UNE OFFRE DE SERVICES PENSÉE POUR LES ÉTABLISSEMENTS DE SANTÉ

GESTION DES RISQUES INFORMATIQUES : GPLEXPERT CONFIRME SON SAVOIR-FAIRE

Si le développement de l'hôpital numérique représente un véritable atout pour les établissements de santé et leurs patients, il n'en est pas moins exempt de risques. La sécurisation du système d'information (SSI) impose dès lors la disponibilité de compétences spécifiques, ainsi que nous l'explique Damien Ribeiro, responsable de la sécurité des systèmes d'information (RSSI) pour GPLExpert. Par Pamela Claude

Damien Ribeiro, responsable de la sécurité des systèmes d'information pour GPLExpert

QUELS SONT LES PRINCIPAUX RISQUES INFORMATIQUES AUXQUELS LES ÉTABLISSEMENTS DE SANTÉ SONT AUJOURD'HUI CONFRONTÉS ?

DAMIEN RIBEIRO : Ceux-ci sont de trois ordres. D'abord, les risques externes, pour l'essentiel liés aux cyberattaques. Nous observons ici une montée en puissance des *ransomwares* (ou rançongiciels), qui chiffrent les données contre une rançon. Ils coexistent avec les habituelles pratiques d'ingénierie sociale consistant à manipuler les individus à des fins d'escroquerie, dont les traditionnels spams de *phishing* (ou hameçonnage) imitant parfaitement les messages officiels des opérateurs et autorités, ainsi que les faux techniciens s'introduisant sur le système informatique sous prétexte de virus détectés. Deuxième grande famille, les risques liés aux accès illégitimes des informations, à mettre en regard avec la complexité des dispositifs d'authentification des utilisateurs. Citons pour finir les risques inhérents aux pannes : l'indisponibilité des applications peut alors compromettre le processus des soins. Il faut ici disposer de sauvegardes, d'un fonctionnement en mode dégradé, et de plans de reprise et de continuité de l'activité (PRA/PCA), tous testés et validés en amont, ainsi que le spécifie désormais le programme HOP'EN.

JUSTEMENT, COMMENT RÉPONDRE AUX EXIGENCES DES INSTANCES RÉGULATRICES ?

Il convient de mettre en œuvre une gouvernance adéquate des risques internes, portée par la direction de l'établissement – dont l'engagement est primordial afin que les moyens alloués soient véritablement à hauteur des enjeux. Cette gouvernance doit par ailleurs s'articuler autour d'un RSSI pour le pilotage des politiques de sécurité, et d'un *Data Protection Officer* (DPO) pour la mise en conformité avec les exigences du règlement général sur la protection des données (RGPD). Les deux travaillent de concert mais chacun a des compétences spécifiques, d'où la nécessité de disposer de deux fonctions distinctes – ce qui est loin d'être évident dans toutes les structures.

QUELLE FORME PREND LA GESTION DES RISQUES INFORMATIQUES AU QUOTIDIEN ?

Elle s'appuie sur quatre piliers : sensibiliser les utilisateurs qui sont souvent à l'origine des principales failles de sécurité ; analyser régulièrement les risques pour élaborer un plan d'actions tenant compte des spécificités propres à chaque établissement ; prioriser ces actions en fonction des vulnérabilités identifiées ; et enfin mettre en œuvre une politique de sécurité qui soit à la fois sécurisante et applicable – le curseur étant parfois difficile à placer, d'où l'importance de disposer d'un RSSI connaissant bien le secteur de la santé. C'est là qu'entre en jeu GPLExpert, dont l'offre intègre différents services tels que la réalisation de formations, l'accompagnement et le coaching des RSSI et des DPO nommés, ou encore la mise en œuvre d'audits de sécurité sur des risques spécifiques. Nous proposons également des services de RSSI externalisé et d'infogérance de la sécurité pour détecter, confiner et assainir les menaces informatiques. Signalons pour finir que ce savoir-faire s'inscrit dans une démarche de management de la sécurité des systèmes d'information orientée ISO 27001. ●