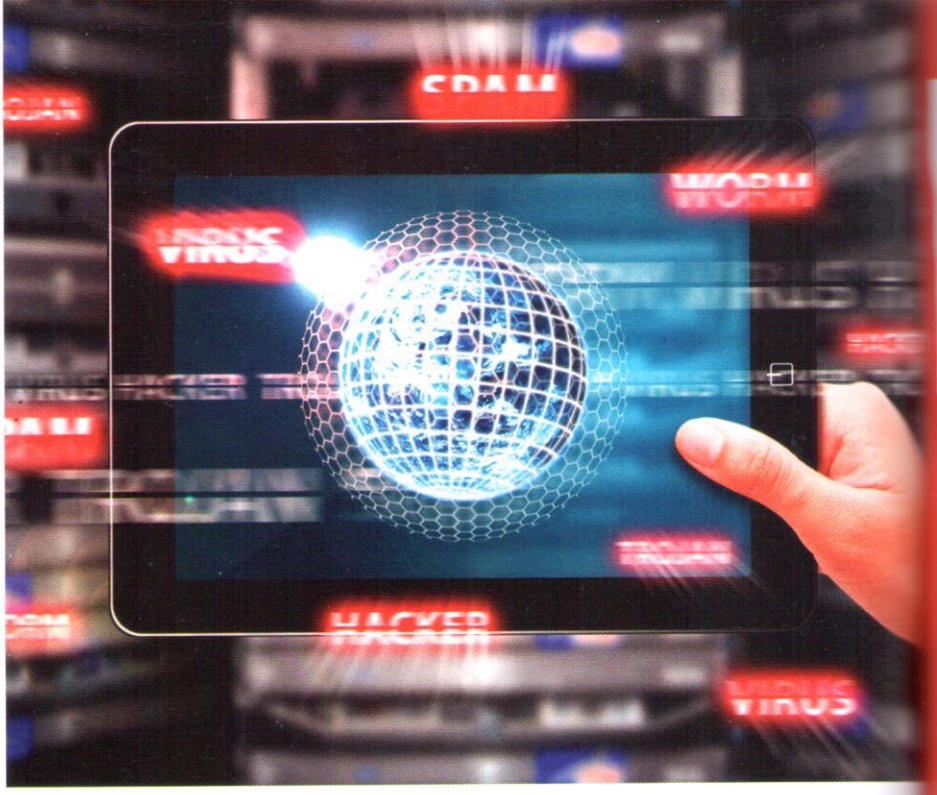
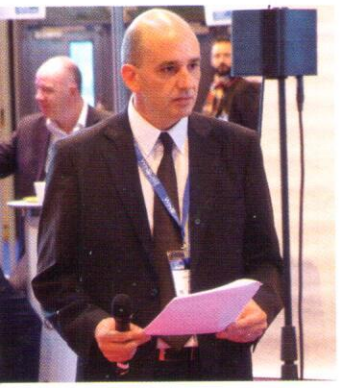
Sécurité des SI : retours du front



En 2014, Vincent Trély, président de l'Apssis[1] et dirigeant du cabinet Proxima Conseil, a formé plus de 200 référents SSI Santé sur l'ensemble du territoire. Il conseille également une dizaine d'établissements de santé dans le cadre de la constitution de leur dossier Hôpital numérique, en particulier sur le volet sécurité des prérequis du programme. Il revient sur les enseignements de cette année de terrain



Vincent Trély, président de l'Apssis et dirigeant du cabinet Proxima Conseil

Ils sont techniciens informatiques à 80 %, mais aussi qualiticiens, gestionnaires de risques, cadres de santé, médecins DIM, directeurs ou comptables, pour les 20 % restants ! Ils cumulent souvent les casquettes. Ils pilotent l'informatique d'établissements de santé publics ou privés, de taille très variable (entre 90 lits en psychiatrie et un CHU). Ils sont le plus souvent débordés, assurant des astreintes étonnantes, et assumant parfois seuls la responsabilité du système d'information global de leur établissement. Leur point commun ? Ils viennent d'être nommés référents ou correspondants Sécurité des SI (SSI) dans le cadre du programme Hôpital numérique ! Certains l'ont demandé… d'autres pas.

Certains ont entamé une démarche SSI cohérente, seuls ou accompagnés, et veulent l'installer dans le temps. D'autres savent qu'ils manqueront de temps, et qu'après la pression de l'atteinte des prérequis, la SSI retombera en priorité 100. Ils le regrettent tous.

D'autres sont sur le pont, mobilisés, et cherchent le chemin critique entre qualité des procédures rédigées et mises en œuvre, délais avant date limite de dépôt Dipisi[2] ou la visite HAS[3], temps nécessaire pour mener à bien cet ensemble d'opérations, soutien du Codir[4] et de la CME[5]. La PSSIE[6], applicable aux établissements de santé, et sa déclinaison par le ministère de la Santé, la DGOS, la HAS, l'Asip Santé, n'est pas une option. 2017 est l'année où cette PSSIE doit être opérationnelle au sein de tous les établissements, publics et privés, tout comme l'atteinte des prérequis du programme Hôpital numérique. Les référents SSI sont les pionniers de ce vaste chantier, premiers acteurs de terrain avec pour mission de faire d'eux-mêmes et des utilisateurs des « maillons forts » de la sécurité des SI de santé ! Ils savent la tâche ardue, mais semblent tous motivés par les enjeux, par la méthode, par la transversalité du projet, celui-ci dépassant de loin la réalité technique quotidienne de leurs jobs.

Des faiblesses à corriger

Pour initier, puis surtout ancrer la démarche SSI et « qualité du SI » sur le terrain, ils ont identifié des points forts, des leviers, mais également des faiblesses, qu'il convient de corriger pour s'assurer de la réussite de la finalité : améliorer la robustesse et la cohérence des SI de santé.

… suite p. 36

[1] Association pour la promotion de la sécurité des systèmes d'information de santé (www.apssis.com).
[2] La plate-forme Dipisi permet l'instruction des projets d'investissement des systèmes d'information des établissements dans le cadre du projet Hôpital numérique ainsi que leur suivi en cas de soutien financier.
[3] Haute Autorité de santé.
[4] Comité de direction.
[5] Commission médicale d'établissement.
[6] Politique de sécurité des SI de l'État.

Les points forts relevés sont les suivants :

- Adhésion totale aux constats de faiblesses des SI de santé et à leur nécessaire sécurisation ;
- Reconnaissance de la cohérence générale des normes et réglementations : Anssi/RGS, critères 5a et 5b de la HAS, prérequis Hôpital numérique, critères SSI dans le processus de certification des comptes, PGSSI-S et guides associés, PSSIE en date du 17 juillet 2014, décret Hébergeur ;
- Motivation et réel intérêt pour le sujet ;
- Accompagnement régional de qualité, lorsqu'il existe…

Les points faibles sont avant tout de source humaine, et l'on peut donc jouer sur ces axes pour atteindre l'objectif poursuivi :

- Manque de temps dédié : moins de 20 % des référents SSI rencontrés ont un temps officiel alloué à la mission/fonction ;
- Déficit de compétences sur certains grands axes de la SSI, mais la formation est justement là pour y pallier ;
- Complexité générale des corpus documentaires pour une personne de formation technique. D'où la bonne idée d'impliquer la qualité/gestion des risques dès que cela est possible !
- Difficultés à faire comprendre les enjeux : moins de 40 % des référents SSI rencontrés ont une direction perçue comme « sensible à la sécurité des SI ». Le corps médical, s'il comprend l'enjeu sécurité, n'est pas suffisamment impliqué/sensibilisé et résiste aux éventuelles contraintes imposées par la SSI ;
- Manque d'encadrement régional. Effectivement, seules quelques régions disposent aujourd'hui, au sein de l'ARS ou d'un GCS, d'une fonction RSSI régionale professionnalisée et dont l'une des missions est d'animer le réseau des correspondants.

Philippe Loudenot, fonctionnaire de sécurité des SI des ministères des Affaires sociales et de la Santé

> *« Plus aucun directeur général ne peut ignorer le risque, plus aucun médecin « informatisé » ne peut être insensible à la problématique de la sécurité numérique. »*

Garder le fort…

… et poursuivre l'effort, en maintenant l'arsenal de procédures (schéma réseau, systèmes, applications, PSSI, PRA[7] testé, même partiellement, plans de sauvegarde et de restauration, indicateurs de performance du SIH), en alliant technicité et mobilisation mesurée des ressources métiers, et en faisant simple.

La fonction « sécurité des SI » est l'une des plus partageables qui soit. 80 % des bonnes pratiques et des corpus documentaires types (PSSI, charte utilisateurs, charte administrateurs, modèles d'indicateurs SIH, procédures SSI, modèles de gouvernance) sont applicables à tout établissement de santé, public ou privé. Les 20 % restants consistent à adapter avec pertinence les principes fondamentaux de la SSI au contexte particulier de chaque établissement. Alors partageons, mutualisons, allons puiser de la connaissance là où elle existe, de façon structurée et organisée (Anssi, DGOS, Asip Santé, normes, entre autres), et avec les moyens dont dispose le système, faisons passer un premier palier critique de maturité aux SI de santé !

Le FSSI (fonctionnaire de sécurité des SI) des ministères des Affaires sociales et de la Santé, Philippe Loudenot, est mobilisé au côté des RSSI et des référents, pour soutenir, accompagner, sensibiliser le top management et organiser une chaîne de communication efficace courant 2015[8].

Fini la naïveté !

Les événements de décembre 2014 ont été suffisamment nombreux et médiatisés pour que l'on convienne que la cybersécurité ne peut plus être pour personne un vague concept aux bordures de la science-fiction. Les attaques sur les systèmes de santé des pays industrialisés ont augmenté de 600 % en 2014 et touché plus de 40 % des hôpitaux américains[9]. L'affaire Sony nous a montré la puissance de frappe des attaquants et l'artillerie logicielle dont ils disposent. TF1 s'est fait voler près de 2 millions de comptes abonnés, informations diverses associées, et Orange Espagne 10 millions de données abonnés pour la nouvelle année 2015 ! Les hôpitaux français ont été en alerte avec un *ransomware* à activation basique, mais doté d'une puissance de frappe exceptionnelle – cryptage des données accessibles et demande de rançon pour obtention de la clé de décryptage – qui a donné des sueurs froides à plusieurs CHU et gros CH français[10]. En résumé, plus aucun directeur général ne peut ignorer le risque, plus aucun médecin « informatisé » ne peut être insensible à la problématique de la sécurité numérique.

La compréhension et l'acceptation du problème, puis le soutien appuyé de la direction générale et de la communauté médicale, par son président, sont essentiels à la dynamique de la SSI. Un RSSI seul est un RSSI démuni. Dans le même ordre d'idées, un référent SSI devra placer le curseur où il faut entre une démarche trop brutale, constituant à tout vouloir mettre aux normes, trop vite, quitte à se heurter à d'infranchissables résistances, et un laisser-aller bien installé de plus en plus sensible et dangereux. La sécurité des SI de santé est une affaire de dialogue, de pédagogie, d'avancées progressives et de percées ciblées. Elle impose de ne pas hésiter à utiliser certains événements pouvant favoriser les prises de conscience.

Le programme Hôpital numérique est pragmatique, à la fois ambitieux et mesuré. La démarche SSI de l'Asip Santé également. Les mentalités sont prêtes. Les bonnes volontés présentes. Nous avons deux à trois ans ! ■

[7] Plan de reprise d'activité.
[8] Lire http://www.dsih.fr/article/998/securite-des-si-en-sante-vers-la-mise-en-place-d-une-chaine-d-alerte.html
[9] Article du MIT, « 2015 Could Be the Year of the Hospital Hack », http://www.technologyreview.com/news/533631/2015-could-be-the-year-of-the-hospital-hack/
[10] Alerte du CERT-USA, https://www.us-cert.gov/ncas/alerts/TA14-353A