Les cyberattaques dans le secteur de la santé sont une réalité

Rosmarie Borle Oussama Zgheb La numérisation étend son influence dans les domaines les plus divers de la vie privée et professionnelle. Les risques et menaces, en particulier dans le secteur de la santé, s'en voient par conséquent augmentés. La protection des communications par le cryptage est plus importante que jamais, pourtant elle ne saurait suffire à l'heure actuelle. Une Interview avec l'expert de HIN, Oussma Zgheb

Oussama Zgheb, expert en sécurité informatique chez Health Info Net AG (HIN), explique, pourquoi la sensibilisation et la responsabilisation des professionnels de la santé (regroupées sous le terme Awareness) jouent un rôle croissant.

Une ergothérapeute ouvre son cabinet et se prépare à une nouvelle journée. Un matin comme les autres, pourrait-on penser. Mais lorsqu'elle essaie de démarrer l›ordinateur, rien ne marche. Les données ont été cryptées pendant la nuit par un cheval de Troie cryptographique – un logiciel malveillant qui rend tous les fichiers de l'ordinateur inutilisables pour la victime. L'ergothérapeute n'a même plus accès aux rendez-vous ni aux coordonnées des patients. À leur place, un «écran de verrouillage» apparaît, qui lui demande de verser aux pirates une certaine somme en bitcoins, afin que les fichiers puissent être décryptés. Qu›elle se laisse prendre au chantage par les pirates ou non: elle a perdu le contrôle de ses fichiers; les données ont peut-être disparu pour toujours – ou sont depuis longtemps sur des serveurs Internet douteux.

Cette histoire est fictive. Cependant, le scénario de menace sous-jacent est parfaitement réel. Ces derniers mois, les médias ont rapporté plusieurs cas dans lesquels des hôpitaux entiers ont été paralysés par des chevaux de Troie cryptographiques. Rien d'étonnant que les données sensibles relatives à la santé soient une cible de prédilection des pirates informatiques. «Ergothérapie» s'est entretenu avec Oussama Zgheb au sujet des menaces actuelles et des mesures défensives appropriées.

Quelles conséquences un cas comme celui décrit ci-dessus pourrait-il avoir pour un ergothérapeute touché?

Oussama Zgheb: La conséquence immédiate serait une certaine pagaille au cabinet si la planification des rendez-vous et les dossiers électroniques des patients n'étaient soudainement plus disponibles. Toutefois, les conséquences à long terme seraient encore plus dramatiques. Une attaque de pirates informatiques peut avoir pour conséquence la transmission de données sensibles à des personnes malveillantes ou même leur divulgation au public. Imaginez la perte de confiance des patients ou des médecins traitants. Ils auraient l›impression que leurs données sont traitées de manière négligente – une catastrophe pour le cabinet et les ergothérapeutes qui y travaillent.

«La protection infaillible n'existe pas.»

Que pouvons-nous entreprendre pour nous protéger contre les menaces virtuelles?

Les dangers de la numérisation sont nombreux et variés. Les mesures de protection envisageables sont donc multiples. Ces mesures peuvent être divisées en trois catégories: les mesures de protection techniques, organisationnelles et comportementales. Je vous le dis franchement: il n'existe pas de protection infaillible. Cependant, il est important de maintenir le niveau de protection si élevé que l'effort d'une attaque n›en vaille pas la peine pour un pirate informatique. L'homme, et donc aussi un agresseur, suit toujours la loi physique du «moindre effort». Par conséquent, vous pouvez augmenter considérablement votre protection sans grands efforts.

Je suppose qu'un programme antivirus sur mon ordinateur serait une telle mesure technique?

Exactement, les mesures de protection techniques comprennent un antivirus ou un pare-feu. Ces deux mesures peuvent être mises en œuvre sans grand ef-

Oussama Zgheb
Responsable de l'ingénierie et de la sécurité, Health Info Net AG (HIN)
Par son statut de Security Officer, Oussama Zgheb est responsable de la promotion et du contrôle de la sécurité de l'nformation. En tant que responsable Engineering et Security, il supervise la direction des ressources de développement et la coordination des projets de développement.

fort et améliorent considérablement la protection de vos équipements. Il est également conseillé de toujours installer les mises à jour dès leur parution – de préférence automatiquement – afin de combler immédiatement les failles de sécurité.

Si vous n'êtes pas particulièrement expert en informatique ou préférez vous concentrer sur votre cœur de métier, vous pouvez également déléguer la protection technique de vos appareils à un partenaire spécialisé dans ce domaine. Nos prestations de services à cet égard sont proposées sous forme d'« Endpoint Security Service», lequel inclut un logiciel de protection moderne pour les outils et la connexion au centre d'opérations de sécurité HIN. En cas d'attaque, nos experts en sécurité vous aident à libérer vos outils des logiciels malveillants.

«Le meilleur détecteur de virus est inutile si les collaborateurs ne sont pas sensibilisés.»

Que dois-je imaginer dans le cadre des mesures organisationnelles?

Les mesures techniques seules ne suffisent pas. Le meilleur et le plus onéreux antivirus est inutile, si les personnes qui travaillent avec l'appareil en question ne maîtrisent pas les règles de base de la sécurité informatique. C'est là q'›interviennent les mesures organisationnelles. Il s'agit notamment de lignes directrices, par exemple concernant le traitement des données à caractère personnel, mais aussi de processus efficients, comme des sauvegardes régulières – si vous possédez une copie complète de vos données stockées à un endroit sûr, il sera plus difficile de vous faire chanter. La formation des employés est un aspect capital. Ils doivent être formés régulièrement afin d'être conscients des risques et d'adopter un comportement soucieux de la sécurité – par exemple, ne pas ouvrir à la légère une pièce jointe suspecte d'un e-mail. C'est ce que nous appelons «Awareness». HIN organisera une telle session de formation cet automne, en collaboration avec le SVE. Par ailleurs, nous avons développé un outil d›apprentissage en ligne permettant de rafraîchir régulièrement les connaissances des utilisateurs. Je tiens à souligner encore que la sécurité des données est l›affaire du patron. Les mesures organisationnelles doivent être initiées, soutenues et appliquées «d'en haut».

«Un fournisseur digne de confiance ne demande jamais un mot de passe par e-mail ou par téléphone.»

Vous avez également parlé de mesures comportementales. Quelles sont-elles?

Les mesures comportementales constituent le troisième pilier de la sécurité informatique, après la technologie et l'organisation. Il ne faut surtout pas le négliger. Voici un exemple: l'ensemble des mesures de sécurité techniques et organisationnelles peuvent être contournées si le mot de passe choisi est facile à deviner – ou s'il est affiché sur un post-it à côté de l'ordinateur... Une des principales règles de conduite est donc de choisir des mots de passe sûrs et de les garder secrets. Une autre mesure comportementale importante est la dissociation stricte des données privées et professionnelles. Cela signifie que vous ne devez pas utiliser votre adresse e-mail professionnelle à des fins privées – par exemple pour vous connecter à vos comptes de médias sociaux.

Qu'est-ce qu'un mot de passe sécurisé?

Un mot de passe sécurisé est complexe et doit comporter au moins dix à douze caractères – lettres majuscules et minuscules, chiffres et caractères spéciaux. En outre, il ne doit pas faire référence à des personnes. N'utilisez donc pas de dates de naissance, de plaques d'immatriculation ou de numéros de téléphone comme mots de passe. Il est important de définir un mot de passe différent pour chaque accès. Si, par exemple, votre compte de messagerie est piraté, il sera facile pour un pirate d'accéder à votre identifiant d'e-banking si vous y utilisez le même mot de passe. Vous pouvez également définir l'authentification à deux facteurs lorsqu'elle est disponible. En plus du mot de passe, un deuxième composant de connexion est alors nécessaire, par exemple un code SMS. Ceci empêche un pirate d'accéder au service correspondant, même s›il a piraté le mot de passe requis. L'authentification à deux facteurs est indispensable dans le domaine des soins de santé. La logique veut que l'on s'en serve aussi autant que possible dans le cadre de l'usage privé.

ABONNEMENT HIN EVS: LA SOLUTION ASSOCIATIVE AVANTAGEUSE

Les ergothérapeutes entretiennent un contact étroit avec les médecins de famille, les hôpitaux et les caisses d'assurance-maladie. En cas de collaboration entre différentes disciplines, le raccordement HIN rend l'échange d'informations électroniques simple, sûr et conforme aux règles de la protection des données. De plus, il sécurise l'accès au dossier électronique du patient. En tant que membre EVS, vous obtenez le raccordement HIN à des conditions avantageuses. L'abonnement exclusif HIN EVS vous permet de communiquer par voie électronique, en toute sécurité, avec tous les prestataires de services et les patients, conformément aux exigences légales.

Plus d'informations et inscription www.hin.ch/evs

Avez-vous d'autres conseils comportementaux que les ergothérapeutes peuvent facilement appliquer?
Même si cela ne semble pas évident: soyez méfiant! Nous avons tous tendance à ne pas accuser d'emblée une personne de mauvaises intentions. Cela vaut également pour l'espace numérique. Un tel bénéfice du doute peut toutefois avoir de graves conséquences, car les cybercriminels exploitent la bonne foi et la négligence de manière ciblée et impitoyable. Il serait sain d'adopter une attitude fondamentalement critique et vigilante. Une attention particulière devrait être accordée aux courriels provenant d'expéditeurs inconnus. Les attaques dites de phishing, dans lesquelles les fraudeurs tentent d'obtenir des données confidentielles d'internautes peu méfiants, sont souvent structurées de telle sorte qu'elles suscitent la peur ou la pression sur le destinataire. Dans une telle situation, il faut être capable de résister à l'envie de réagir sous l'émotion et de garder la tête froide. Toutes les sonnettes d'alarme devraient retentir lorsqu'on vous demande votre nom d'utilisateur et votre mot de passe. Les fournisseurs sérieux ne demandent jamais les données de connexion d'un utilisateur par e-mail ou par téléphone.

FORMATION CONTINUE HIN/EVS DANS LE DOMAINE DE LA SÉCURITÉ ET DE LA SENSIBILISATION À LA SÉCURITÉ INFORMATIQUE

Non seulement les hôpitaux et les homes, mais aussi les cabinets thérapeutiques et autres établissements de soins sont des cibles privilégiées des cybercriminels. Les attaques de pirates informatiques ayant de graves conséquences, telles que la perte de données, la violation de la confidentialité des patients ou des dommages financiers, sont de plus en plus fréquentes. Au cours de cette formation, vous découvrirez les mesures de sécurité importantes et les outils nécessaires pour vous protéger de manière optimale contre les dangers liés à la numérisation.
Date et lieu: 14 septembre 2019, de 9h00 à 11h30, Zurich (voir page 45)
Informations complémentaires et inscription: www.ergotherapie.ch