Des logiciels malveillants aux vols de données: les cabinets médicaux devraient investir dans la cybersécurité, car ils peuvent être la cible de fraudeurs.

Nouvelle newsletter de la FMH sur la cybersécurité

Reinhold Sojer[a], Max Klaus[b], Dominik Kreuter[c]

[a] Dr en biologie humaine, chef de la division Numérisation, FMH; [b] resp. adjoint de la Cybersécurité opérationnelle (OCS), Centre national pour la cybersécurité (NCSC); [c] chef de la division ICT, FMH

La FMH informe désormais des menaces actuelles en matière de cybersécurité dans une nouvelle newletter. Les médecins disposant de leur propre cabinet médical peuvent s'inscrire via l'adresse électronique cybersecurity[at]fmh.ch pour la recevoir.

Les cybermenaces sont un thème à prendre au sérieux, également dans les cabinets médicaux. D'autant plus que les systèmes d'information qu'ils utilisent sont mis en réseau, que les données sont échangées avec d'autres institutions du système de santé, voire qu'elles sont entièrement gérées dans le *cloud* par des prestataires externes ne disposant pas forcément d'une protection suffisante. En lien avec la pandémie du Covid-19, il se pourrait aussi qu'il y ait eu davantage de possibilités d'accès externe aux données d'un cabinet médical par le biais de collaborateurs. Des possibilités d'attaques supplémentaires en résultent pour les escrocs.

Si les cabinets médicaux étaient auparavant sporadiquement affectés par des maliciels tels que des chevaux de Troie d'extorsion qui se propagent via des pièces jointes, cryptent des données et ne les décryptent que contre rançon [1], les médias font état aujourd'hui de manière croissante de vols de données qui touchent des dizaines de cabinets médicaux dis-

Les cabinets médicaux étaient auparavant touchés sporadiquement par des logiciels malveillants; aujourd'hui, on signale de plus en plus de vols de données.

posant des mêmes systèmes vulnérables [2, 3]. Ces données ainsi pillées sont souvent publiées sur le *darknet*, d'où elles peuvent être utilisées ensuite pour d'autres attaques.

Les exigences minimales

A la différence des grandes institutions de santé qui mandatent des experts en sécurité afin de protéger leurs données, il se peut que certains cabinets médicaux ne disposent pas de l'expertise nécessaire. En 2019 déjà, la FMH avait publié des recommandations [4] sur les exigences minimales pour la sécurité informatique des cabinets médicaux. Ces exigences ont pour but de garantir un niveau de sécurité minimal pour les données, les informations et l'infrastructure informatique des cabinets médicaux. Même s'il n'existe aucune protection à 100% contre les attaques, il est important d'appliquer dans leur intégralité ces exigences minimales dans les cabinets.

La FMH recommande aux cabinets médicaux de déterminer la marche à suivre en cas d'incidents de sécurité. Si des données personnelles sensibles ont été dérobées ou effacées, les collaboratrices et les collaborateurs exécutent les mesures immédiates fixées à l'avance. Outre l'isolement ou la mise hors service de certains services ou appareils, il est impératif d'annoncer toute violation de la sécurité des données au Préposé fédéral à la protection des données et à la transparence (PFPDT). En cas de soupçon d'acte délictueux, la police devrait être contactée au plus vite afin d'éviter que de possibles traces ne soient effacées. La police dispense des conseils et soutient les propriétaires de cabinets médicaux, notamment pour la question de savoir s'il y a lieu de payer ou non une éventuelle rançon.

Centre national pour la cybersécurité

Le Centre national pour la cybersécurité (NCSC) [5] offre également des aides et des informations supplémentaires. Le NCSC a notamment pour mission de protéger les infrastructures d'importance critique en Suisse dont le bon fonctionnement dépend des infrastructures informatiques. Le NCSC publie des rapports de situation qui résument les principales tendances et évolutions en matière de cybersécurité. Il informe en outre des incidents actuels survenus en Suisse et formule des recommandations plus détaillées, par ex. en lien avec différents types d'escroqueries possibles. Vous trouverez sur le site internet du NCSC (www.ncsc.admin.ch) de nombreux modes d'emploi et listes de contrôle, etc. pour exploiter de manière sécurisée votre infrastructure informatique. Vous pouvez aussi annoncer les cyberincidents au moyen du formulaire en ligne et obtenir des conseils pratiques.

Newsletter sur la cybersécurité

Les cybercriminels tirent parti d'événements actuels comme la pandémie de Covid-19 ou la guerre en Ukraine pour leurs activités de fraude. Le recours accru au télétravail ou un besoin croissant d'informations dans un environnement marqué par la peur et l'insécurité sont des facteurs qui ont entraîné une multiplication des cyberattaques pendant la pandémie [6].

La FMH aimerait attirer suffisamment tôt l'attention des cabinets médicaux sur l'existence des menaces actuelles au moyen d'une newsletter.

A l'avenir, la FMH aimerait attirer suffisamment tôt l'attention des cabinets médicaux sur l'existence des menaces actuelles au moyen d'une newsletter similaire à celles qui sont publiées, par ex., par le NCSC. Les cabinets médicaux intéressés peuvent s'inscrire à cette newsletter via l'adresse électronique cybersecurity[at]fmh.ch. Cette offre s'adresse aux cabinets médicaux individuels ainsi qu'aux cabinets médicaux qui, en raison de leur taille ou de leur forme d'organisation, ne disposent pas du personnel requis pour gérer l'infrastructure technique de sécurité.

Références
Liste complète des références sous www.bullmed.ch ou via code QR

FMH
Division Numérisation / eHealth
Elfenstrasse 18
CH-3000 Berne 15
Tél. 031 359 11 11
eHealth[at]fmh.ch

Crédits photo
Alexandersikov | Dreamstime.com