DOC
LE RENDEZ-VOUS
DES MÉDECINS
VAUDOIS

Faire face à une attaque informatique

Les cybermenaces, un cancer à traiter avant sa métastase

L'analogie entre le système immunitaire du corps humain et le système informatique de votre cabinet est des plus pertinentes : dans les deux cas, on cherche autant à réduire le risque de contracter une maladie qu'à diminuer son impact si elle survient tout de même.

Nonobstant le fait qu'avoir une mauvaise hygiène de vie ne va pas pénalement engager notre responsabilité en cas de maladie, il en est tout autre avec l'hygiène numérique au sein de votre cabinet (celle de votre système et équipement informatique ainsi que le niveau de littératie numérique des employé-es et dirigeant-es). Dans le domaine informatique, il va s'agir autant de votre responsabilité morale que juridique et plus spécifiquement de votre réputation.

La nouvelle loi sur la protection des données qui entrera en force en septembre 2023 pourra permettre des sanctions à hauteur de 250'000 CHF si une négligence grave est prouvée (art. 8 nLPD Sécurité des données). Et, si les données médicales d'un cabinet sont touchées, celui-ci aura alors l'obligation d'annoncer les violations de la sécurité des données aux personnes concernées (art. 24 nLPD) [1].

La clé, c'est d'anticiper

Si le cadre légal peut donner une idée des limites à ne pas dépasser et des sanctions qui peuvent en découler, anticiper les risques inhérents à la transformation numérique de notre société sur son secteur d'activité est aussi une responsabilité morale, d'autant plus quand on parle de données médicales. Le code informatique est une conception humaine et l'humain est faillible. Pour se faire une idée du problème, il suffit simplement d'observer la fréquence des mises à jour destinées à corriger des failles de sécurité sur des applications, son smartphone, son système d'exploitation.

Dès lors, à l'instar des mesures prises pour lutter contre la pandémie de Covid-19, il est tout aussi important d'appliquer des gestes barrières au niveau de l'hygiène numérique de son cabinet ou de son personnel. C'est l'application de l'ensemble de ces mesures techniques et humaines qui va se révéler efficace. Pour aider les professionnel-les de la santé dans cette tâche complexe, la FMH a publié les « Exigences minimales pour la sécurité informatique des cabinets médicaux » [2]. Le Centre national pour la cybersécurité (NCSC), quant à lui, donne accès à différents documents utiles dont « Cybersécurité dans le secteur de la santé : recommandations » [3] publié en juillet 2022, ainsi qu'un blog dédié à ce secteur, de même que des conseils sur la manière de prévenir ou de réagir à des attaques par logiciels de rançon [4]. C'est rébarbatif, mais ces conseils sont à lire et appliquer de bout en bout. Un peu comme pour la notice qui accompagne un médicament…

Tester régulièrement son dispositif et former son personnel

Quand les cybercriminel-les utilisent des logiciels de rançon, par exemple, la majorité des attaques qui réussissent ont impliqué une action humaine dans leur déroulement. D'autres attaques se sont appuyées plutôt sur l'existence de failles techniques et de sécurité du système informatique. Et les attaques ne se résument bien sûr pas aux seuls logiciels de rançon, même s'il s'agit d'une des menaces les plus critiques à l'heure actuelle. Il faut donc tout mettre en œuvre pour pouvoir anticiper au mieux ce type de risque.

A ce titre, il est important de constamment tester son système en commençant par un audit de sécurité qui englobe toute l'infrastructure informatique et son utilisation par les personnes qui y ont accès. Et par la suite compléter cet audit par des tests de pénétration réguliers (hacking éthique). Il est aussi primordial de former l'ensemble de son personnel à adopter les bons comportements numériques (authentification multifactorielle, utilisation de gestionnaires de mots de passe, gestion des droits d'accès, chiffrement des données et des échanges, travailler avec des systèmes à jour et protégés) et les entraîner à avoir les bons réflexes (ingénierie sociale, phishing, lecture des liens internet et ouverture des documents ou pièces jointes).

Le but de ces actions de prévention est non seulement de réduire le risque qu'une cyberattaque puisse réussir, mais aussi de savoir exactement comment réagir en cas d'incident. A cet effet, il est vivement recommandé de prendre contact en amont de tout problème avec une entreprise spécialisée dans le domaine de la cybersécurité et créer ainsi les conditions optimales d'une intervention rapide en cas de sinistre. Que ce soit pour le prévenir grâce à l'audit de sécurité, ou pouvoir le juguler ou en analyser la portée grâce aux connaissances acquises en amont de l'attaque.

Les mesures prises préventivement sont aussi à considérer comme un outil de gestion de crise. Elles permettent de diminuer l'impact négatif sur la réputation du cabinet en cas d'intrusion et de vol ou perte de données. Aux yeux du public, et plus spécifiquement des patient-es, il y aura une plus grande tolérance si on peut démontrer que le cabinet avait pris toutes les mesures nécessaires pour protéger leurs données médicales.

Demande de rançon : faut-il payer ?

En cas d'exfiltration de données médicales et d'une menace de leur publication sur le Darknet, faut-il payer ou pas la rançon demandée par les cybercriminels ? C'est une question épineuse. D'un côté, les autorités conseillent fortement de ne pas payer, car il s'agit d'une sorte d'encouragement à cette forme de cybercriminalité. Et ce faisant on alimente le système que l'on veut combattre. Mais, d'un autre côté, il y a les données médicales des patient-es qui sont prises en otage alors qu'ils et elles avaient fait confiance à leur praticien-ne pour en assurer la sécurité.

Une fois que les données sont publiées sur le Darknet, il n'est en l'état pas possible de les retirer et tout le monde peut y accéder, pour une durée indéterminée. Ce n'est pas compliqué du moment que l'on a le nom du groupe cybercriminel à l'origine de l'attaque. Si l'on paie la rançon, il n'y a aucune garantie que ces données ne soient pas publiées ou retirées, mais l'usage démontre que dans la très grande majorité des cas, les cybercriminel-les tiennent parole.

Néanmoins, que les données médicales volées ne soient pas publiées en ligne ne signifie pas que les cybercriminel-les ne les ont pas gardées en leur possession ni éventuellement vendues sur un forum sur le Darknet. Il n'y a donc pas une réponse unique à donner, mais une analyse au cas par cas à faire tout en se faisant accompagner dans cette démarche d'évaluation par un-e expert-e du domaine. La complexité du traitement de ce genre de problème démontre l'importance des mesures à même de réduire son apparition.

Soigner ses patient-es, c'est aussi sécuriser leur données

Comme pour le domaine de la santé, il est important d'être assuré-e au niveau des cyberrisques, que ça soit pour pouvoir bénéficier d'une prise en charge adéquate ou pour réduire l'impact financier des dégâts causés par une cyberattaque. Certes, toutes ces mesures représentent des coûts non négligeables, mais à l'heure actuelle ce type d'investissement est une condition sine qua non à l'utilisation des outils numériques, et par ailleurs une obligation légale. Pour les petites structures, il est possible de se regrouper pour aborder certains des aspects liés à la sécurisation de leurs systèmes informatiques ou à la formation de leurs employé-es.

DOC
LE RENDEZ-VOUS
DES MÉDECINS
VAUDOIS

Quelle que soit l'approche choisie, il est essentiel non seulement d'être actif, mais aussi proactif dans la sécurisation de ces données et la formation de son personnel. Les données numériques à caractère médical, ce sont avant tout une version dématérialisée de ses patient-es. Le médecin aura à cœur d'en prendre soin dans leur forme digitale comme dans leur forme humaine.

Stéphane Koch
Vice-président d'Immuniweb SA