« La communication numérique devient plus complexe »

Le vol, voire l'usurpation de données est un phénomène en constante augmentation. Il est d'autant plus important que les cabinets médicaux **protègent les données de leurs patients et de leurs collaborateurs.**

Texte : Andrea Renggli, rédaction SDJ ; photo : Pixabay

De fausses annonces publicitaires qui conduisent à des sites Web frauduleux, de l'hameçonnage (phishing) au nom des CFF avec un prétendu jeu-concours ou des courriels frauduleux provenant soi-disant de la police : cet automne, en l'espace d'une seule semaine, le Centre national pour la cybersécurité (NCSC) a reçu 1517 annonces de cyberincidents en Suisse, soit le nombre le plus élevé au cours des douze derniers mois. Mais en réalité, ce nombre est sans doute largement sous-estimé.

Comment peut-on se protéger de ces attaques ou tentatives de manipulation récurrentes, notamment dans un cabinet dentaire qui conserve et traite des données particulièrement sensibles de patients ?

Tout appareil contaminé est un danger sur Internet

Je décide de me renseigner auprès d'un expert en la personne de Rolf Lanz, professeur de communication de données et de sécurité informatique à la Haute école spécialisée bernoise. Il m'appelle quelques jours plus tard. Il a ouvert et lu mon courriel bien qu'il ne connaissait pas l'expéditeur et que j'avais joint un fichier Word. Mais une recherche rapide lui a permis de constater que j'étais sans doute bel et bien la personne que j'affirmais être.

Première leçon en matière de cybersécurité : ne pas ouvrir des e-mails d'un expéditeur inconnu, surtout lorsqu'un document est joint. Même des fichiers Office normaux peuvent contenir un vi-

Les dommages occasionnés par les pirates informatiques augmentent chaque année. Les hackeurs peuvent prendre le contrôle de tout appareil contaminé qui représente ainsi un danger sur Internet.

rus qui infecte l'ordinateur dès l'ouverture du document. Il faudrait, si nécessaire, appeler la personne et lui demander si elle est réellement à l'origine de l'envoi.
Cela me semble quelque peu compliqué dans mon quotidien professionnel, dans lequel je suis amenée à envoyer et à recevoir des dizaines de courriels par jour. La possibilité de communiquer simplement et rapidement par e-mail a extrêmement simplifié nos vies. Cet avantage serait réduit à néant si je devais appeler chaque expéditeur inconnu.
La communication numérique deviendra beaucoup plus complexe à l'avenir qu'elle ne l'a été jusqu'à maintenant, confirme Rolf Lanz. Car les « dommages occasionnés par des pirates informatiques augmentent, hélas, massivement chaque année. Les hackeurs peuvent prendre le contrôle de tout appareil contaminé qui représente ainsi un danger sur Internet, lequel pourrait toutefois être évité par une utilisation correcte des moyens informatiques. »

Évaluer le risque résiduel d'une attaque
Un autre exemple de communication plus complexe est l'authentification à deux facteurs, qui est désormais possible, voire obligatoire, dans de nombreux systèmes. Étant donné que nous travaillons sur diverses plates-formes et avec différents fournisseurs dans notre quotidien professionnel, cette mesure de sécurité est jugée chronophage et laborieuse. Mais Rolf Lanz précise que « pour tous les systèmes et données auxquels on peut accéder depuis l'Internet, l'authentification à deux facteurs est actuellement LA ‹ norme › impérative dans les échanges professionnels. Cela concerne tout particulièrement les données médicales des patients. »
Mais le standard FIDO2 met déjà des techniques à disposition qui simplifient considérablement le quotidien tout en garantissant une sécurité encore plus élevée (voir encadré). FIDO2, dont l'acronyme signifie « Fast IDentity Online », remplace les mots de passe lors de l'inscription à des services en ligne. Les efforts à fournir initialement ne doivent toutefois pas être sous-estimés, estime Rolf Lanz.
Où se situe donc la limite pour pouvoir travailler en toute sécurité moyennant un effort raisonnable ? Rolf Lanz recommande, d'une manière générale, de veiller à ce que la sécurité informatique soit aussi élevée que le permet un prix encore abordable, tout en étant capable de supporter le risque résiduel en cas d'attaque.

Des erreurs fréquentes
L'ouverture de pièces jointes à des courriels d'origine inconnue est l'erreur la plus courante commise par les utilisateurs en matière de sécurité informatique, précise Rolf Lanz. Mais selon lui, le fait de cliquer sur des liens dans des courriers indésirables, de naviguer sur des sites douteux ou non nécessaires à l'activité professionnelle, d'ignorer les mises à jour et de ne pas utiliser les versions logicielles actuelles des applications installées est aussi fréquemment à l'origine d'une cyberattaque. Il ajoute que « les affaires professionnelles et privées devraient absolument être gérées sur des comptes et des systèmes séparés. Autrement dit, les ordinateurs professionnels avec les comptes correspondants doivent être différents des ordinateurs portables et des comptes privés. »
Le problème est aggravé par le fait que les instruments d'intelligence artificielle rendent les spams de plus en plus crédibles. Selon Rolf Lanz, quelques mesures personnelles simples permettent également d'y remédier. Il ne faut notamment pas ouvrir les spams et les supprimer directement. Il convient de vérifier attentivement les adresses e-mail d'expéditeurs inconnus – pas seulement le nom affiché de l'expéditeur, mais l'adresse d'expédition effectivement utilisée (voir encadré).
L'entreprise doit, en outre, faire analyser tous les courriels par un logiciel antimalware local (scanner de virus) avant leur distribution. De plus, les courriels peuvent également être contrôlés par le fournisseur d'accès Internet. Cette prestation est toutefois payante.

Les attaques sur les PME peuvent rapporter gros
Rolf Lanz explique que les PME, mais aussi les petites entreprises artisanales et de services, peuvent être des cibles très lucratives pour les hackeurs. « Peu de ces entreprises investissent suffisamment dans leur infrastructure informatique, elles présentent donc souvent des points faibles connus. Les pirates informatiques les connaissent et s'en servent pour passer à l'acte. Plus une entreprise dépend d'une infrastructure informatique fonctionnelle, plus elle devient intéressante pour une tentative d'extorsion, par exemple une demande de rançon contre la libération des données préalablement cryptées par l'attaquant au moyen d'un rançongiciel. »
Les données des patients enregistrées dans les cabinets dentaires sont une cible très lucrative pour un pirate informatique, si l'on en croit l'expert. « Il s'agit de données médicales particulièrement sensibles, qui ne doivent pas tomber entre les mains de tiers. Elles se prêtent donc parfaitement à un chantage, lorsque le pirate menace de publier les données volées. »

Mesures pour augmenter la sécurité informatique
Les mesures suivantes sont, selon Rolf Lanz, des exigences essentielles pour augmenter la sécurité informatique :
- Ne connecter le réseau local à l'Internet que via un pare-feu correctement configuré.
- Installer en temps utile toutes les mises à jour disponibles.
- Utiliser les versions actuelles des logiciels.
- Créer des sauvegardes quotidiennes selon la règle 3-2-1 (voir encadré)
- Utiliser exclusivement des comptes individuels.
- Ne pas créer de comptes généraux utilisés par plusieurs personnes.
- Ne pas utiliser de comptes avec des droits d'administrateur (root ou admin) pour le travail quotidien.
- Faire contrôler et, si nécessaire améliorer, la sécurité informatique actuelle à intervalles réguliers (chaque année environ) par un spécialiste digne de confiance.

Liens utiles

Conseils du NCSC pour les entreprises :
www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen.html

Règle des 3-2-1 pour les sauvegardes :
www.synology.com/de-de/dsm/solution/data_backup (en allemand)

Informations à propos de FIDO2 :
www.forgerock.com/fr/resources/whitepaper/go-passwordless-authenticate-securely

Informations sur l'adresse e-mail d'expédition effectivement utilisée :
www.spamhaus.com/de/resource-center/source-code-bosartiger-e-mails/ (en allemand)