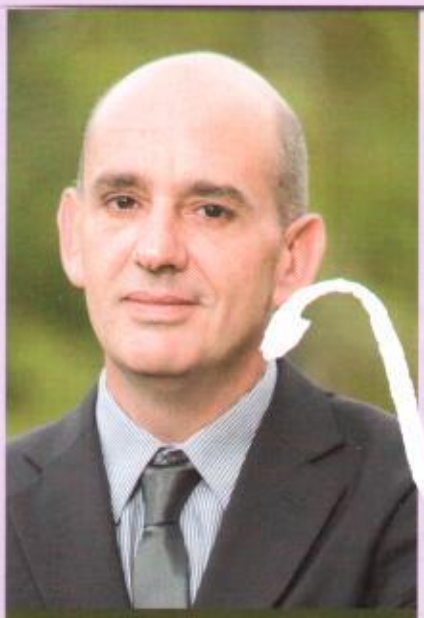
techniques hospitalières

781
mars-avril 2020
75e année

FHF
SPH éditions

Vincent Trély



Vincent Trély
Président & fondateur de l' Association pour la sécurité des systèmes d'information de santé (Apssis)
Directeur associé & consultant expert chez Weliom

« Tout l'écosystème est conscient et mobilisé. Les planètes semblent alignées, et 2020 doit être l'année de la réelle, de la vraie sécurité numérique, prise à sa juste mesure. »

Depuis le début du XXIe siècle, notre système de santé vit sa révolution numérique. Dédiés dans un premier temps aux fonctions supports (finances, ressources humaines, admissions, achats), les systèmes d'information supportent maintenant tous les processus de soins : urgences, blocs opératoires, circuit du médicament, dossier patient informatisé, imagerie, biologie et spécialités. Cette numérisation massive ainsi que les échanges nécessaires à la coordination des parcours de soins sont indiscutables et apportent fluidité, qualité et sécurité au système de santé. Pour autant, la surface numérique ainsi développée à ouvert la porte à la cyber insécurité et les structures de santé sont les victimes récurrentes de cyber attaques.

L'intérêt porté aux données de santé, dont le vol et la revente sont sources d'importants revenus, le blocage des systèmes d'information contre demande de rançon, comme ce fut le cas récemment au CHU de Rouen ou au sein du Groupe Ramsay, entre autres nombreux exemples, constituent deux menaces sérieuses, dont les impacts peuvent être critiques, sur les plans économique et sanitaire.

Dans son discours du jeudi 28 novembre 2019, prononcée lors de l'étape parisienne du tour de France de la e-santé, notre ministre, Agnès Buzyn, déclarait : *« Face aux risques de cyberattaques du système de santé, la cybersécurité à l'échelle de chaque établissement de santé est donc devenue une priorité nationale »*. Une action nationale de sensibilisation des professionnels de santé est lancée le même jour : « Tous cyber vigilants ». Il aura fallu une dizaine d'années, deux programmes de financements nationaux (Hôpital Numérique et HOP'EN), le RGPD, l'activisme d'un écosystème soudé et une série d'incidents de sécurité notables pour que le sujet soit enfin pris à sa juste mesure. Nous ne pouvons que nous réjouir du constat factuel réalisé et de la rédaction de la doctrine du numérique en santé qui intègre la sécurité au cœur de ses priorités.

Les responsables sécurité des SI (RSSI), professionnels de terrain, sont prêts, même si pas encore parfaitement positionnés et entendus et même s'il reste à leur donner des moyens concrets, humains et financiers, pour agir. L'offre industrielle est de bonne qualité, avec des solutions de plus en plus sophistiquées, comme a pu le montrer le Forum international de la cybersécurité (FIC) 2020, alliant les technologies traditionnelles aux nouvelles fonctions d'analyse comportementale basée sur des IA. De nouvelles obligations vont peser sur les industriels du biomédical et de l'IoT, afin qu'ils proposent des solutions sécurisées pour supporter leurs équipements. Tout l'écosystème est conscient et mobilisé. Les planètes semblent alignées, et 2020 doit être l'année de la réelle, de la vraie sécurité numérique, prise à sa juste mesure, et déployée dans l'intérêt des professionnels de santé, principaux usagers des systèmes numériques, et dans l'intérêt des patients, de la qualité et de la fluidité de leurs parcours de soins et de la sécurité de leurs données personnelles.