La sécurité des données des patients, une priorité

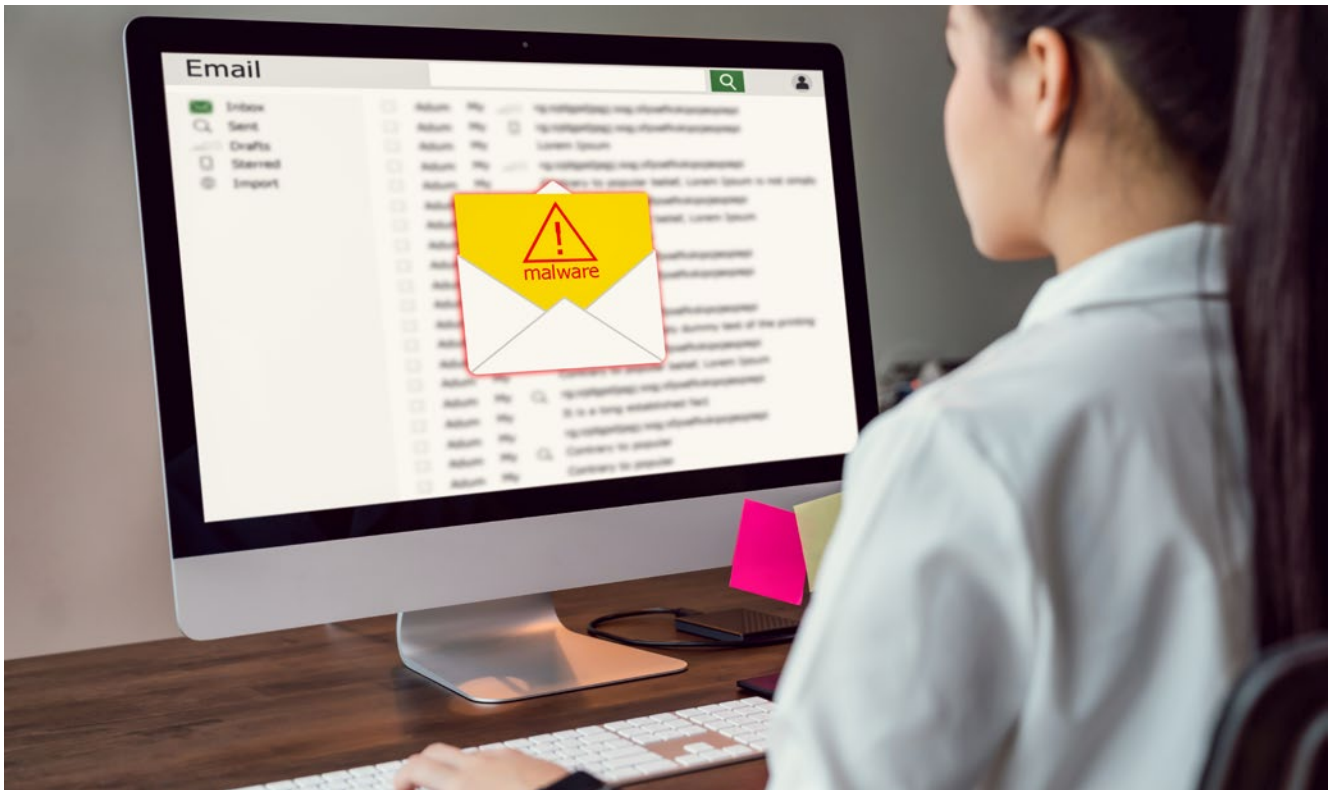
Les petites entreprises telles que les cabinets dentaires sont aussi **la cible des hackers.** Expert en sécurité informatique, Uwe Gempp nous explique comment les propriétaires de cabinet peuvent améliorer la sécurité des données de leurs patients.

Entretien : Andrea Renggli ; photo : Istock

Uwe Gempp, ce printemps les ordinateurs de plusieurs cabinets médicaux neuchâtelois ont été piratés. Les hackers ont volé les données de patients, menaçant de les publier si la rançon demandée n'était pas payée. Comment se fait-il que même des petits cabinets soient la cible de pirates informatiques ?
Les petites entreprises sont souvent concernées par ce type d'attaque. Non pas que les pirates les visent particulièrement, mais ils parcourent la Toile de manière automatisée 24 heures sur 24 et dès qu'ils détectent une faille, ils accèdent au système et analysent s'il est possible d'obtenir un gain important chez la victime. S'il s'agit d'un médecin-dentiste ou d'un médecin, on suppose que la victime sera plus encline à payer. D'une part, parce que son revenu est comparativement élevé et, d'autre part, parce que la publication des données de patients représente un risque réputationnel pour le cabinet.

Apparemment, tous les cabinets concernés utilisaient le même logiciel pour leurs dossiers électroniques des patients. Comment peut-on s'informer sur la sécurité d'un logiciel ?
Cela reste difficile à évaluer pour un non-spécialiste. Vous pouvez cependant demander à l'éditeur du logiciel quelles mesures de sécurité il applique régulièrement pour détecter et éliminer les failles du produit. Il existe d'ailleurs des certifications à ce sujet, la plus connue étant la série de normes ISO/IEC-27000. Il faut demander cette attestation.

Comment faut-il réagir après une attaque ?
Cela dépend des cas. Dès que vous constatez le piratage de l'ordinateur, il faut éteindre le système et le déconnecter du réseau, de façon à stopper la fuite des données. Le propriétaire du cabinet devrait aussi impérativement déclarer l'incident au Centre national pour la cybersécurité (NCSC, www.ncsc.admin.ch), qui lui fournira informations et assistance.



Plus on enregistrera de données numériques, plus le risque que des pirates cherchent à les monétiser va augmenter.

Comment devrait-on réagir aux demandes de rançon ?
Nous recommandons de ne pas céder au chantage et de déposer immédiatement plainte auprès de la police. En payant, on encourage les pirates, car chaque paiement augmente l'attractivité des attaques et fournit des moyens supplémentaires pour réaliser de nouvelles attaques. De plus, le paiement de la rançon ne vous garantit pas que les données seront restaurées ou qu'elles ne seront pas publiées par le pirate. Après avoir pénétré dans le système, les pirates agissent souvent en deux temps : ils exfiltrent les données, puis ils les cryptent. Ils promettent ensuite à la victime de lui livrer la clé de décryptage contre le paiement d'une rançon. Si celle-ci ne cède pas au chantage, ils demandent un montant supplémentaire pour ne pas publier les données volées. Mais même si l'on cède à cette exigence, on ne peut avoir aucune certitude sur ce qu'il adviendra des données.

Quelles mesures peut-on prendre pour éviter ce type de chantage ?
Il faut être attentif à la protection informatique élémentaire (voir encadré), qui comprend des mesures organisationnelles et techniques. Mais il faut aussi se poser des questions toutes simples. Le logiciel est-il à jour ? Est-ce que je fais régulièrement les mises à jour de sécurité ? L'antivirus est-il encore actuel ? Mes mots de passe sont-ils assez sûrs ? Est-ce qu'il y a des sauvegardes régulières du système ?

Comment peut-on se protéger contre les rançongiciels qui cryptent les données sur l'ordinateur ?
La meilleure protection consiste à faire des sauvegardes régulièrement et à enregistrer une copie de sécurité sur un dispositif externe. Nous conseillons aussi de se doter d'un appareil standalone, par exemple un ordinateur portable qui n'est pas connecté au réseau du cabinet. Cela permet de poursuivre les activités du cabinet même si l'ordinateur principal est attaqué et qu'il doit être éteint. Enfin, il vaut la peine d'être en contact avec un fournisseur de services informatiques que vous pourrez appeler en cas de cyberattaque. Cela vous évitera beaucoup de stress et en plus, vous bénéficierez d'une assistance plus rapide.

Dans un cabinet, l'ordinateur n'est pas le seul appareil connecté au réseau. Peut-on imaginer une attaque du système informatique du cabinet via ces dispositifs connectés ?
Oui, c'est tout à fait possible. Les dispositifs médicaux de marque présentent moins de risques, parce que la sécurité des appareils est une priorité des fabricants. Le problème vient plutôt des appareils bon marché que l'on achète dans le commerce, tels que des enceintes pour écouter de la musique ou des caméras de vidéosurveillance. Je ne connecterais pas ce genre d'appareils au réseau du cabinet, car la sécurité informatique n'est pas toujours une priorité de leurs fabricants et les failles connues ne sont pas réparées. Il vaut mieux connecter ces appareils à un réseau distinct, ce qui est possible avec la plupart des routeurs Internet. Vous trouverez des informations à ce sujet sur le site du NCSC : www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-iot.html.

Peut-on s'occuper de la sécurité informatique du cabinet soi-même ou faut-il obligatoirement faire appel à un expert ?
La plupart des propriétaires de cabinet peuvent s'en sortir par leurs propres moyens pour la protection informatique élémentaire. Il n'est pas nécessaire d'être informaticien pour cela. Il faut juste connaître le système d'exploitation et suivre une check-list (p. ex. www.hin.ch/fr/blog/protection-cyberattaques ou recommandations de la SSO sur les exigences minimales pour la sécurité informatique). De nombreux médecins-dentistes n'ont guère le temps de se pencher sur les questions d'informatique et ils accordent moins de priorité à ce sujet qu'à leur compétence métier qui est de traiter les patients de manière optimale. Il est toutefois important qu'ils prennent conscience du fait que l'ordinateur est devenu un outil de travail aussi essentiel que le fauteuil dentaire. Par conséquent, tout propriétaire de cabinet devrait aussi se préoccuper de la qualité et de la sécurité de son environnement informatique.

La numérisation du secteur de la santé va se poursuivre. Selon vous, quels sont les risques de cette évolution ?
Plus on enregistrera de données numériques, plus le risque que des pirates cherchent à les monétiser va augmenter. Le risque de cyberattaque va donc résolument s'accroître. Le grand avantage de la numérisation est qu'elle permet une meilleure mise en réseau, ce qui va déboucher sur une plus grande efficacité du système de santé. Nous ne pouvons pas échapper à cette évolution, mais nous pouvons apprendre à vivre avec les cyberrisques. Nous devons aussi accorder une plus grande priorité à la sécurité des données et rester sensibilisés aux défis liés au numérique.

Portrait

Uwe Gempp est Security Officer auprès de Health Info Net AG (HIN) depuis début 2022. Cette entreprise protège les données des patients dans le monde numérique et elle est considérée comme la norme en matière de communication sécurisée et de gestion des données sensibles par les experts de la santé suisses. Dans sa fonction d'architecte CSO & IT, Uwe Gempp est responsable de la sécurité de l'information auprès de HIN. Il fait état d'une longue expérience dans le secteur informatique.

Recommandations de la SSO sur la protection informatique élémentaire

En collaboration avec la FMH, la SSO a édité une publication intitulée « Exigences minimales pour la sécurité informatique des cabinets dentaires SSO » à l'attention de ses membres, dans laquelle elle présente quelques recommandations pour la protection informatique élémentaire du cabinet. Cette publication a pour but de soutenir les propriétaires de cabinet lors de la mise en place et de la maintenance de leurs plans de protection des données et de sécurité informatique. La publication ainsi qu'une affichette sur ce sujet sont disponibles dans l'espace sécurisé (cockpit) du site Web de la SSO (rubrique Documents SSO > Cabinets dentaires).