DOC
LE RENDEZ-VOUS
DES MÉDECINS
VAUDOIS

Cabinets médicaux face à l a cybercriminalité

La FMH vous conseille et vous soutient

Selon l'enquête actuelle du Swiss eHealth Barometer, les médecins jouissent d'une grande confiance de la part de leurs patient-es en ce qui concerne la protection et la sécurité des données.

Jusqu'à aujourd'hui, les médias avaient majoritairement relaté des cas de cyberattaques auprès de grands fournisseurs de soins américains. Le dégât principal était le vol de centaines de milliers de dossiers de patient-es contenant également des données sur des comptes bancaires. Ces derniers mois, ce ne sont pas seulement de grands établissements de santé qui ont été touchés, mais aussi de petites entreprises comme les cabinets médicaux.

La créativité des cybercriminel-les

Cela n'est finalement pas étonnant puisque les systèmes d'information exploités dans un cabinet médical sont mis en réseau et que les données sont échangées avec d'autres établissements du secteur de la santé. Une menace sérieuse provient de logiciels malveillants tels que les ransomwares (chevaux de Troie d'extorsion) qui se propagent via les pièces jointes des e-mails et cryptent les données. Les cybercriminel-les exigent ensuite une rançon pour le décryptage desdites données.

Les méthodes utilisées par les cybercriminel- les sont variées et les attaques ne sont souvent pas reconnaissables au premier coup d'oeil. Les victimes potentielles reçoivent de plus en plus souvent un e-mail les invitant à saisir des données confidentielles. Le contenu de ces messages peut être des factures fictives ou une demande de confirmation ou de mise à jour de ses propres comptes d'utilisateur. Début septembre 2022, le Centre national de cybersécurité (NCSC) a signalé des cas où des collaborateurs/trices reçoivent un courriel de leur imprimante multifonction qui prétend qu'un document numérisé a été envoyé et qu'il peut être téléchargé en cliquant sur un lien ou est disponible en pièce jointe. L'ouverture du fichier provoque alors le téléchargement d'un logiciel malveillant.

> Les cybercriminel-les collectent des informations librement disponibles sur Internet afin de lancer des attaques ciblées.

Développer un plan d'action

Les cybercriminel-les collectent des informations librement disponibles sur Internet afin de lancer des attaques ciblées. Toutefois, ils et elles peuvent également utiliser des informations provenant de comptes de messagerie déjà piratés. Ces messages donnent ainsi une impression de confidentialité et d'authenticité. Outre les mesures techniques, telles que le blocage des pièces jointes dangereuses, les collaborateurs/trices d'un cabinet médical doivent être conscient-es des risques et développer un plan d'action en cas de cyberincident.

La FMH met à la disposition de ses membres des outils leur permettant de mieux faire face aux cybermenaces. Des recommandations sur la protection informatique de base pour les cabinets médicaux sont ainsi librement accessibles sur son site web, et des informations sur les cybermenaces actuelles sont régulièrement transmises par newsletter.

Dr Alexander Zimmer
Membre du Comité central de la FMH, responsable du département Numérisation / eHealth

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.