DIE BEDROHUNG DURCH CYBERANGRIFFE IST REAL!

Lucas Schult

IT-Leiter (CIO) und Stv. Geschäftsführer der Health Info Net AG

Die Risiken und Bedrohungen in der digitalen Welt nehmen laufend zu. Daher reicht es längst nicht mehr, die Kommunikation durch Verschlüsselung zu schützen und den Zugriff zu sichern. Lucas Schult, IT-Sicherheitsexperte der Health Info Net AG, verrät, weshalb auch der Schutz von Endgeräten und insbesondere die Awareness von Gesundheitsfachpersonen eine immer zentralere Rolle spielen.

Eine MPA betritt am Morgen die Praxis. Ein Morgen wie jeder – könnte man meinen. Doch als sie versucht, den Computer zu starten, geht nichts mehr. Die Daten wurden durch einen Krypto-Trojaner verschlüsselt und die MPA hat nicht einmal mehr Zugriff auf Termine und Kontaktangaben der Patienten.
Von Szenarien wie diesem hört man heute leider immer wieder. Die Verschlüsselung von Daten durch Krypto-Trojaner mit anschliessender Erpressung durch Hacker sind vermehrt auch im Gesundheitswesen ein Thema. Die sensiblen Daten des Gesundheitswesens sind ein beliebtes Ziel von Hackern.

«Vollkasko bezüglich Sicherheit gibt es nicht.»

Nicht nur die Verletzung des Berufsgeheimnisses und der Verstoss gegen den Datenschutz könnten Folgen eines solchen Angriffes sein. Das Chaos, das in der Praxis entsteht, wenn keine Termine mehr verfügbar sind, die Patienten im Wartezimmer warten und die MPA nicht mehr weiss, warum der Termin überhaupt vereinbart wurde, gehört zu den harmloseren Folgen. Wenn der behandelnde Arzt nicht auf behandlungsrelevante Dokumente zugreifen kann, können die Konsequenzen für den Patienten sogar lebensgefährlich sein.

Wenig Aufwand – mehr Schutz

Die Gefahren, welche die Digitalisierung mit sich bringt, sind vielseitig und lassen sich nicht verleugnen. Den Bedrohungen aus dem Internet ist man allerdings nicht hilflos ausgeliefert. Mit verhältnismässig wenig Aufwand wird der Schutz vor Cyberangriffen massiv erhöht: *«Einen 100-prozentigen Schutz bezüglich Sicherheit gibt es nicht. Es lohnt sich jedoch, den Schutz so hoch wie möglich zu halten»*, so Lucas Schult.

Eine Kombination von Massnahmen

Viele Schutzmassnahmen sind ohne grossen Aufwand umzusetzen und erhöhen den Schutz der Geräte massiv. Die wichtigsten Schutzmassnahmen lassen sich in drei Kategorien einteilen: technische, organisatorische und verhaltensbezogene Schutzmassnahmen. Zu den technischen Schutzmassnahmen gehören unter anderem der Schutz von Arbeitsgeräten mit einer Firewall und einem Virenscanner. Ausserdem ist es empfehlenswert, Updates immer umgehend zu installieren, um Sicherheitslücken sofort zu schliessen. HIN bietet hier beispielsweise den Endpoint Security Service an, der modernste Schutzsoftware für Arbeitsgeräte bietet und zusätzlich mit dem HIN Security Operation Center ergänzt wird. Damit kann das System vor Bedrohungen geschützt werden, und im Ernstfall werden betroffene Kunden durch erfahrene Sicherheitsexperten proaktiv betreut.

Lucas Schult

HIN

Health Info Net AG
Tel. 0848 830 740
lucas.schult@hin.ch
www.hin.ch

«Der beste Virenscanner ist nutzlos, wenn die Awareness der Mitarbeitenden fehlt.»

Doch technische Massnahmen alleine reichen nicht aus: *«Der beste und teuerste Virenscanner nützt nichts, wenn die Personen, die mit dem Gerät arbeiten, nicht in Bezug auf IT-Sicherheit ausgebildet wurden»*, so Lucas Schult.

Und hier kommen die organisatorischen Massnahmen ins Spiel. Ein Virenscanner kombiniert mit einer gut ausgebildeten MPA erhöht den Schutz massiv. Die regelmässige Schulung von Mitarbeitern ist also essentiell – hier bietet HIN beispielsweise Awareness Schulungen vor Ort oder via eLearning (Awareness Portal) an.

Eine MPA, welche die wichtigsten Verhaltensregeln in Bezug auf IT-Sicherheit kennt, kann unter Umständen grossen Schaden verhindern. Würde beispielsweise die Antivirussoftware bei der Überprüfung eines E-Mail-Anhanges versagen, könnte eine in Awareness geschulte MPA Schaden verhindern, indem sie den Anhang nicht einfach unüberlegt öffnet.

Die Wahl des Passworts

Zu den wichtigen Verhaltensregeln im Zusammenhang mit IT-Sicherheit gehört auch die Wahl eines sicheren Passwortes. Die gesamten Sicherheitsvorkehrungen sind nutzlos, wenn das gewählte Passwort leicht zu erraten ist. Doch was macht ein sicheres Passwort aus? Lucas Schult weist diesbezüglich auf die folgenden Punkte hin: Ein sicheres Passwort ist komplex und sollte aus mindesten zehn bis zwölf Zeichen (Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen) bestehen. Zudem darf es keinen Bezug zur Person haben (Geburtsdatum, Auto-Kennzeichen, Telefonnummer etc.). Es ist wichtig, nicht dasselbe Passwort für unterschiedliche Accounts zu verwenden. Wird beispielsweise ein E-Mail-Konto geknackt, ist es für die Hacker ein Leichtes, an das E-Banking-Login zu kommen, wenn dort dasselbe Passwort verwendet wurde.

2-Faktor-Authentisierung nutzen

Die 2-Faktor-Authentisierung (Identitätsnachweis eines Nutzers mittels zweier unterschiedlicher und unabhängiger Faktoren) ist im Gesundheitswesen state-of-the-art und von Gesetzes wegen vorgeschrieben.

Wo immer eine 2-Faktor-Authentisierung angeboten wird, ist es empfehlenswert, diese zu nutzen.
Da bei dieser Art der Authentisierung immer zwei Komponenten für den Zugriff benötigt werden, kann ein Hacker nicht auf den jeweiligen Dienst zugreifen, selbst wenn er das benötigte Passwort geknackt hat.

Misstrauisch sein

Als Grundsatz gilt: kritisch sein. Misstrauen in Bezug auf Cyberkriminalität ist immer angebracht. Aufmerksamkeit ist insbesondere bei E-Mails von unbekannten Absendern geboten.

«Ein seriöser Dienstleister wird nie per E-Mail oder Telefon nach dem Passwort fragen.»

Phishing-Attacken, bei denen Betrüger versuchen, an vertrauliche Daten ahnungsloser Internet-Nutzer zu kommen, sind oft so aufgebaut, dass sie beim Empfänger Angst auslösen oder Druck auf ihn ausüben. Skepsis ist insbesondere dann angebracht, wenn in einer E-Mail nach Benutzername und Passwort gefragt wird. Seriöse Anbieter fragen nie per E-Mail nach den Login-Daten eines Nutzers.
Mit einigen einfachen technischen Massnahmen der Sensibilisierung und regelmässigen Schulungen in Bezug auf Cyberkriminalität ist bereits ein wichtiger Schritt in Richtung integraler Sicherheit getan.

Lucas Schult fasst zusammen: *«Erfolg verspricht die richtige Kombination technischer und organisatorischer Schutzmassnahmen, sowie einige essentielle Verhaltensregeln, die befolgt werden sollten.»*

LA MENACE DES CYBERATTAQUES EST BIEN RÉELLE

Lucas Schult

Responsable IT (CIO) et directeur adjoint de la société Health Info Net AG (HIN)

Dans le monde numérique, les risques et les menaces ne cessent d'augmenter. Il ne suffit plus de crypter les communications et de sécuriser l'accès aux données pour s'en prémunir. Lucas Schult, expert en sécurité informatique chez Health Info Net AG, nous explique ci-après pourquoi la protection des terminaux et en particulier la sensibilisation des professionnels de la santé jouent un rôle toujours plus important.

Cela aurait dû être un matin comme un autre. Une assistante médicale se rend au cabinet pour son travail ; mais au moment d'allumer l'ordinateur, plus rien : les données ont été chiffrées par un cheval de Troie et l'assistante médicale n'a plus aucun accès ni à l'agenda ni aux coordonnées des patients.

Les scénarios comme celui-ci sont malheureusement en constante augmentation. Le milieu de la santé n'est pas épargné par le chiffrage de données suivi d'une demande de rançon de la part du pirate informatique. En effet, les données sensibles de ce secteur constituent une cible particulièrement appréciée des pirates.

« Il n'existe aucune protection complète en matière de sécurité. »

La violation du secret médical et de la protection des données n'est pas la seule conséquence de ce type d'attaques. Quant au chaos dans lequel se retrouve le cabinet lorsque l'agenda n'est plus accessible, que les patients attendent et que l'assistante médicale ne sait même plus pourquoi les rendez-vous ont été pris,

il fait partie des conséquences les moins graves. La situation peut en revanche prendre une toute autre tournure lorsque le médecin traitant n'a plus accès aux dossiers médicaux ; dans ce cas, c'est la vie des patients qui peut être en jeu.

Une sécurité accrue grâce à des mesures simples

Si l'on ne peut nier les dangers du monde numérique et les nombreuses menaces que représente internet, des solutions existent pour se protéger. Grâce à quelques mesures simples, il est possible de diminuer sensiblement le risque de cyberattaque : *« La protection à 100% n'existe pas mais il vaut la peine de tout mettre en œuvre pour s'en prémunir le mieux possible »*, explique Lucas Schult.

Une combinaison de mesures

Les mesures de protection peuvent être classées en trois catégories : les mesures techniques, organisationnelles et comportementales. Parmi les mesures techniques figure notamment la protection des outils de travail à l'aide d'un pare-feu et d'un logiciel antivirus. Il est également vivement recommandé d'installer sans attendre les nouvelles mises à jour afin de corriger immédiatement les failles de sécurité. HIN propose par exemple le logiciel Endpoint Security Service, un logiciel de protection moderne qui peut être complété par le Security Operation Center. Il est ainsi possible de protéger les systèmes contre les menaces et d'être pris en charge de manière proactive par des experts en sécurité expérimentés en cas d'urgence.

« Le meilleur antivirus ne sert à rien si les collaborateurs n'ont pas été sensibilisés. »

Seules, les mesures techniques ne sont toutefois pas suffisantes : *« Le meilleur antivirus ne sert à rien si les utilisateurs n'ont pas été formés à la sécurité informatique »*, poursuit Lucas Schult.

C'est ici que les mesures organisationnelles entrent en jeu. Un antivirus combiné à une assistante médicale bien informée permet d'améliorer sensiblement la sécurité. La formation régulière des collaborateurs revêt une importance essentielle ; HIN propose des formations et sensibilisations au cabinet ou à distance (Awareness Portal).

Une assistante médicale qui connaît les principales règles comportementales en matière de sécurité informatique peut contribuer à éviter des dommages importants. Lorsque le logiciel antivirus échoue lors de la vérification d'une pièce jointe, une assistante médicale sensibilisée saura qu'il lui faut éviter de l'ouvrir si elle a le moindre doute.

Le choix du mot de passe

Parmi les principales règles comportementales en matière de sécurité informatique figure également le choix d'un bon mot de passe. Toutes les autres précautions ne servent à rien si le mot de passe choisi est facilement identifiable. Voici les conseils de Lucas Schult pour choisir un mot de passe sécurisé : le mot de passe choisi doit être complexe et se composer d'au moins dix à douze caractères (majuscules et minuscules, nombres et caractères spéciaux). Le recours à des informations personnelles est à proscrire (date de naissance, numéro de plaque ou de téléphone, p. ex). Il est par ailleurs important de ne pas utiliser le même mot de passe pour différents comptes, car si un de ces comptes est piraté (messagerie, p. ex.), le pirate peut alors facilement accéder aux autres comptes de l'utilisateur comme le e-banking par exemple.

Activer la validation en deux étapes

La validation en deux étapes (identification de l'utilisateur au moyen de deux facteurs différents et indépendants) est LA méthode à privilégier dans le secteur de la santé et elle est du reste préconisée par le législateur. Il est donc vivement recommandé d'activer systématiquement cette fonction lorsqu'elle est proposée.
Comme cette méthode a toujours recours à deux modes d'authentification pour autoriser l'accès à un service, les pirates ne peuvent pas y accéder même s'ils ont piraté le mot de passe.

Faire preuve de méfiance

De manière générale, il convient de faire preuve de méfiance en matière de cybercriminalité. Une attention particulière est requise notamment lors de la réception de messages de la part d'expéditeurs inconnus.

« Un prestataire sérieux ne demandera jamais un mot de passe par courriel ou par téléphone. »

Les attaques par hameçonnage (ou phishing), lors desquelles les pirates tentent d'accéder à des données confidentielles en exploitant la crédulité des utilisateurs, sont souvent conçues de manière à susciter la peur de ce dernier ou d'exercer une pression sur lui. Il est donc important de se montrer sceptique lorsque l'on reçoit un message demandant de communiquer son identifiant ou son mot de passe. Les prestataires sérieux ne demanderont jamais ces données par courrier électronique.
Grâce à quelques mesures techniques simples, à la sensibilisation à la cybercriminalité et à la formation des utilisateurs, un pas important peut être franchi en direction d'une sécurité informatique intégrale.

Et Lucas Schult de conclure *: « La juste combinaison de mesures de protection techniques et organisationnelles, couplée à quelques règles comportementales de base, sont la clé du succès. »*