DOC
LE RENDEZ-VOUS
DES MÉDECINS
VAUDOIS

Témoignage anonyme

« Mon cabinet a été cyberattaqué »

« Vous avez été piraté… ». Avez-vous déjà imaginé votre réaction si vous aviez à lire ce message en arrivant à votre cabinet un lundi matin, lorsque vous allumez votre ordinateur ?

C'est ce qui m'est arrivé en mars 2022, à l'instar d'autres cabinets romands. J'ai eu quelques premiers réflexes quasi reptiliens qui se sont avérés très utiles pour continuer à recevoir et soigner mes patient-es le temps que la situation se rétablisse, soit deux semaines plus tard. Les conséquences principales ont été une perte de temps conséquente, une diminution du chiffre d'affaires qui ne l'est pas moins, et un changement de fournisseur informatique…

Mes réflexes ont été de ne surtout pas cliquer sur le lien suggéré par les pirates et de faire une rapide capture d'écran de l'agenda des deux premières semaines qui était resté ouvert. A ce moment, je me suis rendu compte de l'ampleur du problème. Impossible d'accéder depuis les différentes machines du cabinet à un quelconque fichier, à l'agenda ou à un dossier patient-e alors que le premier arrivait. La faille venait-elle du logiciel Mediway utilisé dans de nombreux cabinets médicaux en Suisse ou de mon fournisseur IT, pourtant leader en Suisse romande dans son domaine ?

J'ai immédiatement appelé ce dernier qui a eu une attitude peu réactive – je comprendrai plus tard que c'était certainement lié aux nombreux autres appels qu'il recevait simultanément – et plutôt inadéquate. Son premier réflexe fut de se décharger de toute faute et d'incriminer le personnel de mon cabinet qui aurait éventuellement cliqué sur un e-mail malveillant ou effectué une mauvaise manipulation.

Ma chance a été de suivre les conseils d'un ami informaticien.

Sauvegardez vos données sur un serveur externe !

Il s'est avéré par la suite que la cyberattaque a été effectuée par le biais d'une vulnérabilité des accès VPN reposant sur une technologie obsolète, et dont les failles de sécurité avaient même été publiées sur le net. Malgré les dizaines d'attaques similaires et simultanées qui ont touché mes confrères et consoeurs, dont nous avons pris connaissance en communiquant entre nous, mon fournisseur n'a à ce jour toujours pas reconnu sa responsabilité dans cette cyberattaque. Fait encore plus étrange : ce même fournisseur avait, deux semaines auparavant, changé tous les mots de passe de mon cabinet – sans me prévenir ! – chose qu'il n'avait jamais effectuée durant les cinq dernières années. Il était en fait au courant d'attaques itératives depuis plusieurs semaines.

Sachant que le logiciel Mediway crypte toutes les données des patient-es, celles-ci ne peuvent pas être divulguées sur le Darknet. Mais elles ont été surcryptées par les pirates, empêchant leur récupération. Ma chance a été de suivre les conseils d'un ami informaticien et de faire une sauvegarde personnelle de toutes ces données sur un serveur extérieur. C'est ce qui m'a permis de rétablir la situation après deux semaines de sueur, sans conséquence médicale.

J'ai bien entendu tiré plusieurs leçons de cet événement. J'avoue que j'étais insuffisamment informé du risque et que j'ai fait entièrement confiance à mon prestataire IT. Depuis, j'ai changé de fournisseur dont les protocoles de sécurité n'ont rien à voir : authentifications à double facteur, pare-feux, antivirus mis à jour fréquemment et mots de passe changés régulièrement. Je me sens désormais confiant et rassuré, même si la cybersécurité à 100% n'existe pas.

Ce contenu peut être utilisé dans un cadre privé ou pour la formation postgraduée et continue. Toute autre utilisation est subordonnée à l'autorisation écrite préalable de la Société Vaudoise de Médecine (SVM), éditrice et détentrice exclusive des droits.

DOC
LE RENDEZ-VOUS
DES MÉDECINS
VAUDOIS

Médecin vaudois connu de la rédaction

Ce contenu peut être utilisé dans un cadre privé ou pour la formation postgraduée et continue. Toute autre utilisation est subordonnée à l'autorisation écrite préalable de la Société Vaudoise de Médecine (SVM), éditrice et détentrice exclusive des droits.