion des incidents SSI

Le temps d'un incident, est multiple : non seulement les étapes sont nombreuses et n'ont ni la même durée ni la même importance, mais ce découpage n'est pas le même selon que l'on se place du point de vue de l'utilisateur, de la DSI ou du RSSI.

Cédric Cartau, RSSI et DPO du CHU de Nantes et du GHT44, est également chargé de cours à l'EHESP et à l'ESIEA . Il collabore régulièrement à la revue DSIH et a publié plusieurs ouvrages, notamment « La sécurité du système d'information des établissements de santé », seconde édition (Eyrolles, 2017).

Dans un monde parfait, les serveurs ne plantent pas, les sauvegardes n'échouent jamais et il est toujours facile et rapide de les restaurer, les liens réseau et Internet sont opérationnels à 100% du temps. Mais, en attendant le monde parfait de l'Ile aux enfants, les serveurs lâchent, les fils sont coupés et les sauvegardes plantent, et il faudra bien gérer les incidents, ce qui est beaucoup moins facile qu'il n'y parait.

Détection par les utilisateurs

Pour les utilisateurs, l'incident commence… dès qu'il commence : lorsque **« ça » ne marche plus**. Qu'il s'agisse d'une panne de la borne Wi-Fi dans un service, de la panne d'un progiciel métier, d'une fuite de données patient, d'un bug logiciel, les utilisateurs sont souvent les premiers à détecter l'incident, surtout dans la catégorie des incidents en disponibilité. C'est moins net pour les incidents en confidentialité – qui peuvent être signalés par les usagers eux-mêmes – ou ceux en intégrité : dans ce dernier cas, les modes de détection sont multiples, allant de la détection automatisée à celle par la DSI ou par les usagers. Le pire étant les incidents qui sont détectés longtemps après s'être produits : on pense évidemment à l'accident d'Epinal (sur-irradiations massives détectées des années après le début du dysfonctionnement) ou à des fuites massives de bases patients que l'on apprend des mois après.

Déroulement des contre-mesures

Vient ensuite **le temps des contre-mesures immédiates**, qui se divisent en deux catégories : celles mises en place par les utilisateurs (les procédures dégradées métier), et celles mises en place par la DSI. Là encore, les temps ne sont pas les mêmes. Pour un incident en disponibilité, les informaticiens vont travailler immédiatement au déroulement des contre-mesures (bascule de serveur ou de salle, restauration de données, etc.), alors que les utilisateurs vont attendre un laps de temps – plus ou moins long – avant de décider de passer en procédure dégradée. Cette dernière a en effet un coût organisationnel qui varie selon les services (très élevé pour les urgences par exemple, très faible pour certains services logistiques). Pour les fuites de données, à part « boucher le trou » quand cela relève de la technique, les contre-mesures sont par contre souvent du seul ressort des métiers. Révision de la politique d'habilitation, analyse des traces d'accès, signalement des incidents aux personnes concernées : le Délégué à la Protection des Données doit travailler avec la MOA. Idem pour les incidents en intégrité.

> « Vient ensuite le temps du signalement, car l'époque est à la transparence, ce qui est une bonne chose. Il y a peu de temps, aucun signalement n'était obligatoire pour un incident SI, même grave »

Reprise d'activité

Une fois les failles techniques corrigées par la DSI, si le travail est terminé pour elle ce n'est pas le cas pour les métiers. Il faut **saisir des données manquantes dans le système** en même temps que saisir les données qui arrivent du fait de la reprise d'activité. Le véritable retour à la normale pour les métiers survient bien après la résolution technique de l'incident par la DSI, tout du moins pour les incidents en disponibilité. Là encore, l'analyse est différente pour les incidents en confidentialité et en intégrité puisque, dans certains cas, le retour à la normale peut-être beaucoup plus lent, voire impossible : dans le cas par exemple d'une fuite massive de données médicales sur Internet.

Signalement

Vient ensuite **le temps du signalement**, car l'époque est à la transparence, ce qui est une bonne chose. Il y a peu de temps (avant 2016), aucun signalement n'était obligatoire pour un incident SI, même grave. Depuis, nous avons vu passer le décret 2016-1214 du 12 septembre 2016 (obligation de déclaration des incidents SSI graves), le RGPD (obligation de déclaration des incidents relatifs aux traitements de données

personnelles, à la CNIL et / ou aux personnes concernées selon les cas) et la directive NIS (loi 2018-133 du 26 février 2018) qui impose aussi un signalement des incidents SI et dont nous attendons les modalités pratiques sous peu. Dans certains cas, il faudra donc réaliser quatre déclarations !

> « Le véritable travail du RSSI commence une fois la situation redevenue normale, avec l'analyse post-mortem de l'arbre des causes »

L'action du RSSI

Le lecteur attentif aura certainement remarqué qu'à ce stade, nous n'avons pas une seule fois évoqué **l'action du RSSI** : c'est normal, pendant le temps de la panne et de la remédiation, il ne sert pas à grand-chose sur le plan technique. Son véritable travail commence une fois la situation redevenue normale, avec l'analyse post-mortem de l'arbre des causes, car il faut faire en sorte que cet incident ne se reproduise plus jamais, ou que les impacts soient maîtrisables si d'aventure il survenait à nouveau. Je connais des recruteurs qui posent une question en apparence anodine en fin d'entretien : quel est le moment le plus important dans un incident SI pour le RSSI ? Question anodine mais question piège : la réponse est « Après ».

Outiller le processus de gestion des changements

Beaucoup d'incidents de sécurité sont induits par une absence, ou une mauvaise gestion, des changements apportés aux différents composants supports du SI. Le processus de Gestion des Changements est un levier important de diminution des risques. Il doit s'appuyer sur des outils dont les différents modules sont décrits ici.

Stéphane Moneger, Responsable SI du Centre Hospitalier de Brive depuis 2001, est engagé depuis quatre ans dans une politique de sécurité du SI. Ingénieur EPITA 1991, spécialisé en IA, il a précédemment travaillé pour le CNRS, ITN Consultants, Arthur Andersen, Sopra, Cogema Japon. Il est responsable de la partie Santé de l'étude MIPS 2018 du Clusif (Menaces informatiques et pratiques de sécurité en France)[1].

Le SI hospitalier évolue en permanence. Tous les jours, ou presque, des composants (matériels, logiciels ou organisationnels) du SI font l'objet de changements : des ajouts, des mises à jour, des remplacements ou suppressions. Ces changements, plus ou moins bien maîtrisés, peuvent engendrer des incidents, potentiellement graves.
Afin de maximiser l'efficacité d'un processus de gestion des changements, il est nécessaire de s'appuyer sur quelques outils simples et efficaces.
Tout d'abord, il est indispensable de bien connaitre le périmètre concerné par les changements et de l'avoir cartographié.

> « Trop de changements non terminés indiquent qu'il y a soit un problème d'organisation et de planification, soit un problème de ressources. Dans tous les cas c'est un facteur de risques supplémentaires »

Recenser les applications

Les applications doivent être recensées avec au moins les indicateurs suivants :

- Le responsable ou référent (en relation avec le module de gestion des utilisateurs)
- Un mode dégradé est-il prévu en cas de maintenance ou de panne
- Liste des changements des deux dernières années, en particulier des mises à jour. Une application à jour est en théorie plus sécurisée (en relation avec le module de gestion des changements)
- Liste des revues de droits (utilisateurs affectés au bon profil, départs gérés)
- Liste des incidents DIC: disponibilité, intégrité, confidentialité (en relation avec le module de gestion des incidents)

Des données de dimensionnement peuvent être utiles pour mieux évaluer les impacts d'un incident, d'un changement :

- Nombre d'utilisateurs
- Fonctionnement H24

Enfin, ce module peut embarquer la gestion documentaire de l'application :

- Déclaration CNIL (avant le RGPD)
- Documents d'exploitation, Mode dégradé

Identifier les flux et interfaces

De même, les Flux ou Interfaces entre applications doivent être identifiés et décrits :

- Applications source et cible (en relation avec le module de gestion des applications)
- Passerelle d'échange éventuelle avec descriptif du protocole d'échange
- Serveurs source et cible (en relation avec le module de gestion des serveurs)
- Le responsable ou référent (en relation avec le module de gestion des utilisateurs)

Les Serveurs qui hébergent les applications et flux doivent être identifiés et décrits :

- Caractéristiques IP
- Présence antivirus
- OS : type et version
- Serveur patché ?
- Machine physique ou virtuelle

Les indicateurs

Le module de Gestion des changements doit proposer les indicateurs suivants :

- L'état d'avancement (Demandé, annulé, en cours, suivi post prod, terminé) est pertinent : avoir trop de changements non terminés indique qu'il y a soit un problème d'organisation et de planification, soit un problème de ressources. Dans tous les cas c'est un facteur de risques supplémentaires.
- Un indicateur (mode de gestion) doit tracer si le

1 Menaces informatiques et pratiques de sécurité en France. https://clusif.fr/conferences/etudes-menaces-informatiques-pratiques-de-securite-edition-2018/

changement est « géré » (respecte le processus), ou « non géré ». Le retour d'expérience sur trois ans est édifiant pour notre structure, puisqu'un tiers des changements « non gérés » induisent des incidents, alors que moins de 10% des changements « gérés » sont source d'incidents.

- Comme pour toute activité, il faut un responsable garant de la bonne réalisation. L'intérêt de cet indicateur est aussi de contrôler que ce ne sont pas toujours les mêmes ressources qui assurent cette charge, ou alors de le mettre en évidence. Là encore, c'est un facteur de risques supplémentaires.
- L'objet doit être décrit (action, composant concerné, version, pourquoi) en relation avec les modules qui gèrent les composants et les acteurs.

.Le demandeur doit être décrit (utilisateur, service) en relation avec les modules qui gèrent les acteurs et services.

- Le formulaire doit lister les incidents induits (en relation avec le module de gestion des incidents).

Enfin, dans la mesure où un changement peut être un projet, il est possible de le lier à la liste des actions à réaliser (action, acteur, date). L'intérêt est alors de pouvoir ainsi alimenter pour chaque acteur une liste de travail « mes actions ». On parle de SDA (Schéma Des Actions), ou de RACI (matrice des responsabilités : Responsible, Accountable, Consulted, Informed).

Tableau de bord

Afin de disposer d'une vision synthétique, un tableau de bord doit permettre d'agréger les données de tous les changements et d'identifier rapidement les changements « non gérés », sans responsable, qui produisent des incidents, qui ont dépassé leur date de mise en œuvre…
Le calendrier des changements (semaine, mois, année) doit être visualisable en un clic et partageable à toute l'équipe SI sur un affichage de service (« management visuel »).

Gérer les incidents

Les changements étant une des sources d'incidents DIC, l'outillage doit embarquer un module de Gestion des Incidents avec au moins les indicateurs suivants :

- L'origine de l'incident (Dysfonctionnement après mise à jour, défaillance d'exploitation, panne, malveillance…) est importante afin d'avoir une démarche corrective efficace.
- Le responsable ou gestionnaire (en relation avec le module de gestion des utilisateurs)
- Le Logiciel ou Matériel impacté (implique de les avoir cartographiés)
- Les impacts : DIC

L'analyse des « causes » se fait à deux niveaux (Cause apparente / Cause racine) car il faut aller au-delà des apparences afin d'identifier l'origine profonde.

Les actions entreprises se situent aussi à deux niveaux :

- Actions correctives : traitement immédiat
- Actions préventives : traitement de fond

Le module peut aussi embarquer des documents (Fiche de signalement des incidents / évènements indésirables, compte-rendu d'analyse...)

Pour un outil complet

Si l'on souhaite disposer d'un outil complet, il doit s'appuyer sur un module de gestion des utilisateurs en relation avec l'annuaire AD d'entreprise dans lequel chaque acteur retrouve :

- Les changements dont il est responsable
- Les actions qu'il doit réaliser dans le cadre des changements
- Les incidents dont il est gestionnaire
- Les composants SI dont il est référent (applications, flux, serveurs)

Enfin, cet outil pourra proposer un module de gestion des fournisseurs de composants, en relation avec les modules de cartographie (Applications, Flux) et les acteurs des changements. Il pourra aussi assurer le rôle d'annuaire des contacts (adresse, tel, mail, fonction).

Pour ceux qui ne disposent pas d'outil spécifique de gestion des login/password techniques (serveurs, bases de données, télémaintenances…), il peut être intéressant d'intégrer dans les différents modules de cartographie un volet codes d'accès avec cryptage de mots de passe.

Quelques copies d'écran du portail SSI que nous avons développé à l'aide du générateur d'applications Peanut Builder.

L'enjeu de la gestion contractuelle dans l'atteinte de la conformité des SI en santé

La gouvernance contractuelle doit désormais intégrer l'enjeu de mise et de maintien en conformité. Il s'agit bien de rendre au contrat son sens premier, celui d'outil de pilotage de la relation entre deux parties : le contrat est alors le reflet du partenariat client-fournisseur.

Senior Manager Sopra Steria Conseil, spécialisée en conformité des données de santé, **Pauline Berry**, diplômée ESSCA (Ecole Supérieure Sciences Commerciales Angers) est experte en transformation de processus et SI, et maîtrise l'approche pluridisciplinaire en compliance santé. Consultante depuis 13 ans, elle a rejoint Sopra Steria Conseil Lyon en 2012. Elle co-anime le Club des Pilotes de Processus (C2P), qui réunit les professionnels du management transversal des organisations, et contribue au Comité Santé Syntec Numérique. Elle a piloté de grands projets en santé : accréditation SI laboratoires, sécurisation SI santé, hébergement de données de santé, formation. Ambassadrice du Programme Passer'elles Groupe Sopra Steria pour la mixité, elle contribue au programme de formation et à la promotion des métiers du numérique auprès des lycéennes.

Isabelle Zablit, présidente de Clavesis Conseil en Stratégie Santé Numérique, est co-présidente du Comité Santé Syntec Numérique et présidente le Programme #5000startups. Elle a co-fondé Wellfundr, start-up e-santé. Administratrice IHEST (Institut des Hautes Etudes pour la Science et la Technologie), vacataire en santé numérique à l'EFREI (école d'ingénieurs), en gestion des risques internationaux à Paris 1–Panthéon Sorbonne et tuteur ENA, elle a été Business Development Executive IBM Europe et France, où elle a dirigé l'entité Conseil Shared Services, après avoir été Business controller chez Tenneco Automotive Europe et LafargeHolcim, et chargée de cours à l'Université Libre de Bruxelles (ULB). Ingénieur Solvay Brussels School of Management et agrégée en sciences économiques de l'ULB, Isabelle est administrateur de société certifiée ESSEC et auditeur de l'IHEST.

La gestion des contrats de prestations numériques est jugée particulièrement complexe par les responsables de traitement de données de santé. Ce n'est en réalité pas surprenant, au regard du contexte réglementaire évolutif constaté dans l'ensemble de l'économie, et en particulier dans le secteur de la santé.

Plus que d'autres, le secteur de la santé fait face à des évolutions spécifiques et importantes telles qu'illustré récemment par le passage d'un agrément pour l'hébergement agréé données de santé à une certification. La complexité réglementaire ressentie par l'ensemble de l'écosystème provient également de l'expérience limitée des collaborateurs en matière de gestion contractuelle, les contrats de prestations étant souvent gérés par des experts. Or aujourd'hui, du fait même de l'impact des évolutions, le contrat doit davantage être maîtrisé par les équipes opérationnelles. Il faut en outre être conscient que les évolutions attendues du cadre réglementaire, liées à l'éthique, aux pratiques et aux enjeux de protection des données, dans un écosystème où les métiers eux-mêmes font l'objet de transformations, ne vont probablement pas simplifier la gestion des contrats dans les années à venir. Il est donc important d'accorder une vigilance particulière à ces éléments.

Dans ce contexte, la gouvernance contractuelle est essentielle pour répondre aux enjeux de maintien en conformité, et elle tend à devenir un élément déclencheur de la remise à niveau des contrats. Jusqu'à présent, les contrats de prestations étaient revus périodiquement principalement en raison des aspects financiers. L'accent qui est mis aujourd'hui sur la conformité réglementaire n'est cependant ni nouveau, ni récent. Mais aujourd'hui, il s'agit de la placer au cœur de la gouvernance contractuelle, afin d'accompagner plus largement les changements en cours.

En pratique, une gestion contractuelle plus structurée et partagée au niveau opérationnel permet de piloter cette transformation et redonne au contrat son sens premier, celui d'outil de pilotage de la relation pour les deux parties. Utiliser cette approche dans un esprit de partenariat entre le client et le fournisseur de prestations en y intégrant les aspects opérationnels aide à mieux anticiper les évolutions des prestations, ce qui est particulièrement important dans un contexte de transformation numérique. Le contrat reprend ainsi son rôle initial : être le reflet du partenariat qui unit les parties dans cette démarche.

Compléter les exigences SSI

L'impact de la montée en puissance des politiques de sécurité au sein des organisations ou des établissements de santé et de leurs partenaires, renforcé par la mise en œuvre du règlement européen sur la protection des données personnelles, et par celle du cadre spécifique lié au traitement et

L'enjeu de la gestion contractuelle dans l'atteinte de la conformité des SI en santé

à l'hébergement de données de santé, a nécessité d'inclure ou de compléter de manière substantielle les exigences en matière de sécurité des systèmes d'information (SSI) dans la plupart des contrats. Ces évolutions ont conduit à réaliser non seulement une mise à jour des clauses contractuelles elles-mêmes, mais aussi à revoir les conditions et moyens technologiques et organisationnels de réalisation des prestations concernées.
Ces nouveautés sont aussi dues à l'évolution des périmètres de responsabilité respectifs entre client et fournisseur. L'impact de ces changements nécessite une vigilance particulière dans le suivi contractuel, et peut se retrouver dans les éléments de mesure de satisfaction à travers la définition d'indicateurs de qualité de service adaptés car ces mesures contribuent à exprimer les attentes de chacune des parties de manière explicite, à identifier en amont les rôles et responsabilités réciproques. La clarification des responsabilités (par exemple entre responsable de traitement – éditeur de logiciel – hébergeur) peut induire des choix d'architectures techniques et des choix d'outils technologiques différents, et inviter à adapter certaines procédures de gestion.

Vérifier les périmètres de responsabilité sur les données personnelles

La remise à plat des contrats de prestations numériques dans un objectif de maintien ou de mise en conformité devient un sujet majeur pour les directions des responsables de traitement ; la mise en œuvre du RGPD qui a amené les responsables de traitement à revoir méthodiquement, et par priorisation progressive, l'ensemble de leurs contrats, a aussi contribué à souligner son importance. Cette dynamique a obligé chacune des parties prenantes (fournisseur, client, sous-traitant…) à intégrer by design les conditions de sécurisation des données. Ainsi, la mise en œuvre du RGPD a contribué à mettre en lumière le fait que les négociations contractuelles nécessitaient plus qu'auparavant (et certainement moins que demain) une approche et des compétences pluridisciplinaires.
La prise en compte de la conformité et de la sécurité des systèmes d'information en amont des contrats, la rédaction des appels d'offre et des contrats nécessitent aujourd'hui de mobiliser non seulement le service juridique et le service des achats ou avant-vente des parties, mais aussi et davantage le RSSI, les gestionnaires de projets métier et SI et le DPO ainsi que les équipes techniques… Cette démarche n'est pas seulement consultative et elle tend à devenir un projet à part entière ; elle contribue ainsi à la gestion du changement apportée par la mise en œuvre du contrat sur les différents rôles opérationnels.

Le corps du contrat et ses annexes

Notre retour d'expérience montre qu'il est généralement pertinent d'inscrire dans le contrat l'ensemble des clauses relatives aux audits sécurité, au PRA/PCA (Plan de Reprise d'Activité/Plan de Continuité d'Activité), à la gestion des données personnelles, à la confidentialité, et de mettre en annexes les éléments détaillés relatifs à la description des services, aux niveaux de service, aux plans qualité et assurance sécurité, au plan de réversibilité, à la matrice de responsabilité liée aux spécificités sur les traitements des données de santé - dont l'hébergement - et aux modalités pratiques d'information et/ou recueil de consentement relatifs aux traitements de données personnelles. Le choix de traiter ces éléments dans le corps du contrat ou dans les annexes contractuelles correspond, au-delà des choix juridiques à opérer, à une organisation pratique des équipes. En effet, lorsque les éléments contractuels correspondent à des aspects détaillés traités par des équipes d'experts, il est plus aisé de les placer en annexe du contrat que dans le corps du contrat. Par exemple, le plan d'assurance sécurité est en général uniquement maîtrisé par les experts du sujet sécurité, et dans une moindre mesure par le gestionnaire du contrat, il fait donc l'objet d'une annexe contractuelle. Dans certains cas, cette organisation contribue aussi à répondre à un souhait de limiter les cas où un avenant au contrat serait nécessaire.
Pour renforcer la sécurité des systèmes d'information et des données, être attentif à la rédaction du contrat fait partie des actions à mettre en œuvre. Ce principe est également valable pour atteindre l'objectif de conformité à un cadre réglementaire pour les périmètres de prestations objets de ces contrats : dès lors, le contrat de prestation détermine le contexte de la collaboration dans laquelle chacune des parties a un rôle à jouer en vue d'atteindre les objectifs fixés. Les parties doivent par exemple veiller à la formation des équipes en charge de l'exécution de ces contrats, tant sur les aspects classiques de la gestion que sur les obligations et responsabilités relatives au périmètre sensible de la gestion des données et des systèmes d'information en santé.

Externalisation et évolution des profils de compétences

En cas d'externalisation des prestations de services numériques, les enjeux précités sont renforcés. Si l'externalisation recentre le responsable de traitement sur son cœur de métier, elle le place en pilote de l'exécution des prestations de services numériques. Cela entraîne parfois une conduite du changement importante pour faire évoluer les profils de compétences dans les équipes. La responsabilité opérationnelle des équipes projets s'en trouve profondément transformée et peut requérir d'adapter les compétences, et même de faire intervenir de nouveaux profils de compétences.
La bonne compréhension sur l'évolution du contexte, l'éclairage sur les nouveaux rôles opérationnels et la prise en compte de la gestion du changement à mettre en œuvre pour chacun des membres des équipes sont des prérequis incontournables pour déployer de manière optimale les solutions technologiques en santé et veiller à ce qu'elles soient utilisées selon les bonnes pratiques.
La gestion des contrats de prestations numériques est jugée particulièrement complexe par les responsables de traitement de données de santé : elle nous paraît avant tout être une opportunité à saisir dans le contexte où les organisations cherchent à atteindre leur objectif de conformité. Mettre en place une véritable gouvernance contractuelle, avec la contribution des équipes opérationnelles et non des seuls experts juridiques ou sécurité nous paraît être un facteur clé de succès pour réussir une mise en conformité de manière optimisée.

0.6 CONFORMITÉ ET AUDITS

La démarche d'homologation de sécurité des systèmes de santé : susciter l'adhésion, **Astrid Lang** P. 91 À 93
Comment organiser le suivi de conformité interne, **Lénaïc Plouvier** P. 94
Cahier spécial Audit, **Mauro Israel** P. 96 À 109
- Les concepts et principes de l'audit
- Le déroulement d'un audit
- La check-list de la cybersécurité

La démarche d'homologation de sécurité des systèmes de santé : susciter l'adhésion

Forte de son expérience dans le montage et la conduite d'opérations d'homologation de sécurité à l'AP-HP, Astrid Lang partage ici ses observations et conseils : à quelles réactions s'attendre ? quels sont les facteurs de succès ? Comment installer la dynamique autour des projets ? Retour d'expérience en 5 points forts.

Astrid Lang est Responsable du Pôle Sécurité et Architecture / Département SI Patient au sein de la Direction des Systèmes d'Information de l'Assistance Publique – Hôpitaux de Paris (AP-HP). Avec plus de 30 ans d'expérience de direction de projets dans la santé, Astrid a mené des opérations d'informatisation sur l'ensemble des hôpitaux de l'AP-HP dans le contexte médical, médico-technique, finance/ achat/ logistique/ patrimoine. Elle est depuis 2008 RSSI du Système d'Information Patient, dans le cadre de la refonte du système d'information lié au patient qui impacte 80 000 utilisateurs. Sa mission porte en particulier sur le respect de la sécurité et de la réglementation dans l'utilisation du dossier électronique du patient. Elle participe à divers travaux nationaux relatifs à la sécurité du SI Santé et anime le Club des RSSI des CHU-CHR.

Dans un établissement de santé, mener l'homologation de sécurité d'un système communiquant avec les usagers ou avec une administration n'est pas toujours une sinécure !
Parfois, elle est vécue comme un frein : une instance en plus du comité de pilotage ? Pour la maîtrise d'ouvrage, face à la portée stratégique du projet: cela ne retarde-t-il pas le lancement opérationnel ? Pour la DSI: n'est-ce pas comme se faire auditer dans un domaine qui est son cœur de métier ?
En tout cas, c'est une obligation réglementaire depuis mai 2013 ! C'est en voyant les réactions en interne, mais aussi en entendant les difficultés que rencontrent certains collègues RSSI pour mobiliser leur direction, qu'il m'est paru intéressant de partager - en toute modestie - mon expérience en la matière.

Obligatoire depuis mai 2013

Aujourd'hui, un établissement de santé qui se lance dans un projet numérique innovant ou stratégique travaille souvent dans l'urgence. Ce qui compte, c'est d'aller vite dans la mise en œuvre du projet, de voir rapidement le résultat et les impacts auprès des utilisateurs, de pouvoir mesurer le retour sur investissement et le rayonnement généré le cas échéant.

Lorsque l'équipe Sécurité SI signale que le système, ouvert et communicant avec les patients et/ou les partenaires, est soumis, avant ouverture du service, à l'obtention d'une attestation formelle de son autorité administrative, c'est-à-dire l'homologation de sécurité, ni les équipes projet et technique, ni la maîtrise d'ouvrage ne s'en réjouissent de prime abord. On ne voit pas d'un bon œil cette étape, instituée par l'ordonnance n°2005-1516 du 8 décembre 2005 et son Référentiel Général de Sécurité (RGS) des systèmes d'information, puis rendue obligatoire en mai 2013.
N'est-ce pas du temps perdu pour le projet ? Une complexité réglementaire que l'on découvre, voire des complications pour les maîtres d'œuvre ? Des acteurs supplémentaires qui « se mêlent de tout »? Des charges et des coûts non prévus ?
Le montage et la conduite d'opérations d'homologation de sécurité à l'AP-HP, et les réactions observées auprès des parties prenantes, m'ont amenée à veiller à certains points qui sont devenus pour moi des facilitateurs de succès de la démarche. Je les aborde ci-après, tels que je les ai vécus et sans vouloir mettre d' ordre chronologique ou d'importance.

> « Si vous ne disposez toujours pas de Commission d'homologation à ce jour, proposez sa création en vous appuyant sur un projet porteur »

1 Alerter et refuser de déployer un système soumis au RGS, si l'homologation de sécurité n'est pas faite ? Facile à dire ! Préparer un dossier d'homologation n'est pas une mince affaire si on ne l'a jamais fait. Et le nombre d'établissements disposant d'une structure ad hoc pour prononcer la décision d'homologation se compte au maximum en dizaines à ce jour.
A l'AP-HP, depuis fin 2014, à l'occasion du projet de paiement en ligne, la DSI a proposé au secrétariat général la constitution d'une Commission d'Homologation : la démarche était lancée.
Si vous ne disposez toujours pas de Commission à ce jour, proposez sa création en vous appuyant sur un projet porteur, voire urgent, et rappelez la réglementation en vigueur. Surtout, veillez à préciser que les travaux dans ce cadre sont déjà engagés (identification des risques, démarche sécurité proposée) afin d'être moins alarmiste.
Si le projet ne prévoit pas de passer par l'homologation pour des raisons de délai ou autres, tirez la sonnette d'alarme.

La démarche d'homologation de sécurité des systèmes de santé : susciter l'adhésion

2 Impliquer les décideurs et les métiers, en leur montrant leur rôle et leur pouvoir de décision, en mettant le contexte à leur portée.

Autour de la table

En plus de l'autorité administrative, il est important pour la Commission de disposer d'un comité rassemblant un public averti, motivé, curieux, soucieux de pouvoir mettre en œuvre le système. Il faut, autour de la table, la maîtrise d'ouvrage (MOA) opérationnelle, donc celle qui porte le projet à sa réussite, les équipes projet et techniques qui œuvrent à la construction du système, et aussi des invités : par exemple, d'autres départements techniques en interface, ou tout simplement des personnes intéressées ou qui vont se lancer (MOA ou chefs de projets) ; cela apporte une forte motivation et une émulation extraordinaire dans les débats en séance.

Pour que les décideurs acceptent de participer à une Commission, et ne rechignent pas à se réunir à cette fin, il faut susciter leur intérêt :

- Disposer pour la séance d'un support simple, compréhensible par les métiers, même si le dossier d'homologation respecte une forme imposée,
- Présenter ou rappeler dès le début le contexte, les risques réels, ce surtout dans leur propre langage, en évitant des termes trop techniques sans traduction de l'impact fonctionnel, organisationnel ou juridique,
- Veiller à une forme (écrite et orale) courte et percutante, qui incite constamment au questionnement et à l'interactivité,
- Penser à indiquer, pour éclairer la décision, une synthèse des risques résiduels pour le métier, des possibilités de décision (avec les variantes), et pour chaque cas la conséquence ou le risque, afin de les amener à décider en connaissance de cause,
- Lors d'un deuxième passage en Commission d'homologation, il faut leur montrer les progrès déjà accomplis (grâce à leur précédente décision), en pointant le cas échéant le lien avec l'objet de la nouvelle homologation,
- Et s'ils veulent passer, lors de la 2e ou 3e homologation, d'une séance de 2h30 à 1h, voire « une demi-heure en commençant à la page 23 » (c'est du vécu !)… il faut accepter de le faire, et on sait le faire si on domine fonctionnellement et techniquement le sujet.

Les décideurs s'impliquent alors tellement qu'ils s'orientent parfois vers une décision qui n'était pas de celles imaginées ou proposées, mais une décision parfaitement juste, basée sur la perception de la stratégie qui leur est propre.
Ils imposent par exemple un nouveau rendez-vous d'homologation plus tôt qu'envisagé : ils prononcent une homologation partielle, en limitant la mise en œuvre du système à certaines fonctions, pour forcer à diminuer les risques sur les autres fonctions avant ouverture ; ou en limitant à un service pilote, pour vérifier le processus de fonctionnement et disposer d'un REX (retour sur expérience) avant déploiement plus large ; ou en décidant d'une homologation pour 15 mois car une nouvelle version du système promet l'amélioration de certains points.

3 Préparer l'homologation en étant proche des équipes Projets et de la Maîtrise d'Ouvrage sous l'angle fonctionnel
Il faut expliquer aux maîtrises d'ouvrage (MOA) l'intérêt de l'homologation de leur projet, et illustrer avec des exemples vécus. Alors les MOA s'expriment d'elles-mêmes sur les besoins de sécurité du système, souvent complémentaires voire différents des besoins exprimés par l'équipe projet DSI. En compilant les éléments évoqués, les équipes projets et MOA comprennent les enjeux et les risques, et vont pousser en ce sens aussi bien que nous, spécialistes en la matière.
Parfois, c'est à nous RSSI d'attaquer sur tous les fronts pour les rendre conscients des risques (exemples : exposition des données sur un délai trop long, épuration des données non utiles pour la finalité) ; on réussit même à faire bouger le fournisseur, surtout sous la pression de la MOA, pour livrer des fonctions plus adaptées.
Il y a une dynamique qui s'installe autour de l'opération, où les propositions de la MOA et du projet fusent (exemples : renforcer le dispositif avec une charte, compléter une convention, déporter l'ouverture des accès sur une équipe plus armée en la matière, élargir ou restreindre le périmètre, etc.).

> « Expliquer aux maîtrises d'ouvrage l'intérêt de l'homologation de leur projet, et illustrer avec des exemples vécus »

4 Durant toute la préparation de l'homologation, ne pas lâcher l'équipe projet, les équipes infrastructure et le fournisseur du système
Si les mesures de sécurité nécessaires ne sont pas en place, il ne faut pas hésiter à « menacer » de décaler la date de la Commission déjà planifiée (depuis plus d'un mois), voire d'annuler, plutôt que d'arriver devant une Commission avec un dossier immature. Cela met une pression positive et motivante, et l'ambiance devient étonnamment « corporate », dirait mon directeur.
Il faut aussi revérifier si les mesures sont toujours actives : citons le cas où un rapide contrôle d'intrusion avant ouverture du système nous a révélé que des paramètres de sécurité avaient « sauté » !

La démarche d'homologation de sécurité des systèmes de santé : susciter l'adhésion

5 Ne pas hésiter à se faire accompagner dans la démarche d'homologation, mais surtout rester en Assistance à maîtrise d'ouvrage (AMOA)

Il est intéressant de prendre une société spécialisée pour construire la démarche et réaliser l'analyse des risques et les tests d'intrusion, mais il faut rester en AMOA auprès de tout interlocuteur MOA ou Projet.

En effet, il est primordial de sous-traiter ce qu'on ne fait pas bien ou ce qui prendrait trop de temps (on ne peut être spécialiste, sauf entraînement constant), et aussi pour être complémentaire et veiller au dynamisme de l'opération. Notre « plus » en tant que RSSI Santé est notre connaissance du SI et du métier.

Souvent la collaboration avec une société apporte aussi plus de neutralité et de force de conviction pour des points délicats.

Si on s'implique bien dans la démarche et si on domine le sujet fonctionnellement et techniquement, les coûts d'accompagnement peuvent être réduits voire optimisés.

> « Ne pas hésiter à sous-traiter ce qu'on ne fait pas bien ou qui prendrait trop de temps »

En conclusion, la démarche d'homologation est bien acceptée et suscite un fort intérêt des parties prenantes et des décideurs, si l'on arrive à instaurer un esprit de confiance de bout en bout. Une communication compréhensible par tous, une transparence et un partage des constats, la persévérance : ce sont les moteurs à « faire vibrer » dans ce cadre, et ils nous amènent, en plus, à progresser avec nos interlocuteurs en matière de maturité sécuritaire.

En amont

Si le système n'a pas été homologué précédemment chez un autre client, il est important de prendre le sujet en vue de l'homologation très en amont, et de faire par étapes. Par exemple, de procéder à des tests d'intrusion sur un environnement de tests nous a permis d'identifier des problèmes de taille, et ainsi de laisser à l'éditeur, au projet et à l'infrastructure le temps de se caler, d'adapter et de relivrer le système, avant les tests et vérifications en production.

Comment organiser le suivi de conformité interne

Le besoin de conformité qui pèse sur la sécurité des systèmes d'information de santé est multiforme et en constante évolution (PGSSI-S, certification des comptes, Hôpital numérique, …), d'où la nécessité d'une gestion de la conformité, basée sur un plan de contrôle et d'audit.

Lénaïc Plouvier, diplômé de l'Institut Informatique d'Entreprise en 2002, a rejoint Pictime Groupe en tant qu'administrateur système, sécurité et réseau en 2007. Après avoir mené différentes missions techniques, il manage aujourd'hui l'équipe de Direction Technique Cloud & Sécurité de Pictime Groupe, composée d'experts, tout en étant porteur des risques infrastructures et relais pour ISO 27001. Il participe également au comité sécurité.

La gestion de la conformité peut prendre plusieurs formes. Il peut s'agir d'un mélange de stratégies, procédures, documentations, d'audits internes, d'audits de tiers et de contrôles de la sécurité. Elle s'inscrit en général dans un système de gestion de la qualité, ce qui permet de faire appel à des appréciations. Car il est généralement admis que toutes les règles ne peuvent pas être suivies dans tous les cas. Par conséquent, des exceptions doivent être faites pour permettre à l'établissement de fonctionner de son mieux, tout en respectant autant de règles que possible. Le meilleur dénominateur commun pour la conformité des systèmes d'information de santé semble être la norme ISO 27001. Le piège à éviter est d'être conforme par l'application des bonnes pratiques de sécurité mais sans prise en compte du contexte, et donc sans atteindre l'objectif de la qualité et de la sécurité des soins.

Vérifier la mise en place des actions

Quoiqu'il en soit, l'audit interne reste un moyen incontournable de gestion de cette conformité. Ce doit être une activité indépendante et objective, afin de donner à l'établissement de santé une assurance sur son degré de maîtrise des opérations et son contrôle sur les données. L'approche doit être systématique, méthodique, mais rester pragmatique en apportant conseils et propositions aux équipes.

Pour illustrer la mise en place de la conformité liée à notre agrément HDS et à notre certification ISO 27001, afin de nous assurer que toutes les mesures de sécurité définies dans la déclaration d'applicabilité soient bien en place et répondent aux besoins afin de couvrir les risques, nous avons mis en place un plan de contrôle et d'audit pour organiser leur révision.

Le plan de contrôle vérifie la mise en place des actions et l'efficacité du système de management de la sécurité de l'information, notamment en planifiant les contrôles à effectuer et en définissant les acteurs responsables de la surveillance, de l'analyse et de la présentation.

Une semaine qualité

Maintenir la conformité dans le temps nécessite des efforts de mobilisation en transverse des équipes, en instantané comme au long cours, la diffusion et la mise à jour de l'information. Une semaine qualité a été mise en place afin de reconcentrer les équipes, chaque mois, sur l'atteinte des objectifs fixés, dégager du temps pour permettre la réalisation en synergie des actions prévues, la prise de recul sur le travail quotidien, la projection pour le futur et l'amélioration de l'existant. La planification en automatique, ajoutée à la mise à jour constante des tâches à réaliser, permet le suivi de la conformité en interne.

Les problèmes sont toujours possibles, certains incidents en sont parfois l'illustration, et font partie du système en tant que non-conformités. Il convient de les relever, les prendre en compte, identifier les solutions qui éviteront qu'elles se reproduisent pour finalement les corriger. Les non conformités ne doivent pas être vécues en tant qu'échec mais comme un moyen de s'améliorer.

> « Maintenir la conformité dans le temps nécessite des efforts de mobilisation en transverse des équipes, en instantané comme au long cours, mais aussi la diffusion et la mise à jour de l'information »

Le plan d'audit quant à lui organise les audits internes et externes. L'audit interne sert à mettre en évidence des non-conformités, il peut aussi vous entrainer en vue de l'audit externe certifiant. On y retrouvera donc toutes les phases d'un audit certifiant : la revue documentaire, l'interview des porteurs de risques et de mesures de sécurité, le contrôle des salles d'hébergement et la rédaction du rapport.

En conclusion, la conformité n'est un succès que quand les acteurs sont convaincus de l'utilité de leurs actions au quotidien et en constatent le bénéfice. Le management de la qualité nécessite donc de savoir contrôler, maîtriser, prévenir mais aussi motiver et convaincre.

APSSIS

Association Pour la Sécurité des SI de Santé

FORMATION

VERSION 3

RSSI / SSI

Porter la SSI et la conformité numérique : technicité et savoir-faire

EVOLUTIVE 2019-2021

JOUR 1

Cybersécurité Santé
Actualités
Réglementaire
Programme HOP'EN
7h00

JOUR 2

Maîtrise technique et humaine de la SSI Santé
7h00

JOUR 3

Maîtrise du plan d'action sécurité & Atelier technique
7h00

CAHIER SPÉCIAL AUDIT CYBERSÉCURITÉ

PAR MAURO ISRAEL

1. Les concepts et principes de l'audit P. 97 À 101

2. Le déroulement d'un audit P. 102 À 107

3. La check-list de la cybersécurité P. 108 À 109

1. Les concepts et principes de l'audit

La fonction d'audit est fondamentale dans tout système de management pour apprendre de ses erreurs et les corriger. Le plan d'action qui suit l'audit doit être défini et mis en œuvre sans délais. Il s'agit d'un processus continu d'amélioration.

Mauro Israel est manager cybersécurité du groupe Orpea. Il se concentre actuellement sur la conformité et la certification en cybersécurité, de même que sur les plans de continuité d'activité, dans le domaine de la santé. Expert, il intervient depuis plus de 30 ans lors de sensibilisations à la sécurité, effectue des audits de sécurité et du consulting. Il a obtenu les certifications professionnelles de Programmeur de l'Armée Française, Master CNE Novell, Microsoft Certified Professional, proCSSI de l'Université Léonard de Vinci, Master ISO 27001 et Certified Lead Auditor et Implementer, et réalisé plus d'un millier de missions de conseil et d'audit. Auteur de plusieurs livres et articles parus dans de nombreux magazines spécialisés sur la sécurité informatique, Mauro dispense des conférences, entre autres aux Assises de la Sécurité, pour Infosecurity et NetFocus. Il a enseigné la sécurité de l'information à l'Ecole Nationale Supérieure des Télécommunications de Paris, ainsi qu'à la Commission Européenne et à l'Université d'Economie de Lille.

Toute activité humaine est sujette à des erreurs ou « bugs ». « *Errare humanum est* », l'erreur est humaine. Mais… « *perseverare diabolicum* » : l'entêtement (dans l'erreur) devient diabolique. Tout le processus d'amélioration continue et de qualité est issu de cette maxime. Voyons quelles failles de sécurité sont présentes dans le système d'information et trouvons les parades appropriées.

La supervision permanente et les tests d'intrusion permettent de vérifier la sécurité au fil de l'exploitation du système d'information, ou lors de changements majeurs. Inconvénient : l'équipe qui exploite le système le supervise également**.** Il peut donc y avoir négligence ou complaisance. Par ailleurs, le test d'intrusion est lui aussi intéressant, en ce sens qu'il met en lumière les failles de sécurité et vérifie l'aptitude d'un attaquant à exploiter ces failles. Cependant, cela ne concerne pas la vérification de l'organisation et des procédures, mais seulement les scenarii d'une attaque**.**
L'audit complète alors ces deux dispositifs de supervision et de tests d'intrusion, devenant ainsi l'élément le plus important de la vérification de la sécurité. Mais, contrairement à la supervision, son principe fondamental, valable quelle que soit l'activité humaine auditée, implique la séparation des intérêts entre l'auditeur et l'audité. Autrement dit, on ne peut pas être juge et partie.

Cela implique notamment que l'audité (celui qui est la cible de l'audit) ne peut pas être le supérieur hiérarchique de l'auditeur (celui qui effectue l'audit). Imaginez que cela soit le cas. A l'issue de l'audit, l'auditeur émettrait un rapport jugeant du niveau de sécurité, avec des recommandations et un plan d'actions correctives, voire préventives, des problèmes constatés. Imaginez que son supérieur (par exemple le directeur informatique) n'accepte pas ces conclusions et ne mette pas le plan de corrections en œuvre. Quelle est la situation de l'auditeur « subalterne » ? Soit il insiste et il se trouvera en difficulté hiérarchique, soit il ne dira rien et l'audit n'aura donc servi à rien. Cela vous rappelle quelque chose ?
Tous ces rapports d'audit qui ont fini au fond d'un tiroir ?! De même, l'audit ne sert à rien si l'auditeur n'a pas la légitimité de faire appliquer le plan de corrections, qui s'appelle, en fait, « plan de réduction des écarts », comme nous le verrons plus loin. C'est pour cela que les audits en comptabilité-finances sont effectués par des entités externes, indépendantes de l'organisme audité. Il doit en être de même pour l'audit en sécurité.

> « On ne peut pas être juge et partie »

1 Les divers types d'audits

Il existe différentes formes d'audit **:** l'audit de première partie, l'audit de seconde partie et l'audit de tierce partie.
Un audit de première partie est un audit dont le commanditaire est le manager du système à auditer. On l'appelle aussi « audit interne », car il fait partie de la phase « Check » de la roue « Plan – Do - Check - Act » de l'amélioration continue.

Roue de la qualité et de l'amélioration continue

Là nous touchons un point crucial de l'activité humaine : **on ne peut s'améliorer que si on s'aperçoit que l'on a commis une erreur.**
Si on n'audite pas le système, on peut ne jamais s'apercevoir que l'on a commis une erreur. L'audit est là pour vérifier que ce qui avait été prévu a été réalisé correctement.
C'est pour cela que, dans un audit, on parle « d'écart ». Il s'agit de l'écart entre ce qui avait été prévu et ce qui a été effectivement mis en place.

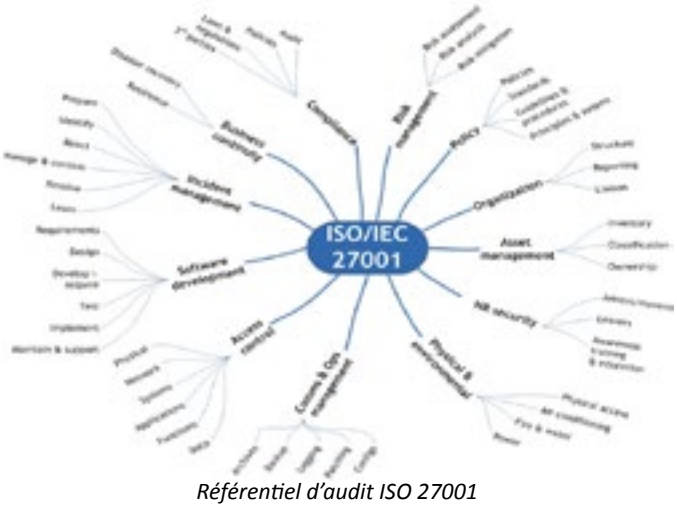
Le plan de correction consiste alors à réduire ces écarts, voire à les empêcher préventivement de se reproduire. Si on n'a plus d'écart, le système est jugé « conforme » et peut donner lieu à une certification, comme ISO 27001, sur le périmètre de ce qui était audité. Pour obtenir cette certification il faut obligatoirement faire appel à un **audit externe, dit « de tierce partie »**, réalisé par un organisme complètement indépendant du commanditaire et habilité par une entité nationale, qui en vérifie la probité et l'indépendance (comme le COFRAC en France : COmité FRançais d'ACcréditation).

Il existe une troisième possibilité : **l'audit de « seconde partie »** mis en œuvre lorsque c'est un client, par exemple, qui invoque sa possibilité d'auditer le système de son fournisseur.

Dans chaque cas, il faut bien comprendre que c'est le commanditaire qui détermine si l'audit est « externe » ou « interne » et non pas les personnes qui le réalisent. Ainsi, il est sage de faire appel à des sociétés externes à l'entité, y compris pour les audits internes, surtout quand le RSSI est hiérarchiquement placé auprès de la direction Informatique, de manière à respecter le principe fondamental d'indépendance de l'audit.

2 Quelques définitions

Chaque fois que l'on vérifie un point (on appelle cela **une exigence**), comme la mise en place d'un élément de sécurité, on appelle cette entité élémentaire un **critère d'audit**. La somme de tous les critères d'audit s'appelle un **référentiel d'audit**.



Référentiel d'audit ISO 27001

Ce référentiel d'audit correspond à toutes les exigences d'une norme, si l'on cherche à suivre les exigences de cette norme. Par exemple, pour être certifié ISO 27001, il faut répondre à toutes les exigences spécifiées dans cette norme (y compris l'annexe A pour les clauses applicables). On peut avoir également des exigences qui proviennent des métiers de l'entreprise, liées à la disponibilité, l'intégrité, la confidentialité des données. On peut y ajouter des exigences règlementaires ou légales, comme, en France, le respect des données personnelles et de la vie privée, ou bien la règlementation sur l'hébergement des données de santé ou des jeux en ligne.

Une simple exigence s'exprime sous la forme d'une phrase du type : « L'entité doit faire ceci ou cela, ou respecter ceci ou cela ». Comment l'auditeur transforme-t-il cette exigence en critère d'audit ? Il faut trouver une preuve que l'exigence est respectée ou pas. Pour trouver une preuve, il faut expliciter une méthode de preuve. Il existe de nombreuses méthodes de preuves, une fois que l'on a compris ce qu'était une « preuve », ou *evidence* en anglais. En lisant l'énoncé de la preuve, le lecteur aussi doit trouver « évident » ce qui est avancé. Autrement dit, **une preuve est un énoncé qui montre la réalité de ce qui est avancé par le jugement : conforme ou pas à une exigence de sécurité.**

> « Le travail de récolte et d'énoncé de preuves nécessite une grande rigueur »

Ce travail de récolte et d'énoncé de preuves nécessite une grande rigueur, car quelquefois on peut nier « l'évidence » si elle est mal rédigée ou mal expliquée.
Nous avons donc trois colonnes dans un audit pour chaque critère : l'exigence, la ou les méthodes de vérification, l'énoncé de la preuve.

L'auditeur juge alors si il y a un écart, ou non, entre l'exigence et les éléments de preuve avancés. L'auditeur a un rôle à la fois d'investigation, de récolte de preuves et de juge. Il est donc fondamental de savoir comment on récolte des preuves valables.

Requirement	Methods and means for verification	Proof of verification
Les principaux processus (ou activités) business du site ont-ils été recensés et un plan de continuité d'activité établi (BCP, Business Continuité Plan) ? Ce plan doit lister tous les IT processes qui sont critiques pour le site et ceux qui peuvent être considérés comme négligeables, en cas d'incident de sécurité. Ces IT processes critiques constituent la base du plan de restauration après catastrophe (DRP,	Vérifier l'existence d'un document BCP ou au moins, d'une liste d'applications avec évaluation des risques.	Liste des applications critiques avec le BCP correspondant.

3 Les méthodes de preuve

Dans la police scientifique, les méthodes de preuve consistent essentiellement à trouver de l'ADN ou des empreintes sur la scène de crime. Mais elle utilise aussi d'autres méthodes, comme les interrogatoires, de manière à créer un « faisceau de preuves » plus à même d'influencer le juge, puisque juge ou jury il y a, dans ce cas. Dans le cas de l'audit comptable, de l'audit qualité ou de l'audit sécurité, l'auditeur dispose de différentes méthodes de preuves.

• « Stick to the ***facts*** ». Il faut s'en tenir aux faits et les faits sont établis par *des procédures écrites et des enregistrements de l'activité ou la lecture de la documentation.* Il s'agit de vérifier que les procédures et les enregistrements (comptes rendus, etc.) sont conformes à ce qui est vérifié. Par exemple, il est exigé que le comité de sécurité analyse les incidents de sécurité chaque mois. On constate que ce comité ne s'est pas réuni depuis trois mois, ou qu'il n'y a aucun compte rendu écrit de cette réunion. C'est un écart. Pire, on s'aperçoit qu'il n'y a pas de comité de sécurité du tout alors qu'il est clairement prévu dans les processus… C'est un écart « majeur ». Ainsi on peut hiérarchiser les écarts en fonction de leur gravité, à condition de le prouver. Quelque chose de « grave » est quelque chose qui met en risque de manière évidente le système qui est audité.

• « ***Act locally*** ». L'échantillonnage constitue une autre façon de recueillir une preuve : allons sur tel poste de travail pour vérifier que les *patches* de sécurité ont été bien installés et sont à jour. On ne va pas aller sur tous les postes mais sur un « échantillon représentatif ». Le gros avantage de l'échantillonnage est de faire gagner un temps précieux. Imaginez d'aller voir un par un les 2 000 ordinateurs de l'établissement ! Il suffit d'en voir quelques-uns, à condition que cet échantillon représente les cas typiques d'ordinateurs de cette organisation ! même système d'exploitation, mêmes logiciels installés. Le tout est de savoir *combien* d'ordinateurs doit comporter l'échantillon. Dans une entité qui a un « master » pour ses postes de travail, quelques unités suffiront. Bien entendu, il faudra aller sur chaque site où de tels ordinateurs sont actifs.

• « Go and talk to the ***people ».*** Ceci permet d'énoncer une règle fondamentale de l'audit et plus généralement de l'activité humaine : allez géographiquement, physiquement, là où se trouve le système audité et parlez avec les gens concernés ! La troisième méthode de preuve consiste donc tout simplement à demander aux personnes concernées et à constater avec ses propres yeux. L'interview (comme l'interrogatoire pour les policiers) est une méthode de preuve valide… jusqu'à preuve du contraire ! Autrement dit, vous pouvez interroger la personne en charge des *patches* : « Installez-vous *régulièrement les patches sur tous les postes de travail ?* ». Elle peut vous répondre « oui », mais cela ne suffira pas pour faire un faisceau de preuves. C'est un bon début qui respecte ce principe fondamental : « Demandez aux gens concernés par le problème ».

• « Show me ». Ceci nous amène à la quatrième méthode de preuves : « Montrez-moi la console qui permet d'envoyer les patches sur les machines, de manière à voir s'il n'y a pas eu d'erreurs ». Il s'agit de s'aider d'outils liés à l'exploitation informatique ou à des consoles d'outils de sécurisation. Bien entendu, comme pour les preuves précédentes, il faudra noter les réponses ou bien faire une copie d'écran, comme preuve. Le fait de mettre dans un rapport : « oui j'ai vu l'écran, c'est bon », n'est pas une preuve ! Encore pire : Le fait de cocher juste « oui » dans un rapport.

• « Experts at ***work*** ». La cinquième méthode consiste à utiliser des outils de vérification de la sécurité. Par exemple, nous voulons savoir si des données sensibles circulent « en clair » sur le réseau. Pour cela, nous installons temporairement un outil de sonde réseau, en évitant de gêner ou de bloquer le travail des utilisateurs. Nous choisirons l'outil en fonction de sa fiabilité et de notre connaissance de son utilisation, évitant ainsi des dénis de service. Ce cinquième élément de preuve est plutôt l'affaire de personnes qui s'y connaissent en informatique en général et en sécurité en particulier. Si l'auditeur n'a pas ce profil, il peut se faire aider d'un spécialiste (réseaux, systèmes, bases de données), voire demander à l'audité s'il a ce type de compétences dans son équipe.

Ces cinq éléments de preuve nous montrent clairement **ce qu'il ne faut pas faire** pour avoir une idée du niveau de sécurité d'un système :

- demander à l'audité de faire lui-même l'audit,
- se contenter de déclarations à distance comme un email ou une grille Excel,
- répondre à une exigence par « oui » ou « non », sans apporter de preuves liées à cette réponse,
- prendre un échantillon qui « arrange » le résultat. Je reviendrai sur ce point un peu plus loin,
- considérer les déclarations orales comme étant valables sans preuve écrite de l'activité (compte-rendu, check-list, etc.)
- mais le pire de tout est de ne pas vérifier la sécurité concrètement et de se contenter de vérifier que les procédures sont documentées. Ce que je veux dire ici c'est que **l'audit vérifie une conformité à un référentiel**. Si ce référentiel et ces critères d'audit posent les « mauvaises questions », on ne sera pas plus avancé, même si le système est jugé « conforme ».

> « Si le référentiel est biaisé ou incomplet, l'audit le sera aussi »

4 Les référentiels

Le plus simple pour concevoir un référentiel d'audit en sécurité est de s'appuyer sur la norme ISO 27001. Notez bien que ceux qui ont écrit la norme étaient conscients qu'il ne suffisait pas de vérifier le système de management de la sécurité (clauses 4 à 10 de l'ISO 27001:2013) ; ils ont alors ajouté une annexe qui contient les fameuses 114 bonnes pratiques de sécurité réparties sur 35 thématiques. Ces 114 bonnes pratiques font l'objet d'une norme détaillée appelée ISO 27002. Encore faut-il transformer ces bonnes pratiques en exigences pertinentes par rapport au métier et aux risques associés. Le point fondamental à comprendre ici est que **l'audit ne vérifie qu'une conformité par rapport à un référentiel.**

Si ce référentiel est biaisé ou incomplet, l'audit le sera aussi. Notez également que l'audit de conformité n'est pas le seul type d'audit : on peut demander un **audit d'opinion**, qui fait un état des lieux de la sécurité par rapport au bonnes pratiques liées au métier et à son exposition à Internet et/ou à la compétition économique. Ce type d'audit est très intéressant quand le management veut faire une « levée de doutes » : par exemple , dans une situation où la direction informatique, ou le RSSI, disent que « tout va bien » alors qu'un piratage retentissant vient d'avoir lieu. Il est également valable de faire ce type d'audit quand on « bascule » son métier sur Internet ou quand on dématérialise des processus ou des services :

Domaine d'évaluation	Niveau de conformité	Constats
Contrôle d'accès	✔	*La salle machine principale se situe à côté du bureau des administrateurs. Afin d'y accéder, il est donc nécessaire de rentrer dans ce bureau qui dispose d'un contrôle d'accès par badge. La porte de cette salle machine n'est pas fermée à clé. Il s'agit d'une porte simple en forme « baie vitrée ». Les badges sont nominatifs et les habilitations sont demandées suivant un process bien défini. L'ensemble de la salle machines est contrôlé par un mécanisme de surveillance vidéo (caméra IP).*
Détection et protection incendie	✔	*Le système de détection d'incendie est basé sur des détecteurs de fumée au plafond. Des extincteurs sont disponibles dans cette salle.*
Protection inondations	✔	*Le bâtiment hébergeant les serveurs n'est pas situé en zone inondable. Des bouches d'évacuation ont été identifiées.*
Climatisation	✔	*Deux climatisations indépendantes sont actuellement installées dans la salle machines. Celles-ci sont alimentées par le générateur, en cas d'arrêt électrique.*
Installation électrique	✔	*Un groupe électrogène existe afin d'assurer une autonomie de 2 heures en cas de perte d'alimentation électrique.* *Deux onduleurs sont installés dans la salle machines principale (onduleurs Merlin Gerin)*
Câblage	✔	*Le câblage est globalement bien réalisé avec un étiquetage correct.*
Organisation de la salle	ECART	*La répartition des baies est organisée sous forme de silos fonctionnels (ESX, sauvegardes, réseau, SAN, etc.) permettant ainsi de regrouper les équipements et d'optimiser les opérations de maintenance. A noter toutefois que les baies de stockage sont ouvertes et nous avons identifié un DONGLE USB branché sur un serveur (licence) par un prestataire (aucune vérification n'a été réalisée).*

Exemple de référentiel d'audit avec preuves

5 Le déclenchement de l'audit

Les audits se déclenchent différemment en fonction du commanditaire. Si l'audit est interne de « première partie », il fait partie du cycle habituel d'un programme d'audits. On essaie de couvrir la totalité des critères d'audit sur un an. Le déclenchement est fait par le RSSI ou par le département d'audit interne suivant une planification préétablie. Notez bien qu'un audit n'est pas une « descente de police » **: l'audité doit être informé à la fois des dates et du contenu de l'audit (le référentiel**). Il doit être en mesure de le préparer. J'ai coutume de commencer tous mes audits lors de la réunion de lancement par : « Nous venons pour vous aider, nous sommes avec vous, pour que vous puissiez vous améliorer, nous sommes de votre côté ».

Si l'audit est externe, de « seconde partie », il est déclenché typiquement par le client qui voudra vérifier la sécurité, de son hébergeur par exemple. Cet audit peut être impromptu si cela est prévu dans le contrat. Il ne peut pas « déborder » sur autre chose que le périmètre, le plan d'audit et les critères d'audit qui ont été préalablement définis. C'est de la responsabilité des auditeurs de prévenir l'audité s'ils s'aperçoivent d'une faille de sécurité qui peut impacter la totalité de leurs clients, au-delà du client qui est le déclencheur de l'audit. Notez bien que l'on ne peut pas déclencher un audit chez un sous-traitant si on n'a pas explicitement prévu cette clause dans le contrat. Vous ne pourrez pas déclencher un audit chez Google ou Amazon, parce que vous avez acheté un hébergement de vos documents dans le cloud pour 10 euros par mois !

Enfin, **si l'audit est de tierce partie**, c'est l'organisme en charge de la vérification du système qui déclenche l'audit suivant un programme défini à l'avance. La plupart des audits de certification ayant une validité de trois ans, il y a un audit initial, puis des audits de surveillance, tous les ans ou tous les six mois. Il peut y avoir également des audits de levée d'écarts lorsque l'audit précédent s'est soldé par des non-conformités que l'audité s'est engagé à résoudre rapidement. L'audit porte alors uniquement sur les non conformités non résolues initialement. Bien entendu, l'organisme auditeur définit la date de l'audit avec l'audité et établit un plan d'audit d'un commun accord. Les seuls à pouvoir faire des audits de manière impromptue, sont les entités étatiques comme la CNIL (Commission nationale de l'informatique et des libertés), qui intervient notamment sur plainte, pour vérifier le respect de la vie privée dans le système d'information.

Un référentiel pertinent

Supposons un centre d'appels de service après-vente. Le critère d'audit concerne la vitesse de réponse à un appel, exprimée en nombre de sonneries avant de décrocher. On estime, en général, que la vitesse optimale est de trois sonneries. Mais, dans ce site, on a estimé que le nombre optimal de sonneries avant de décrocher était de… 12 ! Quand l'audit a lieu, en regardant les logs du logiciel de réponse aux appels on s'aperçoit que 100% des appels ont reçu un décrochage téléphonique avant 12 sonneries. Le système est donc conforme. En réalité, en choisissant 12 sonneries l'audité a enfreint les bonnes pratiques. Le plus important dans un audit est donc de faire en sorte que le référentiel respecte les bonnes pratiques dans une fourchette raisonnable et adaptée au métier. Une activité d'urgences hospitalières ou de lutte contre les incendies aura des critères beaucoup plus exigeants que les sociétés qui vendent des pelotes de laine… Autrement dit, les critères d'audit dépendent du métier. Il faut donc parfaitement connaître le métier pour concevoir un référentiel d'audit pertinent.

2. Le déroulement d'un audit

Tout ce qu'il faut savoir pour être (ou devenir) un bon auditeur, de l'étape de planification au traitement des informations recueillies et à la clôture de l'audit, en passant par la préparation, la conduite des réunions et entretiens de visite, la récolte et l'examen des preuves… sans oublier le plan de correction.

Une fois que la décision de faire un audit est prise, il faut élaborer un plan. Cette étape est valable quel que soit l'audit et quelle que soit l'activité.

1 Le plan d'audit

Il comprend sous forme synthétique les éléments suivants :

- **Objectifs** : pourquoi fait-on cet audit ? Pour vérifier la conformité par rapport à un référentiel, aux bonnes pratiques, faire une « levée de doute », avoir une opinion sur le niveau de sécurité, vérifier la résistance du système aux attaques de piratage, faire un état des lieux de la situation et/ou de l'avancée des chantiers, faire une enquête sur un piratage avéré, sur un incident de sécurité, sur une fuite d'informations…
- **Champ et critères** : le champ d'un audit indique l'angle de l'audit, dans notre cas, un audit de sécurité du système d'informations. On peut coupler un champ « sécurité » avec un champ « qualité » (ISO 9001), performance informatique (ISO 20000-1) ou « environnement » (ISO 14001), pourvu que les systèmes audités soient homogènes, notamment au niveau de leur périmètre. On dénomme ces audits, des **audits combinés**. Si plusieurs sociétés d'audit interviennent en même temps, on appelle cela un **audit conjoint**. Les critères d'audit (exigences) doivent être explicités, un par un, en général sous forme de questionnaire. Afin d'éviter d'alourdir le document, on peut faire figurer le questionnaire dans un document annexe, en spécifiant la référence, par exemple: Referentiel_audit_ISO 27001_XYZ. Celui-ci peut également faire référence à la norme dont il s'inspire ou carrément indiquer qu'il s'agit, de manière exhaustive, de toutes les exigences d'une norme. On dénomme parfois ce document « déclaration d'applicabilité », c'est à dire que l'on indique, parmi la liste complète des critères d'audit d'une norme comme ISO 27002 (il y en a 114), lesquels ont été intégrés dans l'audit.
- **Périmètre technique et organisationnel** : Il s'agit de déterminer le périmètre que l'on va vérifier. Le périmètre est défini sous forme géographique, les sites visités, les personnes interviewées (leur rôle), les systèmes et réseaux concernés, les applications, les services, etc. Il est important de définir correctement le périmètre d'audit, car un auditeur ne peut pas « sortir » de ce périmètre initialement prévu, sauf, une fois encore, dans le cas de l'Etat, lorsqu'il dispose de prérogatives judiciaires. Ainsi, lors d'un audit de certification, celui-ci ne peut s'appliquer qu'au périmètre défini par l'audité. Autrement dit, la définition d'un périmètre clair et homogène est fondamentale dans le processus de certification.

2 Dates, lieux, équipe

L'audit ne peut pas être impromptu : les dates et le lieu doivent être fixés à l'avance entre les auditeurs et les audités. On ne peut pas intervenir par surprise, sauf si c'est clairement prévu contractuellement (audits de seconde partie). A part une action judiciaire, les audits ont, dans l'intérêt de l'audité, un préavis, ce qui permet à l'audité de préparer correctement l'audit : récupérer toutes les preuves, documentaires ou autres, liées aux questions posées lors de l'audit et mettre en place des mesures correctives rapides, dans le cas d'un oubli ou d'une négligence.

> « La définition d'un périmètre clair et homogène est fondamentale dans le processus de certification »

Informations sur les réunions de démarrage et de clôture. Tout audit commence et finit par une réunion. Il faut fixer, dès la réunion de démarrage, la date et l'heure de la réunion de clôture sur site, de manière à restituer toutes les non-conformités à l'audité. La réunion d'ouverture est fondamentale, car elle explicite à l'audité sur quoi va porter l'audit et comment cela va se passer. Comme les humains ont peur de l'inconnu, cette réunion est une bonne occasion, surtout quand c'est la première fois que l'audité *subit* un audit, de dédramatiser la situation (du moins dans l'esprit de l'audité). La bienveillance est ainsi une qualité fondamentale des auditeurs.

Information sur l'équipe d'auditeurs et des audités. Les membres de l'équipe d'audit doivent être présentés. Ils ne peuvent pas être anonymes et s'engagent personnellement en signant les éventuelles fiches d'écart. Cela permet de savoir qui a fait quoi et de retrouver les preuves en suivant la même piste d'audit (le même questionnaire), ce qui est fondamental pour la crédibilité des résultats exposés.
Il peut y avoir d'autres types de personnes qui assistent à l'audit, à part les auditeurs : il s'agit des **guides**. Ceux-ci, notamment dans le domaine industriel, facilitent la visite des sites et permettent notamment le respect des consignes de sécurité physique. On peut également avoir des guides qui servent de traducteurs, car l'anglais dans certains pays est très approximatif par rapport aux besoins de l'audit.
Il peut également y avoir des **observateurs**. Il s'agit de personnes qui n'interviennent pas dans l'audit proprement dit, mais qui sont des « témoins » de ce qui se passe. Souvent un manager métier voudra être témoin de ce qui se passe dans son département, pour mieux comprendre la situation.

La seule règle est que ces personnes ne peuvent pas intervenir dans les réponses apportées. Si elles ne peuvent pas s'empêcher d'intervenir, on notera leurs réponses en modifiant leur statut d'observateur à **interviewé**.

3 Les contraintes à observer

Confidentialité des données collectées et anonymisation des résultats. On imagine facilement que les *findings*, ce qui a été trouvé lors d'un audit, peuvent être gênants pour l'audité : failles de sécurité, énumération des vulnérabilités ou des négligences. Il est donc fondamental pour l'organisme d'audit de garantir la confidentialité des données récoltées. On réalise cela lors de la signature nominative par chaque auditeur d'une Déclaration de Confidentialité (NDA en anglais – Non Disclosure Agreement). Pour ma part, *je n'emporte jamais aucun document qui m'a été remis pour vérification*, ni sur mon ordinateur, ni sous forme papier. Lors de l'établissement de la preuve, je fais simplement référence au document en mentionnant sa référence dans le système documentaire ou à la personne interviewée, en mentionnant son rôle organisationnel (mais pas son nom) de manière à respecter l'anonymat des personnes. On aura, par exemple, la preuve suivante : « L'interview avec la personne en charge des backups et une vérification physique dans la salle A31, *ont permis d'établir que la procédure de stockage des supports de backup ref XYZ-23 a été suivie correctement sur les échantillons vérifiés correspondant à avril 2014 et août 2013.* »

Contraintes d'exploitation de l'audité. L'audité doit pouvoir continuer à travailler lors d'un audit sans pratiquement aucune perturbation. Il faut donc s'assurer que l'équipe d'auditeurs respecte les horaires d'ouverture du site, les moments où le système d'information est absolument crucial et où les personnes à interviewer ne sont pas dans une période de charge de travail intense (clôture de fin de mois, etc.). Un audit doit faire en sorte de gêner le moins possible, voire pas du tout, le travail courant.

Obtention de la documentation sécurité existante. Pour cela, il faut lister tous les documents qui vont être vérifiés lors de l'audit de manière à laisser à l'audité le temps de les récolter dans son système. Il existe plusieurs manières de fournir un document à un auditeur. La manière la plus basique est de fournir les documents au fur et à mesure du questionnaire, sous forme papier. Plus l'audité prend de temps à sortir le document, plus je pense qu'il a mal préparé l'audit. C'est donc un bon point pour l'audité de bien préparer tous ses documents dans un classeur, dans l'ordre du questionnaire. Mais on peut faire mieux : Il suffit de préparer des liens qui vont afficher le document, directement à partir du système documentaire, sur un vidéo projecteur. Du coup, on comprend que l'audité doit avoir préparé aussi une logistique pour les auditeurs : salle fermée physiquement et acoustiquement, disposant d'un accès au réseau (pour les audités) avec les droits suffisants pour avoir accès à la base documentaire et aux différentes consoles de sécurité. Plus la réponse est rapide, plus l'auditeur sera impressionné favorablement.

Les documents à vérifier

Réunion formelle de lancement. Le lancement de l'audit est toujours marqué par une réunion formelle entre auditeurs et commanditaire, portant sur les modalités de la prestation, notamment en passant en revue tous les points du plan que nous venons de voir et la logistique de la prestation. Il y a lieu également de sensibiliser les audités sur la volonté de ne pas gêner ou de provoquer un déni de service sur l'exploitation, mais « on ne sait jamais »… Notamment pour le cas particulier des « tests d'intrusion ».

Autorisation explicite de test d'intrusion. Dans le cas d'un test d'intrusion, on enfreindrait la loi de manière délibérée puisqu'il s'agit d'une tentative explicite d'intrusion dans un système d'information. La loi punit, en France, ce type d'activité (même si on ne parvient pas à pénétrer le système) : jusqu'à cinq ans de prison et 300 000 euros d'amende pour « tentative d'intrusion dans un système de traitement informatisé ». L'audité doit donc « explicitement » donner l'autorisation aux auditeurs, que l'on appelle dans ce cas des *pentesteurs*, de tenter de « pénétrer » le système. Comme cela peut finir en déni de service ou en révélation de failles de sécurité, il est fondamental que l'audité dispose de la capacité juridique pour donner cette autorisation.

4 La préparation

L'équipe d'audit doit être quantitativement suffisante pour permettre de couvrir la totalité du questionnaire dans les délais prévus. Il vaut mieux être au minimum deux (comme les policiers), car les techniques d'interview et de

récolte de preuves demandent à la fois une bonne faculté d'observation, mais aussi une grande capacité à prendre des notes. Aussi, il est difficile à la fois de parler, de poser des questions et de noter les réponses de manière détaillée. On peut également adjoindre à l'équipe un ou plusieurs spécialistes qui vont pouvoir mettre en œuvre des outils techniques ou comprendre le contenu des consoles ou des journaux de logs.

Planning et rendez-vous. Avant de commencer la visite sur site, il faut la préparer, d'autant plus que le lieu de l'audit peut être situé à des milliers de kilomètres du bureau des auditeurs. Il y a donc à la fois une préparation logistique (voyage, hôtel, déplacements locaux) et une préparation de l'agenda : par tranches horaires, quelles activités auront lieu et avec qui, par exemple : *Jour 1 - 9h réunion d'ouverture – 9h45 analyse des documents du SMSI – 12h pause-déjeuner – 13h15 interview RH – 14h interview DSI, etc.*
Il faut également veiller à ce que chaque interlocuteur soit prévenu de la visite et soit disponible suivant l'agenda défini. Il ne faudra pas hésiter à changer l'agenda pour s'adapter aux contraintes d'organisation de l'audité.
Il est fondamental de demander au commanditaire de vous organiser l'agenda des rendez-vous avec ses collègues, car vous n'aurez aucune légitimité à appeler vous-même. De même, en début d'interview, le responsable de l'audit côté « audité » fera une brève intervention pour expliquer à l'interviewé dans quel cadre et pour quelle raison il est interviewé.

L'élaboration du guide d'entretien. Un entretien ne doit pas être improvisé : il faut établir à l'avance quelles questions vont être posées et à qui. Pour cela, il est intéressant de réorganiser le questionnaire d'audit en catégories, par exemple : Ressources Humaines, Direction Informatique, sécurité physique, services généraux, juridique, etc.
Pour chaque question, on aura préparé les réponses typiques de manière à pouvoir évaluer la maturité de la réponse, et également sa pertinence, en la croisant avec d'autres méthodes de preuve.

Collecte et analyse des documents. La première partie de l'audit consiste à collecter et analyser les documents fournis en lien avec le périmètre de l'audit. Il y a plusieurs types de documents : les documents d'organisation, les procédures, les chartes et documents juridiques, contrats, les journaux d'activité, les comptes rendus de réunions, de tests ou d'actions, les registres de signature, les présentations (diaporama), etc. Tout ce qui contribue à prouver l'exigence de manière écrite est bon à analyser. Une fois le travail d'analyse documentaire terminé, on peut passer à la deuxième partie de l'audit dénommée visite sur site, ce qui inclut également les interviews des parties prenantes du côté de l'audité.

Conduite des entretiens. De même qu'un entretien ne s'improvise pas, la façon de se comporter pendant un entretien ne s'invente pas : le ton de la voix et le débit doivent être maitrisés. **Il faut être rassurant et non pas inquisiteur.** Il est important de partir de questions relativement génériques pour mettre à l'aise l'interviewé. Par exemple : « Pouvez-vous me décrire votre activité ? ». Puis aller plus avant dans le sujet : « Qu'est-ce qui vous pose problème en matière de sécurité ? ». Ou bien : « Avez-vous souvenir d'incidents ou de problèmes de sécurité, récemment ? ».
Votre questionnement doit être semi-ouvert, c'est-à-dire qu'il permet à votre interlocuteur de s'exprimer autrement que par « oui » ou par « non », mais qu'il ne lui permet pas de sortir du sujet. Il y aura ainsi deux ou trois questions pour couvrir une exigence.

L'entretien : un exemple

Vous souhaitez vérifier que les données sensibles ne circulent pas en clair sur le réseau local. La première question à la personne en charge de la sécurité des réseaux peut être : « Avez-vous identifié les flux qui circulent sur votre réseau ? ». Si la réponse est « non », demandez pourquoi ou reformulez la question : « Vous avez des flux http, je suppose ? ». Il ne faut pas hésiter à reformuler pour laisser une chance à l'audité de développer une bonne réponse. Surtout en début d'entretien et avec des personnels plutôt techniques, il y a de fortes chances que la personne réponde « mal », tout simplement pour cause de stress. Si vous voyez que la réponse n'est pas probante, il faut essayer d'autres pistes, par exemple : « Avez-vous une sonde qui identifie les flux réseau ? » Vous pouvez même citer des outils, comme Etherreal (Wireshark). Il se peut que le spécialiste vous réponde alors « oui », ce qui montre que la formulation de la question ne lui était pas accessible. Vous pouvez également expliquer « pourquoi » vous posez cette question. Dans notre exemple, il s'agit de repérer les flux de données en clair et plus précisément les données sensibles comme les mots de passe. En effet, en interceptant les mots de passe sur un réseau on peut, comme avec l'attaque dite « Man in the middle », récupérer le mot de passe et donc se faire passer pour l'utilisateur dans l'application ou la base de données concernées.
Il ne faut pas se contenter d'ailleurs d'une réponse positive. Il faut prolonger la question par « Comment faites-vous ? », « Montrez-moi » etc., ce qui nous amène aux autres moyens de preuve, hormis la documentation et les interviews.

5 La visite sur le terrain et l'examen des preuves

Pour confirmer ce qui est indiqué dans la documentation il faut visiter le site concerné. Il ne s'agit pas de vérifier chaque machine, chaque logiciel, sinon il faudrait un temps incompatible avec le temps imparti. De plus, ça serait fastidieux et redondant. Il faut **catégoriser le**

recueil d'informations pour que chaque catégorie éclaire et complète les réponses que vous avez eues dans la phase statique de l'audit. En effet, alors que la lecture de la documentation et les interviews se sont plutôt déroulées dans un bureau dédié à l'audit, maintenant nous sommes en mouvement, auditeurs et audités en « visite » sur le site. Afin de ne pas partir au hasard, il faut convenir avec le commanditaire d'un **plan de visite**. Typiquement, on trouvera la salle serveurs (datacentre), quelques postes de travail bureautiques, deux ou trois postes métier (s'ils font partie du périmètre), comme les RH ou les admin IT. Les consoles de supervision IT et sécurité (anti-virus, firewall, IPS, WSUS). On voudra également voir différentes configurations : Windows XP, Seven, 8.1, W10, Linux, etc. On vérifiera un ou deux serveurs (virtuels ou pas) et deux ou trois stations de chaque catégorie. On regardera également les supports amovibles, les smartphones…
Le but de cette visite est de recueillir des informations qualitatives, des échantillons quantitatifs et de consolider ces données en preuve.

> « Les écarts doivent être indiqués à l'audité au fur et à mesure de l'audit »

Le point clef de ce travail est la définition de l'échantillon et son caractère « représentatif ». Si, par exemple, vous avez 1 000 ordinateurs sous Windows 7, que vous en vérifiez trois au hasard et qu'ils ont tous leur anti-virus à jour, est-ce que cela prouve que la totalité des ordinateurs l'ont ? Bien sûr que non. Mais si « couplé » à cela on vous montre une console antivirale de centralisation de diffusion des mises à jour et que cette console affiche qu'il n'y aucune anomalie, vous avez alors une preuve, un « faisceau de preuves concordantes », comme disent les juristes.
Et si ce n'était pas le cas ? Si, parmi les trois machines inspectées, l'une d'entre elles a une ancienne version de la base antivirale ? Alors que dit la console ? Si la console dit que tout va bien, cela pose problème. Il faut regarder ce que raconte la console d'administration à propos de cette machine. Vous allez forcément trouver une explication et donc définir que vous avez la preuve d'un « écart » entre ce qui était supposé être et ce qui était réellement. On appelle ce type d'écart, un « écart d'application ». Alors que, lors d'une distorsion entre ce qui est exigé par la norme et l'absence ou l'insuffisance du document, on l'appelle « écart documentaire » ou « écart d'intention » (c'est-à-dire qu'on avait l'intention de faire le document, mais qu'on ne l'a pas fait, comme par exemple le compte rendu d'un comité sécurité).

Point crucial dans le recueil et la formalisation des écarts est le suivant : tous les écarts doivent être indiqués à l'audité au fur et à mesure de l'audit. Il faut documenter la raison de l'écart et l'audité peut très bien intervenir en disant qu'il n'est pas d'accord, soit sur le fait qu'il y ait un écart, soit sur sa gravité. Comme nous avons des écarts « majeurs » ou « hauts », qui mettent en cause de manière directe et urgente la sécurité du site, et des écarts « mineurs » ou « bas » qui ne permettent pas d'en déduire une mise en cause rapide et forte de la sécurité, l'audité peut très bien contester le caractère « grave » de l'écart. Reprenons notre exemple. Supposons que la base antivirale ne soit pas à jour et que la console ne l'ait pas « vu ». Il y a deux possibilités : l'ordinateur a été déconnecté un certain temps du réseau (cas fréquent pour les ordinateurs portables des personnels « nomades »). Du coup la console affiche une information obsolète. Il s'agit d'un écart mineur, car la sécurité du site ou de la machine n'est pas compromise ; Il ne faut pas crier « au feu !» à chaque fois que vous faites cuire une pizza dans votre four à micro-ondes… Ou bien, on s'aperçoit en réalité, après investigation plus poussée, que cette machine est bel et bien contaminée par un virus, qui d'ailleurs a commencé son activité maligne par déconnecter les mises à jour de l'antivirus, donc la console… Du coup la console ne peut plus se connecter à cette machine et si cela s'est produit il y a plusieurs semaines, il s'agit d'un écart « majeur ». Pourquoi cela ? Parce qu'en réalité on s'aperçoit que le processus de lutte antivirale a dysfonctionné. La plupart des utilisateurs croient qu'il suffit d'installer un anti-virus performant pour que l'affaire soit close. Les anti-virus ne sont pas parfaits, même à jour. Il faut donc surveiller le parc de manière attentive et journalière. Ceci n'a pas été fait, il s'agit donc d'un écart majeur, car une machine contaminée depuis plusieurs semaines peut affecter la sécurité de tout un système : c'est comme le Cheval de Troie : une fois que l'ennemi est à l'intérieur de nos murailles, il lui est très facile de nous attaquer.

> « C'est un travail à deux parties - l'auditeur et l'audité - et non pas une enquête de police avec un «gardé à vue» »

En synthèse, il faut bien **documenter chaque écart et l'audité peut argumenter.** Il s'agit d'un travail à deux parties : l'auditeur et l'audité, et non pas une enquête de police avec un « gardé à vue ». Certains auditeurs ont tendance à l'oublier et avoir une attitude un peu arrogante ou condescendante vis-à-vis des audités. C'est contre-productif, aussi, nous allons en profiter pour voir quelles sont, à mon sens, les qualités d'un auditeur.
Comme un auditeur se doit d'être impartial, sa principale qualité sera de s'attacher aux faits « stick to the *facts* » et de là, ne pas faire d'inférences. Une *inférence* est un raisonnement qui à partir d'un certain nombre de réalités en déduit une « vérité ». Un exemple célèbre d'inférence est : « Je ne vois pas plus loin que l'horizon de la mer. La terre s'arrête donc là. Il n'y a plus rien après. ».
Les marins s'étaient déjà rendu compte du « bug » dans le raisonnement, puisque lorsqu'ils quittaient la terre ferme au bout d'un moment, ils ne voyaient plus la terre mais

l'horizon de la mer était toujours là. Il intervient alors un autre élément dans les inférences. *Il s'agit des croyances et des mythes*. Chaque humain, et les auditeurs sont des humains, baigne dans un réseau, un référentiel de croyances. Ainsi les humains au Moyen Age croyaient que la terre était plate –puisqu'ils la voyaient telle- et que la religion leur disait cela. Leur croyance était établie. Lorsque des scientifiques ont mesuré la courbure de la terre et compris ainsi le phénomène de l'horizon, on les a exécutés en place publique, puisque contraires aux croyances. Cela nous donne deux autres qualités d'un auditeur : Il faut récolter des preuves par l'analyse technique (outils, analyse de logs) et il ne faut pas s'en tenir aux croyances, mais uniquement aux faits. Du coup, il faut être opiniâtre lorsque vous avez des preuves pour justifier votre raisonnement.

Croyances et inférences

Voyons un exemple de croyances et d'inférences et comment l'auditeur doit s'en accommoder. Tout le monde a entendu la croyance selon laquelle les systèmes Windows sont « troués » et Linux est sécurisé « par essence ». Et bien ce mythe, cette croyance est fondée sur le fait que de nombreux piratages ont eu lieu sur des systèmes Windows, notamment des stations de travail. En auditant un système Windows, vous pouvez très bien déduire par inférence : « à quoi bon tenter de sécuriser ce système, puisque de toute façon il sera piraté ?! ». Les croyances et les inférences du coup font bon ménage. En fait, n'importe quel système qui n'est pas patché est vulnérable. Le fait que Windows soit autant piraté tient au fait qu'il a quasiment le monopole des postes de travail. Dans un autre domaine comme les smartphones, c'est IOS et Android qui dominent et les pirates s'y attaquent car c'est un « mass market » plus intéressant. Dès qu'un système « réussit », il attire les pirates.
Autrement dit, si vous êtes un auditeur qui agit par inférences et croyances, vous n'allez pas vérifier que les stations sous Windows ont leurs correctifs de sécurité bien à jour, alors que si vous êtes un bon auditeur qui se concentre sur les preuves et les faits, vous allez vérifier si le système de patches est bien à jour. C'est une grande différence de comportement.

Un bon auditeur s'en tient aux faits, n'est pas influencé par ses croyances et ne fait pas d'inférences. Mais ce n'est pas encore suffisant pour faire un bon auditeur. Il faut également savoir travailler avec les échantillons. Même avec la lecture de la documentation, il faut échantillonner, lire en diagonale, car il serait trop long de lire la totalité de la documentation. De même pour le nombre de composants du système d'informations. On ne peut pas vérifier, une par une, dix mille machines. Il faut donc être capable d'observer correctement un système complexe. Le « déjà vu » s'applique pleinement aux auditeurs. En connaissant bien les systèmes d'informations, on va pouvoir analyser de manière pertinente avec un échantillon valable, en allant « là où ça fait mal ». Des qualités d'observation et d'expertise du système audité s'ajoutent. Enfin, l'auditeur doit avoir des qualités de communication, que ça soit lors des interviews, des réunions d'ouverture et de clôture, de la restitution des audits. Ces qualités doivent s'exprimer de manière à la fois écrite et orale.
Ceci nous amène à un point fondamental de l'audit qui pèse sur de nombreuses entreprises surtout par rapport aux audits comptables ou environnementaux, mais qu'on peut retrouver parfois dans les audits de sécurité. Il s'agit de la manipulation des échantillons.

6 Le traitement des informations recueillies

Une fois que l'on a compris qu'il était impossible de tout vérifier, la taille et le choix de l'échantillon revêtent une importance décisive. Voici un exemple. Prenons un échantillon initial de 30 machines. Sur ces 30 machines, deux ont leurs patches qui ne sont pas à jour. Que faire alors ? Il faut voir les caractéristiques de ces deux machines : Disposent-elles du même système d'exploitation ? Sont-elles des machines nomades ? Si oui, vérifions d'autres machines du même type. Sont-elles toutes « en retard » sur les patches ? S'agit-il du même retard ? Si oui, nous avons un scenario d'écart. Si non, il faut essayer de comprendre pourquoi ces machines ne sont pas mises à jour. Quel est le lien entre elles ?
Le traitement des informations recueillies est fondamental pour que l'audit et la formulation des écarts soient pertinents. Inversement, je vais vous indiquer comment des auditeurs peu scrupuleux –et c'est un euphémisme dans le domaine comptable ou environnemental, comme nous l'avons appris récemment lors du contournement des normes anti-pollution des véhicules diesel - manipulent les échantillons pour obtenir le résultat « désiré ».
Supposons un audit de la qualité de l'eau. Il y a eu des prélèvements pendant un mois, tous les jours le matin à 6 heures et le soir à 21 heures, à trois endroits différents. Le taux moyen de nitrates sur les 180 échantillons est de xxx par litre d'eau. Ce taux est inférieur à la norme, donc « c'est bon », mais pas « fantastique ». Si on y regarde de plus près, on s'aperçoit que les prélèvements à l'endroit A, sont en moyenne bien meilleurs. Il suffit alors de ne considérer dans l'étude que l'échantillon provenant de l'endroit A pour obtenir les résultats espérés.

> « Il y a trois types de mensonges : les petits mensonges, les gros mensonges… et les statistiques (Mark Twain) »

Encore pire : Prenons le cas de l'audit comptable. Dans l'échantillon de 50 écritures, 25 sont conformes et 25 ne le sont pas (manque de justificatifs, écriture erronée,

mauvaise affectation de compte, etc.). La comptabilité devra normalement être rejetée ou, au moins, sérieusement remise en question. Que peut faire l'auditeur peu scrupuleux ? Il requalifie son échantillon. Il reprend les 25 écritures correctes et ajoute à l'échantillon une ou deux écritures incorrectes, mais facilement rectifiables (des écarts mineurs). Ainsi on obtient une comptabilité validée, mais avec un échantillon de 27 écritures. Vous commencez à comprendre pourquoi des sociétés font faillite, alors que les commissaires aux comptes ont validé leur bilan pendant des années, ou que des bateaux coulent, alors que l'audit leur avait donné l'autorisation de naviguer, ou bien que des bâtiments s'effondrent… Bien entendu il y a une part d'impondérables, de risque dans toute activité humaine, cependant la base de la transparence et la crédibilité de l'audit doivent provenir de la **démonstration de l'indépendance entre l'auditeur et l'audité.**

L'auditeur doit faire preuve d'intégrité en ne changeant pas l'échantillon pour aboutir au résultat escompté par l'audité. Comme disait Mark Twain : « Il y a trois types de mensonges : les petits mensonges, les gros mensonges… et les statistiques. ».

Un échantillon – qui est une forme de statistique - peut être interprété et manipulé comme on veut, pour arriver à démontrer quelque chose. La conséquence pour l'auditeur est une forme d'humilité, en plus de son intégrité : « De ce que j'ai pu examiner, avec l'échantillon forcément non exhaustif du système, voici ce qu'on peut affirmer… ».

Analyse et restitution. Chaque écart va alors être analysé avec les notes prises pendant l'audit et évalué avant sa présentation lors de la réunion de clôture. Il se peut que l'écart soit modifié dans sa gravité, par exemple, de « majeur » à « mineur » ou l'inverse. Dans un audit de « maturité » on peut également changer le niveau de maturité en fonction de la réévaluation des preuves. Ce qui est clair, c'est qu'un système audité qui présente au moins un écart majeur au moment de l'audit de certification ne peut pas être certifié. Il faut donc repérer tous les écarts pendant les audits internes et y remédier avant toute tentative de certification. Il est également clair que l'entité qui a effectué les audits internes, voire un audit « à blanc » ne peut pas être celle qui va faire l'audit de certification. C'est comme si votre garagiste habituel vous faisait passer (et obtenir) le contrôle technique !

La réunion de clôture est fondamentale dans un processus d'audit, car elle donne une synthèse à l'audité du résultat de l'audit : les écarts y sont résumés et une tendance est donnée. On explique également ce qui peut être fait, dans quels délais et la capacité que l'audité aura de lever ces écarts, c'est à dire que l'on porte un jugement.
Le rôle de l'audit est d'investiguer, puis de porter un jugement sur la qualité et l'efficacité d'un système.

Formaliser l'audit. Mais la réunion de clôture ne termine pas un audit. Il faut faire un rapport écrit qui reprend chaque critère d'audit et qui met en face la conformité ou l'écart avec la preuve correspondante.
Chaque écart doit être hiérarchisé en « Majeur » ou « mineur » ; On peut aussi avoir des « remarques ». Chaque écart doit susciter une action corrective dans un plan d'actions.

> « Le rôle de l'audit est d'investiguer, puis de porter un jugement sur la qualité et l'efficacité d'un système »

Le plan d'action résume qui fait quoi et comment. Bien entendu, un audit n'a de sens que s'il est suivi d'un plan d'actions. Rappelons-nous que l'audit fait partie de la phase « check » et qu'ensuite, il y a la phase « Act », justement un plan d'actions. En résumé l'audit a pointé les dysfonctionnements du système et le plan d'actions va les corriger.
Peut-on faire mieux que les corriger ? Oui, on peut les prévenir ou les empêcher de se reproduire. Dans un plan d'actions, on aura donc des chantiers de correction (en général assez rapides) et des chantiers de prévention (en général plus longs), qui modifient souvent la structure ou les composants du système.
Nous allons maintenant voir quels sont les points qui « font mal » dans la plupart des audits que j'ai pu mener dans ce domaine, de manière à se concentrer sur des fondamentaux avant d'aller vérifier des points annexes. C'est là où mon expérience me fait « relativiser » la norme, car dans la norme chaque critère est pondéré de la même manière. On peut ainsi avoir un écart sur un point très important du point de vue de la sécurité, qui sera « noyé » au milieu d'écarts peu impactants, en vérité. Ceci est vérifié au point où certaines entreprises certifiées ISO 27001, ont été piratées ensuite, malgré leur certification.
J'en suis arrivé à un référentiel de sécurité basé sur la vérification de points qui sont toujours liés à une sécurité réelle et efficace. Il s'agit d'un audit, mais basé sur les réalités des systèmes d'information. Comme tous les référentiels, il devra évoluer en fonction des nouveaux usages ou des nouvelles failles trouvées par les attaquants. Les menaces environnementales (phénomènes naturels), technologiques (perte d'énergie, défaillance matérielle) et physiques (pénétration dans les locaux, vandalisme, vol) sont laissées de côté, car elles sont normalement déjà traitées par les équipes informatiques et les services généraux. Une sensibilisation des utilisateurs viendra compléter ce dispositif, comme nous verrons plus loin.

3. La check-list de la cybersécurité

Et si l'on instaurait un contrôle technique pour la cybersécurité ?
Cela donnerait un certain nombre de points de contrôle obligatoires (20 au total), en commençant par renforcer la sécurité du poste de travail. Calculez votre score et concentrez vos efforts sur vos points faibles.

Celui qui arrive à prendre le contrôle d'un poste récupère non seulement les habilitations de l'utilisateur du poste mais peut l'utiliser pour rebondir sur le reste du réseau et des autres systèmes. En résumé, alors que le défenseur doit gagner tout le temps, sur tous les postes, l'attaquant, lui, n'a besoin de gagner qu'une fois sur un poste pour pénétrer tout le système, puisqu'il sera parvenu « à l'intérieur ». Enfin, l'attaquant pourra usurper l'identité de l'utilisateur du poste (se faire passer pour lui dans un email ou une application) et monter des scenarios d'attaque basés sur cet élément d'usurpation. La sécurisation de tous les postes de travail est donc un « must ».

Voici les points à renforcer, qui sont justement à vérifier lors d'un audit « flash » :

1. Gestion des patches, y compris les Plug-in du navigateur
2. Gestion des anti-virus
3. Informations laissées en clair sur les machines, notamment les mots de passe
4. Protection de la mise en veille/session

Une fois que le poste de travail est vérifié, il faut veiller à ce que l'attaquant ne puisse pas pénétrer par les « flux », autrement dit par le dialogue entre les postes de travail et les serveurs à travers les applications et le réseau. Il s'agit essentiellement de mieux protéger les accès au réseau, de chiffrer les flux qui circulent sur le réseau, notamment les mots de passe qui y circulent, ceux-ci permettant ensuite l'accès aux applications et bases de données.

Réseau, Serveurs & Applications

5. Solidité des mots de passe et mots de passe par défaut - Authentification forte
6. Filtrage des accès internet et des flux sortants
7. Flux réseau en clair notamment les mots de passe, y compris imprimantes et scanners
8. Sécurité des applications web
9. Sécurité des réseaux sans fil
10. Sécurité de la voix sur IP
11. Partages réseau, non sécurisés
12. Solidité de la messagerie, chiffrement et signature

Une fois que nous avons sécurisé « l'intérieur », il s'agira de faire en sorte que les machines qui « sortent » ne soient pas contaminées et ne ramènent pas cette contamination « à l'intérieur », une fois que l'utilisateur reconnecte sa machine sur le réseau interne. Une autre possibilité de contamination provient des machines qui ont un accès distant depuis l'extérieur au réseau interne. Une troisième possibilité provient des dispositifs mobiles, comme les tablettes ou les smartphones qui synchronisent leurs données (emails, fichiers) avec le système d'information en passant par Internet. Il peut également s'agir d'appareils achetés par l'utilisateur et amenés sur le site *(Bring Your Own Device)*, alors qu'ils peuvent être contaminés. N'oublions pas dans cette catégorie de « mobilité » que nous sommes au service des utilisateurs du système, que nous devons les protéger et les servir et non pas les freiner ou les bloquer dans leurs usages.

Mobilité

13. Sécurisation des accès distants et du cloud
14. Sécurité des smartphones, tablettes, BYOD, mémoires amovibles USB, etc.

Enfin, il faut avoir une organisation de la sécurité, même si celle-ci est beaucoup plus allégée que celle explicitée dans un système de management, comme l'indique la norme. Il s'agit de faire le focus sur quelques points fondamentaux et surtout d'être réactif à la gestion des incidents et d'en tirer des enseignements pour s'améliorer. Voici les principaux points à vérifier en termes d'organisation. L'essentiel est de couvrir ces points et non pas d'adopter un principe de management qui ne serait pas habituel dans votre organisation.

Organisation

15. Gestion des incidents de sécurité
16. Gestion des entrées-sorties-mouvements d'utilisateurs
17. Surveillance et traçabilité des administrateurs IT
18. Traçabilité des événements sécurité – gestion des logs
19. Gestion des mises au rebut des supports de données
20. Charte d'utilisation et respect des données personnelles

Calculer un score

Pour chacun de ces points de sécurité à couvrir, nous allons élaborer un critère d'audit tel que ci-dessous :

Exigence de sécurité / scénario- type de risque avec impact / exploitation / méthode de vérification / résultat attendu - constat / mesures de sécurité à mettre en œuvre.

Quand il y aura des outils à mettre en œuvre, il s'agira d'exemples, souvent tirés de logiciels libres de manière à réduire les budgets de mise en œuvre, tout en permettant à la culture sur le sujet de se créer (modèle « freemium » : on

commence par un logiciel « free », puis on achète la version « premium », avec plus de fonctions, une fois que l'outil a été adopté et compris par les équipes).

En synthèse, la sécurité des systèmes d'information tient en 20 points fondamentaux. Vous pouvez auditer ces 20 points et calculer votre score. Vous devez au moins obtenir 15/20 pour considérer que vous avez une sécurité décente. En dessous de 10/20 vous êtes en réel danger. L'avantage de cette méthode en 20 points est que vous pouvez constituer autant de chantiers prioritaires de votre plan d'actions, qu'il y a de points à couvrir. Vous pouvez même regrouper vos chantiers en catégories : postes de travail, mobilité, réseaux-serveurs-applications », organisation. Cela évitera de vous disperser et, comme le préconisait Vauban, vous concentrerez vos efforts sur vos points faibles.

Audits de maturité

Un dernier mot sur les dispositifs d'audit. Un écart est quelque chose de binaire. Soit on est conforme, soit on ne l'est pas. Cela cache souvent une réalité plus complexe, comme des niveaux de maturité, notamment pour l'application de règles.

On peut être « embryonnaire » en sachant qu'il nous faudrait telle ou telle procédure, mais sans en disposer de manière écrite. On va appeler ce niveau la « maturité 1 ». Ensuite, la procédure est écrite, mais elle n'est pas appliquée de manière régulière, c'est le niveau 2. Puis elle est appliquée de manière régulière, mais sans que personne ne vérifie (audite). C'est le niveau 3. Puis la procédure est auditée régulièrement, mais aucune amélioration n'a encore eu lieu, c'est le niveau 4. Enfin, la procédure existe, elle est appliquée et auditée régulièrement et des actions d'amélioration ont été entreprises, c'est le niveau maximum de maturité à 5.
Ainsi l'entreprise disposera d'un système d'audit moins abrupt et s'inscrivant complètement dans l'amélioration continue.

> « Vous devez au moins obtenir 15/20 pour considérer que vous avez une sécurité décente »

0.7

0.7 PROSPECTIVE

Si on adoptait l'angle de vision du patient…, **Philippe Ameline** P. 111 & 112
2028 : année zéro, **Auriane Lemesle** P. 113 & 114
Un permis pour l'accès au SI, **Cédric Cartau** P. 115 & 116
L'éducation au numérique : un investissement d'avenir, **Dominique Lehalle** P. 117

Si on adoptait l'angle de vision du patient…

Changer de référentiel ? Au lieu de surveiller le monde des données au travers de caméras fixées aux murs du centre de soins, cela revient à l'envisager depuis une caméra posée sur la tête de Mme Dupont. Que voyons-nous ? Comment ce nouvel angle peut-il influencer notre approche de la sécurité des systèmes d'information ?

Philippe Ameline est ingénieur civil des Mines et spécialiste de la gestion des connaissances en santé. Il collabore à de nombreux cercles de réflexion, comme le CISP Club[1] ou openEHR[2]. Il a rédigé le modèle Ligne de vie et conçu le logiciel Episodus. Il a participé à la rédaction du Guide pour la dématérialisation des échanges entre donneurs d'ordres et services d'aide et d'accompagnement au domicile et pour la télégestion de l'Edess (Échanges de données dans l'espace sanitaire et social[3]). Il publie un blog (http://philippe.ameline.free.fr/wordpress/) sur lequel vous trouverez une compilation de textes marquants (à propos du management, de la médecine, de l'informatique, des start-up…).

Un plat de spaghettis. Le PowerPoint voulait probablement représenter l'interconnexion des forces en présence en Afghanistan. Mais le résultat évoquait si manifestement un inextricable plat de nouilles que le général en chef Stanley McChrystal[4] répliqua sèchement « When we understand that slide, we'll have won the war ». Traduire, avec le recul historique, « si notre intelligence de la situation ressemble à ça, la guerre est perdue ». Il avait raison !

Un plat de spaghettis, c'est également ce que m'a toujours évoqué la sécurité des systèmes d'information médicaux. Des centaines de métiers et leurs entrelacs de fonctions de soins, d'accueil, d'hôtellerie, dans des lieux largement ouverts au public, et de plus en plus connectés à l'Internet. Pour l'anecdote, cet échographe sur lequel le médecin tape le nom du patient, puis stocke des images et souvent des rapports, c'est généralement, sous la carrosserie, un PC sous Windows XP qui n'a jamais vu la moindre mise à jour ; en d'autres termes, la fâcheuse combinaison d'un pot de miel et d'un cheval de Troie. Il faut heureusement imaginer le pirate informatique pusillanime et repoussé par l'odeur de l'éther… Mais lorsque la vague de la télémédecine aura dispersé des objets du même type aux quatre vents, il pourra s'en donner à cœur joie pendant qu'il veille son grand-père.

1 Club des utilisateurs francophones de la CISP (Classification internationale des soins primaires) : http://www.cispclub.org

2 http://www.openehr.org/

3 Ex-Édisanté.

4 Commandant de l'ISAF (Force internationale d'assistance à la sécurité/OTAN) en Afghanistan entre juin 2009 et juin 2010. Le film War Machine (Netflix, 2017) est inspiré de sa vie.

Le nœud se situe dans le référentiel usuel de l'organisation

Face à une situation complexe, l'homme de l'art est tenté de conserver une forme de contrôle en exhibant un vocabulaire endogène au service d'une réflexion et d'un discours technique ; il expliquera par exemple que la promotion et l'homologation de référentiels de sécurité et d'usage contribuent à la gouvernance et à l'urbanisation des systèmes d'information. Reste, comme l'évoque la remarque acide du général McChrystal, qu'on peut ainsi être à la fois techniquement pertinent et détaché des menaces réelles du terrain. Fort de cette (impertinente) évidence, j'ai fait le pari d'utiliser ma naïveté dans le domaine de la sécurité pour me colleter frontalement avec le plat de spaghettis, si possible de façon efficace, voire scientifique !

Lorsqu'un problème se révèle inextricable, le réflexe usuel du mathématicien ou du physicien est de chercher s'il n'existe pas un référentiel, un autre système de vision, dans lequel apparaissent des solutions naturelles. Puisque le nœud se situe dans le référentiel usuel de l'organisation, de ses bâtiments, ses matériels, et son personnel, avec ses rôles et droits d'accès, on peut tenter de le desserrer en se projetant, par l'esprit dans autre point de vue… par exemple celui du patient. Au lieu de surveiller le monde des données au travers de caméras fixées aux murs du centre de soins, cela revient à l'envisager depuis une caméra posée sur la tête de Mme Dupont. Que voyons-nous ?

Quand les caméras fixes voyaient défiler des patients, notre caméra embarquée verra défiler des soignants. On imagine que ces acteurs pluridisciplinaires qui apparaissent autour du patient sont conscients de former une équipe : on adorerait qu'ils partagent une vision commune du processus en cours, on rêverait qu'ils soient ainsi unis dans une démarche de continuité des soins en fonction des objectifs de vie de Mme Dupont. C'est, en réalité, un défi considérable dans un domaine qui reste actuellement organisé et sécurisé en silos… Les solutions ne peuvent être que radicales.

10% des données concourent à la continuité des soins

Effaçons totalement l'organisation et concentrons-nous sur la « cellule active » autour du patient. Elle doit traiter les informations dans deux dimensions spatio-temporelles : alimenter ponctuellement le processus de soins local (les données de workflow, par essence d'intérêt temporaire) et contribuer au projet de santé au long cours (les données d'intérêt historique).

Si on adoptait l'angle de vision du patient…

Constatons tout d'abord, comme l'affirme Ed Hammond de la Duke University (et ancien président d'HL7), que 90% des données recueillies lors d'un séjour alimentent le processus de soins interne mais n'ont ensuite qu'un intérêt légal ou de recherche. Logiquement, elles devraient être sécurisées au sein de la cellule active pendant le séjour, puis supprimées des systèmes opérationnels et stockées de façon pseudo-anonyme sur des serveurs adaptés aux extractions statistiques, qualitatives ou légales.
Reste les 10% de données d'intérêt historique pour le patient. A l'évidence, puisqu'elles concourent à la continuité des soins, elles ne doivent surtout pas rester stockées dans un silo mais suivre le patient au long cours.

Des technologies explorées depuis plus de dix ans

En résumé, le patient se déplace au long cours dans une bulle d'information (qui m'entoure ?, avec quel niveau de proximité et pour quelle fonction ?) qui héberge les données de son projet personnel de santé. Lorsqu'il débute un séjour, cette bulle s'intègre dans une cellule active pluridisciplinaire qui gère un processus de soins. 10% des informations produites s'intègrent à la bulle et le reste rejoint des archives pseudo-anonymisées lorsque la cellule est démantelée à la sortie du patient (ou à la fin du processus de soins s'il est prolongé par une période de suivi). Le système d'information hospitalier tel qu'on le connait disparait ainsi au profit d'une solution considérablement plus opérationnelle et facile à sécuriser puisque seuls les acteurs de la cellule ont accès aux données nominatives pendant que le processus est actif, et qu'il n'en reste plus aucune une fois la cellule démantelée.

A ce stade de la réflexion, nous avons rendu plausible l'hypothèse d'une résolution élégante du problème par changement de référentiel : de celui de la boîte de l'organisation à celui de la bulle du patient, du cartésien au polaire. Reconnaissons tout de même que, avant de mettre au rebut les actuels SIH, il faudra donner une existence concrète aux concepts de « bulle » et de « cellule » qui supportent la démonstration.

Les éléments de base de la bulle existent depuis le début de ce siècle avec les technologies de la Ligne de vie. Leur système de droits d'accès en fonction de la position autour du patient (les rosaces Odyssée) était même intégré au premier cahier des charges du DMP de juillet 2005.
Pour outiller la cellule, définie par l'ensemble des membres de l'organisation qui rejoignent l'équipe de santé d'un patient pour l'accompagner dans le cadre d'un processus de soins, il faut à la fois organiser le parcours « en interne » et l'intégrer dans la continuité des soins. En interne, il s'agit classiquement d'orchestrer les ressources matérielles et humaines (ce qu'on appelle usuellement un chemin clinique, ou « care pathway ») mais aussi, ce qui est plus innovant, de recruter les compétences internes et externes en fonction de la spécificité du patient et des éventuels aléas rencontrés. L'intégration à la continuité des soins pourra utiliser des outils dont les prototypes ont déjà été développés il y a dix ans en collaboration avec l'équipe Acacia de l'INRIA[5], spécialisée en gestion des connaissances : le staff virtuel qui permet de partager une « carte cognitive » de la situation et le système Question Options Criteria (QOC) qui facilite la prise de décision en environnement complexe par énumération des options possibles et élaboration en groupe de la liste des critères en faveur ou en défaveur de chacune d'entre elles.

> « Le patient se déplace au long cours dans une bulle d'information qui héberge les données de son projet personnel de santé. Lorsqu'il débute un séjour, cette bulle s'intègre dans une cellule active pluridisciplinaire qui gère un processus de soins »

Gestion de projet personnel, orchestration des ressources humaines et matérielles et gestion asynchrone de la prise de décision sont donc autant de technologies qui ont été explorées depuis plus de dix ans et pourraient contribuer à fournir une solution radicale au problème du plat de spaghettis. Mais après tout, ce problème existe-t-il vraiment ? Les experts de la gouvernance et de l'urbanisation sont-ils dans le vrai lorsqu'ils affirment qu'il suffit de promouvoir les bons référentiels de sécurité et d'usage ?
Il serait facile d'y voir une application directe du principe de Shirky qui stipule que, pour perdurer, « les institutions feront tout pour préserver le problème dont elles sont la solution ». Plus prosaïquement, il faut constater que proposer à ces institutions de résoudre les problèmes complexes en quittant leur référentiel pour s'organiser avec une « efficace agilité » autour de chaque individu ressort d'un niveau de conscience collective d'un niveau supérieur. Rien moins que de reconnaitre aux humains des qualités que leur dénie la nécessité ressentie d'une organisation hiérarchique.
Puisque le niveau de conscience est ce qu'il est, il est indubitablement plus raisonnable de conserver le plat de spaghettis. Et de renforcer la gouvernance en ajoutant de nouveaux référentiels et de nouvelles strates hiérarchiques.

5 https://www.inria.fr/equipes/acacia

2028 : année zéro

Faut-il attendre le choc brutal, l'attaque de grande ampleur qui met à bas les systèmes d'information en santé pendant de longues semaines et coûte en vies humaines, pour que les efforts nécessaires à leur sécurisation soient pris au sérieux ? La transformation numérique du système de santé se poursuit à un rythme d'enfer…. Et jusque-là, tout va bien…

Secrétaire générale de l'APSSIS depuis 2015 et Référente régionale de la Sécurité des SI au GCS e-santé Pays de la Loire depuis 2016, **Auriane Lemesle** est en charge de l'animation de la sécurité numérique auprès des structures de santé ligériennes. Auparavant, elle a construit et animé une démarche d'amélioration de la sécurité des SI pour les établissements membres du GCS TéléSanté Centre, durant quatre ans. Elle est diplômée de deux Master II : « Risques sanitaires dans les structures de soins et industries de produits de santé » et « Management de la SSI de Santé ». Depuis 2014, elle est enseignante pour le DU « Sécurité des SI de Santé » et pour la formation ingénieur en « Gestion des risques des secteurs de santé » à l'ISTIA, école d'ingénieurs de l'Université d'Angers.

Je me souviens qu'en 2011 Gérard Péliks (cf page 45) racontait comment le ver Stuxnet avait infecté les centrifugeuses iraniennes d'enrichissement d'uranium, levant le voile sur les immenses possibilités d'attaques des environnements SCADA (système de contrôle et d'acquisition de données fréquemment employé dans l'industrie).

Déclaration volontaire des incidents

Je me souviens qu'en 2014, à son retour au ministère de la Santé, le FSSI des ministères sociaux, Philippe Loudenot (cf page 05), avait mis en place un cercle de confiance pour la déclaration volontaire des incidents de sécurité et lancé les premières alertes SSI santé. Il était ensuite rejoint par Stéphane Pasquier et Fabien Malbranque, le travail d'appui et de prévention auprès des structures ne manquant pas !

Je me souviens qu'en 2012, lorsque les pouvoirs publics ont lancé le programme Hôpital numérique, dont l'un des objectifs majeurs était de prendre en compte la sécurité numérique, à tous les niveaux, nombre de structures ne l'ont pas pris au sérieux et se sont déclarées conformes juste pour obtenir des financements.

Je me souviens que, le 7 avril 2015, Charles Blanc-Rolin (cf page 54) ouvrait le premier forum dédié aux systèmes d'information hospitaliers, lieu incontournable de réflexion et d'échanges pour le secteur, et faisait la part belle à la sécurité numérique sous toutes ses coutures : technique, organisationnelle et humaine...

Je me souviens qu'en 2011, Vincent Trély, après une réflexion prospective, a eu l'idée courageuse de créer l'APSSIS et son congrès national annuel au Mans, premier - et toujours unique - événement dédié à la cybersécurité santé. Certains disaient alors que ça serait difficile à pérenniser, parce que la SSI Santé n'était pas, elle-même, un sujet pérenne… Force est de constater qu'il s'agissait d'une erreur ! L'APSSIS est devenue un acteur incontournable du domaine, réunissant des centaines de structures et un réseau de professionnels dynamiques.

Je me souviens qu'en 2009 Conficker s'immisçait dans les systèmes via les appareils biomédicaux. Des hôpitaux ont dû, en partie, fermer. Malgré la mise à disposition de correctifs de sécurité, le ver perdure ; il a même ressurgi à plusieurs reprises, en 2012 et 2018 notamment.

Valoriser le hacking éthique

Je me souviens, en 2016, avoir rencontré une âme bienveillante, dont l'un des hobbies est de rechercher des vulnérabilités affectant des structures de santé, afin de les en avertir avant que celles-ci ne soient exploitées par des personnes malveillantes. On ne valorise pas suffisamment la communauté des hackers éthiques…

Je me souviens qu'en 2017 la ministre de la Santé plaçait la sécurité numérique comme pilier de l'hygiène informatique pour accomplir le défi de l'essor du numérique, afin de renforcer l'efficacité de notre système de santé. Dans ce cadre, le signalement des incidents de sécurité informatique devenait obligatoire, permettant d'industrialiser le processus d'accompagnement des structures avec la création de la cellule ACSS (Accompagnement Cybersécurité des Structures de Santé).

Je me souviens qu'en mai 2018, quand le RGPD est entré en application, très-très-très peu de structures de santé étaient prêtes et, les semaines précédentes, une vague de panique les avait submergées. Le trio d'avocats spécialisés, Marguerite Brac de La Perrière, Omar Yahia et Pierre Desmarais, les avaient pourtant prévenues lors du congrès de l'APSSIS. Nombre de prestataires (plus ou moins bien intentionnés) s'étaient engouffrés dans la brèche pour proposer des solutions miracles à des coûts exorbitants ! Le soufflé était assez rapidement retombé… jusqu'à ce qu'un hôpital se fasse épingler par la CNIL … en 2022. La première amende dépassant le million d'euros.

2028 : année zéro

Un petit séisme et une prise de conscience désormais permanente des associations fédérées de patients, de plus en plus exigeantes.

Je me souviens qu'en 2013 Cédric Cartau rédigeait ses premiers écrits. Ses analyses et descriptions périodiques de l'actualité sous une tonalité peu conventionnelle et son franc parler ne laissèrent personne indifférent.

Wannacry ? Nous avons eu de la chance

Je me souviens qu'en 2017 les hôpitaux britanniques du NHS furent touchés de plein fouet par le cryptovirus Wannacry : annulation de près de 20 000 consultations et interventions, des services d'urgence dans l'incapacité de recevoir les patients… En France, nous n'étions probablement pas meilleurs mais… sur ce coup-là, nous avons eu de la chance ! Ce ne fut pas le cas pour l'attaque suivante…

Je me souviens que début 2018 Dominique Lehalle affirmait que la cybersécurité n'était pas réservée aux hommes et que l'APSSIS allait s'engager pour promouvoir une plus grande mixité auprès des professionnels du secteur.

Je me souviens que la transformation numérique du système de santé s'est poursuivie à tour de bras, laissant la sécurité numérique au stade de l'intention ; les objets connectés ont continué à envahir notre quotidien, tout cela présentant une surface d'attaque toujours croissante.

Que de belles initiatives individuelles et collectives ! Dommage que les messages et les doctrines qu'elles portaient n'aient pas été suffisamment prises au sérieux, que les budgets n'aient pas été à la hauteur et qu'il ait fallu attendre la (prévisible) catastrophe…

Les systèmes étaient en réalité atteints depuis des années

Je me souviens de ce jour de décembre 2028 où l'attaque de grande ampleur sur des structures de santé à l'échelle nationale impacta de manière irrémédiable le fonctionnement des établissements, rendant difficile, voire impossible, la prise en charge des patients pendant plus de 3 semaines. Les logiciels et dispositifs connectés se sont mis à « foleiller » (perdre la boussole comme on dit dans notre patois angevin), affichant des constantes et présentant des prescriptions complètement erronées. Le contenu des dossiers médicaux n'était plus fiable. Puis tous les équipements connectés se sont brutalement arrêtés. Plus aucune information n'était disponible. Les investigations démontreront que les systèmes étaient en réalité atteints depuis plusieurs années et que, depuis, les informations étaient modifiées de manière aléatoire et imperceptible**.** La Commission d'enquête parlementaire évoque 1 765 morts directement liés à cette attaque. Choc brutal pour la population.

Espérons que cela ne soit que pure fiction et qu'une prise de conscience, couplée à des actions pérennes et correctement dimensionnées, sera opérée…

> « Un hôpital épinglé par la CNIL … en 2022. Première amende dépassant le million d'euros : petit séisme et prise de conscience »

Un permis pour l'accès au SI

Peu de contraintes cadrent l'accès des utilisateurs à un Dossier Patient informatisé malgré les risques que cela comporte. Deux réponses peuvent être avancées, la procédure et la formation, assorties de la mise en œuvre d'un passeport annuel, sans lequel l'accès au SI serait coupé.

Cédric Cartau, RSSI et DPO du CHU de Nantes et du GHT44, est également chargé de cours à l'EHESP et à l'ESIEA. Il collabore régulièrement à la revue DSIH et a publié plusieurs ouvrages, notamment « La sécurité du système d'information des établissements de santé », seconde édition (Eyrolles, 2017).

Dans certains long-métrages de Kung Fu de série C, le héros extermine une brochette de méchants à l'aide d'un cure-dents élimé aux deux bouts, mais l'hypothèse d'une tuerie de masse avec ce genre d'équipement est fortement improbable. C'est la raison pour laquelle les cure-dent restent en vente libre. Par contre, la détention de plutonium ou le pilotage d'un 747 peut provoquer des dégâts considérables. C'est la raison qui explique que la première est réglementée et qu'il faut une licence pour le second. En revanche, côté systèmes d'information de santé (SIS), rien de rien, ou presque

> « On trouve aussi d'excellentes formations ciblées sur les grandes plateformes de MOOC comme fun-mooc.fr »

Le constat

Entre 1987 et 2006, environ 5500 personnes traitées dans le service de radiothérapie du centre hospitalier d'Epinal ont subi des sur-irradiations. En cause : le mésusage d'un logiciel de pilotage de l'appareil d'irradiation qui servait à calculer les doses. Une mise à jour de ce logiciel avait été effectuée tout à fait normalement mais, dans la nouvelle version, un champ avait changé d'unité (passant par exemple de millilitre à litre), et les personnels en charge continuaient de saisir des litres croyant saisir des millilitres, multipliant d'un facteur équivalent (x1000 !) les doses envoyées. Résultat : au moins 12 morts et des centaines de blessés graves, selon les estimations de l'époque[1].

Des procédures ont, depuis, été mises en place pour éviter que ce genre d'incident se reproduise, mais il n'existe que peu ou pas de contraintes réglementant l'accès des utilisateurs à un Dossier Patient informatisé (DPI), alors qu'il permet pourtant de prescrire des tas de produits, et pas seulement des trucs qui font voir des éléphants roses.

Procédures vs formation

Il existe deux réponses globales à cet état de fait : la procédure et la formation.
Dans le dernier tome de son ouvrage phare, Christian Morel décrit en première partie l'enfer de la normalisation et des procédures, et surtout la limite de cette approche (avant le scandale du *dieselgate*, Volkswagen était certifié ISO pour la propreté de ses moteurs…).

> « Les MOOC offrent une palette suffisamment large pour couvrir quasiment tous les besoins en formation »

La seconde réponse, que Christian Morel appelle le développement de l'hyper compétence, part du principe que la seule voie de sortie valable est la formation des professions qui manipulent des systèmes à risque : les pilotes de ligne, les superviseurs de réacteurs nucléaires, les chirurgiens, etc. Former oui, mais qui, à quoi et comment ?

Formations protéiformes

Concernant le « comment », la question est réglée : les MOOC et autres types de formation en ligne, en mode on-premise ou en mode Saas, offrent une palette suffisamment large pour couvrir quasiment tous les besoins. On peut citer l'excellent MOOC de l'ANSSI[2], ainsi que celui, plus récent, du ministère de l'Intérieur[3]. On trouve aussi d'excellentes formations ciblées sur les grandes plateformes de MOOC comme fun-mooc.fr.

1 https://fr.wikipedia.org/wiki/Affaire_des_surirradi%C3%A9s_de_l%27h%C3%B4pital_d%27%C3%89pinal
2 https://secnumacademie.gouv.fr/
3 https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/

Un permis pour l'accès au SI

Pour ce qui est du « qui », il est important de segmenter les populations concernées en au moins cinq groupes :

- la direction générale, car les messages à transmettre sont moins techniques que stratégiques et juridiques
- l'ensemble des agents, car les messages à transmettre sont généraux et touchent à l'usage au quotidien de l'outil : choix des mots de passe, bon usage de la messagerie, vigilance sur les pièces jointes et la navigation Internet, etc.
- les agents de la DSI (qu'ils soient issus des équipes techniques ou des équipes en AMOA), car il faut aller beaucoup plus loin dans les sujets abordés ; le MOOC de l'ANSSI est un bon début mais ne suffit pas
- les « power users », à savoir ceux qui ont accès à des fonctions à haut niveau de privilège dans les progiciels métier ; il s'agit par exemple des administrateurs fonctionnels de la DRH (ils ont accès à la gestion des comptes utilisateurs et font l'objet d'une attention particulière dans la certification des comptes), de l'équipe qui gère l'accès à l'entrepôt de données patients à des fins de recherche, du DIM, etc.
- enfin, le corps médical et le corps soignant, pour les raisons évoqués en début d'article.

Pour toutes ces populations à l'exception de la deuxième (l'ensemble des agents), la cible est claire : un passeport annuel, sans lequel l'accès au SI sera coupé. Certains laboratoires de biologie médicale mettent déjà cela en œuvre dans le cadre de la certification ISO 15189. Nous n'y échapperons pas sur le reste du SI, si l'on en juge par l'avalanche de textes dans ce domaine depuis 2016 : instruction 309, RGPD, directive NIS, etc.

L'éducation au numérique : un investissement d'avenir

La cadence de la transformation numérique s'accélère mais les efforts de formation n'ont pas suivi. D'où un manque de maitrise d'une bonne part des citoyens et professionnels qui pèse sur l'appréciation des cyber risques et comment s'en prémunir.

Dominique Lehalle, journaliste, a créé une agence éditoriale - DL Infos - spécialisée en e-santé pour répondre aux besoins des média professionnels, des institutions et des entreprises: rédaction de numéros spéciaux, livres blancs, dossiers de presse ; études de marché ; conception et animation de programmes de congrès ; conseil en communication.
Elle a participé à la réalisation du Mooc e-santé organisé par l'association FormaTic Santé.

Le Conseil national du numérique nous avait alertés, dès 2013, avec un (brillant) rapport[1], dirigé par Valérie Peugeot : « les enjeux d'inclusion numérique concernent désormais l'ensemble de la population et nous sommes face à une cible mouvante : une personne à l'aise avec le numérique aujourd'hui dans son univers familial et amical pourra se trouver perdue demain quand il lui faudra réinventer son métier numérisé ou soigner une pathologie via un dispositif dématérialisé. » Ce paragraphe, extrait de l'avant-propos, désigne clairement les enjeux qui se sont affirmés depuis. L'accélération des taux d'équipement des Français et de la dématérialisation de leurs activités professionnelles ne devait pas masquer l'inconfort, voire l'anxiété, d'une bonne partie des citoyens face aux TIC.

Perdues dans le cloud

Cinq ans plus tard, il semble que la plupart de ses recommandations se soient perdues… dans le cloud. Jusqu'à ce que les pouvoirs publics prennent, récemment, la mesure du retard, préparent un plan « Pour une France connectée », et annoncent quelques actions pour « Développer les compétences numériques des élèves ». Le diagnostic ? Il tient en quelques indicateurs et un nouveau concept, l'illectronisme. Le Baromètre du numérique 2017 relevait que trois à quatre personnes sur dix se disent « non compétentes » pour utiliser les produits technologiques du quotidien. Cela n'est pas une surprise dans la mesure où la plupart en ont appris le maniement « sur le tas ». Les professionnels de santé ne sont pas mieux lotis : trois sur quatre déclarent se sentir démunis et mal formés en matière de numérique, d'intelligence artificielle et de robotisation[2].
L'illectronisme, une forme d'illettrisme numérique, a été largement médiatisé en 2018, un sondage l'évaluant à près d'un Français sur cinq. D'où la mobilisation du secrétariat d'Etat au numérique. Quant au ministère de l'Education, il ouvre à la rentrée scolaire 2019, un enseignement obligatoire pour les classes de seconde en « Sciences numériques et technologie », soit 1 h 30 par semaine pour apporter «à la fois un apprentissage de l'informatique en tant que science et un questionnement sur la place du numérique dans la société ».
Il était temps !

> « Si vous trouvez que l'éducation coûte cher, essayez l'ignorance (Abraham Lincoln) »

Des acteurs, pas des esclaves

L'éducation a toujours été un investissement d'avenir. « Si vous trouvez que l'éducation coûte cher, essayez l'ignorance », aurait dit Abraham Lincoln. Aujourd'hui, l'éducation au numérique exige aussi un investissement. Pas seulement parce qu'elle contribue à l'employabilité. Pas seulement parce qu'elle permet à tout un chacun de participer activement à la transformation numérique. Pas seulement parce que cette transformation numérique est un gage de compétitivité. Mais surtout, comme le dit si bien Serge Abiteboul[3], chercheur à l'INRIA et auteur de plusieurs ouvrages de vulgarisation, parce que la transition numérique « a besoin d'acteurs maîtrisant ces technologies, et pas d'esclaves de ces technologies. » Or cette maitrise conditionne l'écoute et l'impact de la sensibilisation à la cybersécurité, l'appréciation des risques, la réactivité face aux menaces.
La prise de conscience se fait peu à peu. Elle gagnerait à être accélérée alors que la cadence de la dématérialisation forcit. C'est particulièrement vrai dans la santé. Pourtant, la formation, les compétences dans l'utilisation des systèmes d'information sont encore largement négligées : pas un mot dans les projets de « Virage numérique » et stratégie « Ma Santé 2022 » ! Alors qu'elles étaient déjà quasi passées à la trappe à l'époque d'Hôpital numérique. A chaque acteur de s'en saisir ?

1 « Citoyens d'une société numérique ». https://cnnumerique.fr/files/2018-02/CNNum_rapport_Inclusion_oct2013-sans-annexe.pdf

2 http://www.ticsante.com/Pres-des-trois-quarts-des-professionnels-de-sante-s-estiment-mal-formes-sur-le-numerique-(sondage)-NS_4381.html

3 Dans une tribune, Le Monde du 27 novembre 2018

BIBLIOGRAPHIE

ALEXANDRE Laurent. La guerre des intelligences. JC Lattès, 2017, 250 pages

ALFER Aline, KASHANI-POOR Amandine et MATHIAS Garance. Le Délégué à la protection des données (DPO): Clé de voûte de la conformité. Revue Banque, édition 1, 2017, 120 pages

BABINET Gilles. Big Data, penser l'homme et le monde autrement. Le passeur, 2016, 247 pages

BABINET Gilles. L'Ère numérique, un nouvel âge de l'humanité. Le passeur éditeur, 2014, 236 pages

BERANGER Jérôme. Les Big Data et l'éthique, le cas de la datasphère médicale. ISTE éditions, 2016, 314 pages

BERANGER Jérôme. Les systèmes d'information en santé et l'éthique. ISTE éditions, 2015, 418 pages

BRASSEUR Christophe. Enjeux et usages du big data. Hermes Science Publications, 2ème édition, 2016, 152 pages

CARTAU Cédric. La sécurité du système d'information des établissements de santé, édition 2. Presses de l'EHESP, 2018, 335 pages

CARTAU Cédric. Stratégies des systèmes d'information : vers l'hôpital numérique. Presse de l'EHESP, 2014, 152 pages

CHESNOT Guy. Big data et cloud : Stockage et traitement de données du futur. Vuibert, 2ème édition, 2017, 256 pages

DEBIZE Thomas, ANZALA-YAMAJAKO Alexandre, SOULLIE Arnaud, BILLOIS Gérôme, KOKOS Ary, WOLFHUGEL Christophe et BLOCH Laurent. Sécurité informatique: Pour les DSI, RSSI et administrateurs. EYROLLES, 5ème édition, 2016, 622 pages

DEGOS Laurent. Quelle politique de santé pour demain ?. LE POMMIER. 2016, 164 pages

DORDOIGNE José. Réseaux informatiques - Notions fondamentales (Protocoles, Architectures, Réseaux sans fil, Virtualisation, Sécurité, IPv6.) Editions ENI, 7ème édition, 2017, 702 pages

FERNANDEZ Valérie, GILLE Laurent et HOUY Thomas. Les technologies numériques de santé: Examen prospectif et critique. Transvalor - Presses des mines, édition 1, 2015, 112 pages

FERNANDEZ-TORO Alexandre. Management de la sécurité de l'information, 4e édition: Implémentation ISO 27001. EYROLLES, 4ème édition, 2018, 363 pages

FERNANDEZ-TORO Alexandre. Sécurité Opérationnelle. Conseils pratiques pour sécuriser le SI Eyrolles, édition 2, 2016, 424 pages

GAUSSIER Eric et AMINI Massih-Reza. Recherche d'information - Applications, modèles et algorithmes: Data mining, décisionnel et big data. EYROLLES, 2ème édition, 2017, 274 pages

GHERNAOUTI Solange. Cybersécurité - Sécurité informatique et réseaux. DUNOD, 5ème édition, 2016, 384 pages

GOODMAN Marc. Les crimes du futur. Nouveau Monde Editions, 2017, 790 pages

HARARI Yuval Noah. Homo Deus, Une brève histoire de l'avenir. Albin Michel, 2017, 404 pages

HARARI Yuval Noah. Sapiens: Une brève histoire de l'humanité. Albin Michel, 2015, 512 pages

HAGEGE Claude. L'éthique de l'internet face au nouveau monde numérique. Mais qui garde les gardes ? Editions L'Harmattan, 2015, 208 pages

ISRAEL Mauro. Cyber Security Instinct. Lulu, 2017, 406 pages

MATTATIA Fabrice. Le droit des données personnelles: N'attendez pas que la CNIL ou les pirates vous tombent dessus ! EYROLLES, 2016, 234 pages

MOREL Christian. Les décisions absurdes. Tome III, Gallimard, 2018, 272 pages

OLIVENNES Denis et CHICHPORTICH Mathias. Mortelle transparence. Albin Michel, 2018, 198 pages

PINET Claude. 10 clés pour la sécurité de l'information: ISO/CEI 27001-2013. AFNOR, 2ème édition, 2017, 190 pages

PLOUIN Guillaume. Cloud computing - Sécurité, gouvernance du SI hybride et panorama du marché. DUNOD, 4ème édition, 2016, 288 pages

PUJOL Philippe. Marseille 2040 – le jour où notre système de santé craquera. Flammarion, 2018, 224 pages

SADIN Eric. L'Intelligence artificielle ou l'enjeu du siècle – Anatomie d'un antihumanisme radical. L'Echappée, 2018, 298 pages

STAMBOLIYSKA Rayna. La face cachée d'internet : hackers, dark net… Larousse, 2017, 277 pages

VALLANCIEN Guy. Homo Artificialis. Plaidoyer pour un humanisme numérique. Michalon, 2017, 201 pages.

VALLANCIEN Guy. La médecine sans médecin ?: Le numérique au service du malade. Gallimard, 2015, 304 pages

VASSET Philippe et GASTINEAU Pierre. Armes de déstabilisation massive. Fayard, 2017, 280 pages

ACISSI* (Collectif). Ethical Hacking : Apprendre l'attaque pour mieux se défendre. Editions ENI, 5e édition, 2017, 881 pages

Collectif sous la direction d'Alain BENSOUSSAN. La protection des données personnelles de A à Z. Bruylant Edition, 2017, 262 pages

Collectif sous la direction de Jacques MARCEAU. Quelle santé pour demain ? : quand le numérique bouleverse la médecine. Alternatives, 2014, 208 pages

*ACISSI (Audit, Conseil, Installation et Sécurisation des Systèmes d'Information) est une association à but non lucratif qui forme et conseille sur les enjeux de la sécurité informatique. www.acissi.net/

WEBOGRAPHIE

Active Directory :

https://fr.wikipedia.org/wiki/Active_Directory

https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-active-directory/

https://docs.microsoft.com/fr-fr/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

https://www.comptoirsecu.fr/tags/active-directory/

Introduction à la sécurité des systèmes d'information. Guide pour les directeurs d'établissement de santé. DGOS. Novembre 2013

https://solidarites-sante.gouv.fr/IMG/pdf/guide_-_introduction_a_la_securite_du_systeme_d_information_-_dgos_-_091213.pdf

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD)

https://www.CNIL.fr/fr/reglement-europeen-protection-donnees

Décret n° 2016-1214 du 12 septembre 2016 relatif aux conditions selon lesquelles sont signalés les incidents graves de sécurité des systèmes d'information

https://www.legifrance.gouv.fr/eli/decret/2016/9/12/AFSZ1622277D/jo/texte

Instruction N°SG/DSSIS/2016/309 du 14 octobre 2016 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information (« Plan d'action SSI ») dans les établissements et services concernés

http://circulaire.legifrance.gouv.fr/index.php?action=afficherCirculaire&hit=1&r=41533

http://solidarites-sante.gouv.fr/fichiers/bo/2016/16-12/ste_20160012_0000_0074.pdf

Instruction N° SG/HFDS/2016/340 du 4 novembre 2016 relative aux mesures de sécurisation dans les établissements de santé

http://circulaire.legifrance.gouv.fr/index.php?action=afficherCirculaire&hit=1&r=41530

Arrêté du 13 décembre 2016 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services d'administration centrale, les services déconcentrés, les organismes et établissements sous tutelle des ministères chargés des affaires sociales

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033624998&categorieLien=id

Ordonnance N° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel

https://www.legifrance.gouv.fr/eli/ordonnance/2017/1/12/2017-27/jo/texte

Instruction N° SG/HFDS/DGCS/2017/219 du 4 juillet 2017 relative aux mesures de sécurisation dans les établissements et services sociaux et médico-sociaux

http://circulaires.legifrance.gouv.fr/index.php?action=afficherCirculaire&hit=1&retourAccueil=1&r=42445

Instruction N° SG/SHFDS/FSSI/2017/281 du 26 septembre 2017 relative au rôle des ARS dans la mise en œuvre du dispositif de déclaration obligatoire et de traitement des signalements des incidents graves de sécurité des systèmes d'information des structures de santé

https://solidarites-sante.gouv.fr/fichiers/bo/2017/17-10/ste_20170010_0000_0027.pdf

Article L1111-8-2

https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006072665&idArticle=LEGIARTI000031921128&dateTexte=&categorieLien=cid

Décret N° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel.

https://www.legifrance.gouv.fr/eli/decret/2018/2/26/SSAZ1733293D/jo/texte

La Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S). Juillet 2018

http://esante.gouv.fr/services/politique-generale-de-securite-des-systemes-d-information-de-sante-pgssi-s/en-savoir-plus-0

Guide d'hygiène informatique de l'ANSSI

https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

Directive NIS. Juillet 2016

https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/

Portail d'accompagnement cybersécurité des structures de santé

https://www.cyberveille-sante.gouv.fr/

Portail de signalement des événements sanitaires indésirables

https://signalement.social-sante.gouv.fr

La stratégie numérique du Programme Ma santé 2022

https://solidarites-sante.gouv.fr/actualites/actualites-du-ministere/article/ma-sante-2022-les-10-mesures-phare-de-la-strategie-de-transformation-du-systeme

https://solidarites-sante.gouv.fr/IMG/pdf/masante2022_rapport_virage_numerique.pdf

REMERCIEMENTS

L'ASIP Santé, qui a tout de suite soutenu le projet, s'y associant sur le fond et sur la forme,
Alain Espinoux, RSSI Adjoint - ASIP Santé, membre du Comité de rédaction,
Dominique Lehalle, pour la rédaction en chef,
Marie-Valentine Bellanger, pour le pilotage opérationnel du plan de production
Hélène Daspe, pour le pilotage du volet financement
Notre Graphiste, Tristan Bellanger - Corvy-Graphisme

Le FSSI du Ministère des Solidarités et de la Santé, Philippe Loudenot, pour sa bienveillance et ses propos introductifs

Nos Partenaires, qui nous ont fait le plaisir à la fois d'écrire sur le fond et de nous aider à financer la production de l'Ouvrage : Asip Santé, BeyondTrust, Claranet, Coreye (Pictime Groupe), Enovacom, Trendmicro

Et notre partenaire média : DSIH Magazine

Un grand merci aux Professionnels, RSSI, DSI, Experts, Institutionnels, Avocats… qui ont donné de leur temps pour écrire et donner vie à cet Ouvrage !

Ameline Philippe
Berry Pauline
Blanc-Rolin Charles
Bonnet Didier
Brac de la Perrière Marguerite
Cabon Frédéric
Cartau Cédric
Coupez François
Culbert William
Dachicourt Fabien
Delubac Benjamin
Espinoux Alain
Fourchon Yohann
Gauthier Bruno
Gaston Gérard
Guézo Loïc
Israel Mauro
Jamet Elodie
Jeunot Guillaume
Jodry Christophe
Kadi Nour
Lang Astrid
Le Callonec Christophe
Lehalle Dominique
Lemesle Auriane
Loudenot Philippe
Marty Guy
Moneger Stéphane
Peliks Gérard
Pescarmona Didier
Plouvier Lénaïc
Roman Michael
Sabatier Pascal
Thamier Stéphan
Tourron Philippe
Trély Vincent
Veauvy Thierry
Verbeke Didier
Wetter Sébastien
Zablit Isabelle

Rédaction en Chef : Dominique Lehalle
Comité rédactionnel : Dominique Lehalle, Alain Espinoux, Vincent Trély
Création : Corvy-Graphisme
Crédit photo : Fotolia

À PROPOS DE L'APSSIS

QUELQUES CHIFFRES CLÉS

- 7 congrès
- + de 100 adhérents
- + de 1000 RSSI formés
- + de 2000 visites mensuelles sur le site
- + de 3000 professionnels de santé sensibilisés

L'APSSIS est l'unique organisme français dédié à la Sécurité des Systèmes d'Information de Santé. L'Association a pour objet de constituer et d'animer l'écosystème pluri-professionnel dédié à la réflexion et au développement de la sécurité au sein de l'écosystème numérique de santé.

Prestataire de formation, l'APSSIS propose des formations innovantes spécialement adaptées aux secteurs de la Santé. Ses membres contribuent au déploiement des bonnes pratiques en matière de SIS (présence médias et évènements cyber) et assurent une veille technologique et institutionnelle.

APSSIS

APSSIS

Association Pour la Sécurité des SI de Santé

84 rue du Luart
72160 Duneau

0629365995

secretaire@apssis.com

www.apssis.com

APSSIS

Association Pour la Sécurité des SI de Santé