Premier rapport semestriel du Centre national pour la cybersécurité : focus sur la santé numérique

Frédéric Erard, le 24 mai 2021

Le 11 mai 2021, le NCSC a publié son premier rapport semestriel (Rapport semestriel 2020/2 intitulé « Sécurité de l'information. Situation en Suisse et sur le plan international »). Le thème prioritaire choisi pour ce premier rapport est la santé numérique.

Depuis le 1er juillet 2020 et l'entrée en vigueur de l'Ordonnance fédérale du 27 mai 2020 sur les cyberrisques (OPCy), le Centre national pour la cybersécurité (NCSC) est le centre de compétences de la Confédération en matière de cyberrisques. Il est dorénavant le premier interlocuteur en matière de cybersécurité pour l'administration fédérale, les milieux économiques, les cantons, les établissements d'enseignement ou plus généralement la population. Il centralise à cet égard les notifications concernant les cyberincidents (pour la liste de ses compétences : art. 12 OPCy). Du point de vue structurel, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) est désormais intégrée au NCSC.

Le 11 mai 2021, le NCSC a publié son premier rapport semestriel (Rapport semestriel 2020/2 intitulé « Sécurité de l'information. Situation en Suisse et sur le plan international »), couvrant la période de juillet à décembre 2020. Le thème prioritaire choisi pour ce premier rapport est la santé numérique, soit une bonne occasion pour rappeler quelques éléments importants en lien avec la sécurité de données de santé.

Dans son chapitre consacré à la santé numérique, le NCSC commence par constater que la transformation numérique progresse inexorablement dans le secteur de la santé. Si cette évolution présente de nombreux avantages, elle augmente aussi la surface d'attaque potentielle à l'encontre des données de santé. Or, les données de santé sont considérées comme des « données sensibles » à la lumière du droit suisse de la protection des données et, en tant que telles, bénéficient d'une protection renforcée. Les données traitées dans le secteur des soins présentent de surcroît des caractéristiques particulières : il faut par exemple soigneusement les protéger des risques de destruction puisqu'elles peuvent difficilement être reconstituées (p. ex. : examens médicaux effectués dans le passé) ou les protéger contre les modifications non autorisées (p. ex. : la modification des données relatives au groupe sanguin d'un patient pourrait avoir des conséquences dramatiques).

Le Rapport 2020/2 attire ensuite l'attention du lecteur sur les « traces de données de dispositifs médicaux ». Il souligne l'existence de différents registres dans ce domaine (p. ex. : registre suisse des implants SIRIS) ou la conservation de données en vue de gérer les stocks de matériel au sein des établissements de santé. Ces traitements visent non seulement à servir l'assurance-qualité, mais aussi à assurer la traçabilité des produits utilisés. La garantie d'intégrité et l'accessibilité de telles données doivent faire l'objet d'une attention particulière.

Si les établissements de santé sont sujets aux mêmes types de cyberattaques que les entreprises d'autres secteurs, les conséquences dans le domaine médical peuvent se révéler bien particulières. En raison du caractère non modifiable et sensible des données, une altération ou une indisponibilité des données peuvent directement mettre en danger la santé ou la vie d'individus. Le NCSC recommande d'accorder une attention toute particulière au contrôle des accès et systèmes (notamment par recours à des authentifications à plusieurs facteurs) et à une sensibilisation du personnel face aux risques liés à la cybercriminalité.

Un type d'attaque classique contre les établissements de soins est le chantage reposant sur les données de patients via des rançongiciels (*ransomware*). Les pirates collectent un maximum de données avant de les crypter, puis bloquent leur accès ou menacent de les divulguer à moins qu'une rançon ne leur soit versée. Certains criminels ont même tenté d'opérer ce chantage directement à l'encontre des patients concernés.

Enfin, le NCSC constate que la période de pandémie liée à la COVID-19 a créé des conditions particulièrement néfastes en termes de cybersécurité. Non seulement les conséquences d'une attaque sur un système hospitalier sous pression sont souvent plus graves, mais les risques que de telles attaques réussissent sont exacerbés par l'épuisement des soignants et par le sentiment d'urgence général (p. ex. : les risques qu'un soignant se fasse piéger par un courriel malveillant sont plus élevés). Plusieurs attaques ont été recensées en Suisse au cours de l'année 2020, sans qu'elles aient toutefois eu des conséquences néfastes. Le NCSC recommande ainsi de non seulement mettre en place des mesures de protection techniques suffisantes, mais aussi de mettre en place des processus spécifiques de sensibilisation du personnel dans ce contexte et de détection des tentatives de fraudes ou autres attaques d'ingénierie sociale.

Le reste du rapport offre un aperçu des annonces reçues par le NCSC en matière de cybersécurité et dresse un panorama utile des menaces actuelles. On y apprend notamment que la pandémie et sa course au vaccin a suscité plusieurs cyberattaques avec des visées

d'espionnage économique. Ces attaques étaient en particulier visées contre des institutions de recherche, des entreprises impliquées dans le développement de vaccins ou même contre l'Agence européenne des médicaments. L'attaque menée contre cette dernière aurait conduit au vol de documents déposés auprès de cette agence par les entreprises Pfizer et Moderna. Le NCSC en conclut que quiconque effectue des travaux de recherche sur la COVID-19 doit s'attendre à des attaques d'espionnage économique.

Proposition de citation : Frédéric ERARD, Premier rapport semestriel du Centre national pour la cybersécurité : focus sur la santé numérique, 24 mai 2021 *in* www.swissprivacy.law/74