Menaces informatiques et dernières dispositions réglementaires

La première journée scientifique du Syndicat des biologistes (SDB) a été l'occasion d'une mise au point concernant les dernières dispositions réglementaires en matière de sécurité informatique, notamment l'obligation de déclaration de tout incident grave sur les systèmes d'information à l'ASIP santé et la mise en œuvre du décret 2016-46 relatif à la biologie médicale.

Dans le cadre de l'article L. 1111-8-2 du code de la santé publique, l'arrêté d'application du décret N° 2016-1214 du 12 septembre 2017 rend obligatoire le signalement de tout incident de sécurité sur les systèmes d'information à partir du 1er octobre 2017. À cet effet a été créée la cellule accompagnement cybersécurité des structures de santé de l'ASIP santé (ACSS), qui concerne les établissements de santé civils et militaires, les centres de radiothérapie et les laboratoires de biologie médicale. *« L'objectif est de renforcer le niveau de cybersécurité, d'alerter et d'informer en cas de circulation d'une menace et de partager les bonnes pratiques »,* a détaillé Emmanuel Sohier, de l'ACSS.

Toute une veille sur l'actualité en matière de cybersécurité et santé ainsi qu'un forum à destination des référents sécurité pour favoriser le partage d'expérience sont disponibles sur le site www.cyberveille-sante.gouv.fr. *« L'ASIP santé met aussi à disposition des fiches réflexes pour réagir à un incident de sécurité et des guides de bonnes pratiques »,* a ajouté le spécialiste. Le dispositif de signalement concerne les incidents graves de sécurité informatique ayant des conséquences potentielles ou avérées sur la sécurité des soins, sur la disponibilité, l'intégrité ou la confidentialité des données de santé ou sur le fonctionnement des établissements. Il est à noter que la gestion des incidents reste à la charge des établissements.

Lors d'un signalement sur *https://signalement.social-sante.gouv.fr,*l'évènement est traité par l'ARS qui s'appuie sur l'ASIP santé, il peut y avoir escalade vers la DGS ou l'agence nationale de sécurité des systèmes d'information (ANSSI), avant un retour aux structures pour qualifier l'incident et proposer des solutions de réponses au besoin par une orientation vers des acteurs de proximité. La déclaration à la CNIL est à effectuer en parallèle s'il y a eu violation de données à caractère personnel. En dehors des heures ouvrées et en cas d'incident grave suspecté, le fonctionnaire de sécurité des systèmes d'information pourra être directement saisi (ssi@sg.social.gouv.fr). *« Cette déclaration n'est pas publique et son objectif est l'accompagnement et le partage d'expérience, pas la sanction. Si l'incident concerne un DM-DIV ou le personnel, il y a une double déclaration à effectuer »,* a rappelé le Dr Bruno Gauthier de Bio 86.

Règlementation européenne et protection des données personnelles

Marguerite Brac de la Perrière, du cabinet Bensoussan, et Olivier Panthaléo, de Provadys, ont ensuite dressé un panorama des attaques informatiques, ainsi que des enjeux des réformes règlementaires. *« Tous les jours, nous assistons à des attaques et des exfiltrations de données, pour un coût estimé en 2015 de 3,7 milliards d'euros et en augmentation en 2016 de 30 %. Toutes les entreprises sont concernées. Le délai moyen entre le piratage et sa prise en compte est de 255 jours ! »,* a précisé O. Panthaléo. Se protéger à 100 % relève de l'impossible, le but est aujourd'hui de décourager l'attaquant qui changera de cible si l'attaque s'avère trop complexe. *« Il n'y a pas forcément besoin de dispositifs complexes, le maillon le plus faible est souvent humain. Sur les 24 derniers mois, 68 % des entreprises ont été piratées, 50 % étant des TPE ou PME »,* a chiffré le spécialiste.

Face à cette menace, la règlementation est très vaste. La règlementation européenne en vigueur depuis avril 2016 et applicable au 25 mai 2018, concerne le traitement des données à caractère personnel et l'encadrement de toutes les activités les entourant (collecte, gestion, transfert, accès, hébergement). *« Elle comporte 400 obligations et 99 articles avec des référentiels sectoriels. Il est impossible de tout maîtriser. Le guide doit être le code de conduite pour les LBM qui est en cours d'écriture »,* estime Marguerite Brac de la Perrière. *« Le nouveau règlement introduit la notion de responsabilisation, avec l'obligation d'assurer la sécurité des données. Si les mesures de sécurité appropriées ne sont pas déployées, une répression pourra être appliquée, à hauteur de 4% du CA mondial d'une entreprise ».* Le code de conduite répertoriera donc les exigences techniques et juridiques ainsi que les bonnes pratiques en LBM.

En parallèle, le PIAF (private impact assessment framework), plateforme pour formaliser les analyses d'impact, anticipera les risques encourus pour la vie privée en LBM et signalera les mesures appropriées pour les contrer. *« Après 2018, tous les traitements de données à caractère confidentiel devront faire l'objet d'un PIA »,* a rappelé Olivier Panthaléo.

La société française d'informatique de laboratoire (SFIL) planche actuellement sur les deux dispositifs. Le code de conduite a été établi à la fin novembre, avant l'élaboration du PIAF en fin d'année 2017 puis le déploiement sur un LBM pilote et la,mise à disposition après avril 2018. Une mallette opérationnelle sera associée au code de conduite et au PIAF, avec les référentiels et textes de loi, des exemples de contrats et des fiches types de recueil de consentement.

Mise en œuvre du décret 2016-46 relatif à la biologie médicale

« Les points marquants sur le plan informatique de ce décret intègrent la transmission de la prescription avant le prélèvement, le numéro unique de prélèvement, la validation des résultats avant diffusion, la transmission dématérialisée vers les professionnels de santé, la vérification des DM-DIV une fois par an et la vérification de la cohérence des résultats dans un compte-rendu », a résumé Bruno Gauthier. L'ASIP a publié une note de cadrage le 22 mars 2017 pour définir une trajectoire de mise en œuvre et expliciter le décret. De nombreux chantiers sont en marche. Une mise à disposition par les éditeurs de mails avec deux pièces jointes, PDF et fichier structuré Hprim, qui devait intervenir à la fin du 2nd semestre 2017, a pris du retard.

La DGOS a voulu accélérer par un appel d'offre le développement de la transmission dématérialisée : neuf régions, 21 LBM et 9 éditeurs ont été retenus. *« Un facteur d'accélération a résidé dans la labellisation e-santé des logiciels des centres de santé en 2013 »,* selon Bruno Gauthier. *« Au 31 décembre 2017, ils devaient être en mesure d'intégrer les comptes-rendus de biologie conformes ».* La transmission dématérialisée aux patients, avec une authentification forte de celui-ci et des données constamment chiffrées doit passer par Bluefiles, un dispositif de cryptage agréé par le ministère. L'alignement et la simplification des nomenclatures sur le LOINC, nomenclature pivot des examens de biologie médicale, qui comporte 71 000 codes à l'international et 47 000 en France, est en cours. La transmission de la prescription avant le prélèvement et les conditions d'identification des prélèvements doivent être reprécisées avec la DGS. Enfin, concernant le contrôle des DM-DIV, la SFIL élabore un document pour aider les laboratoires.

Source : Biologiste infos