«Die digitale Kommunikation wird aufwändiger»

Immer häufiger wird bekannt, dass Daten in die Hände von Betrügern geraten. Deshalb ist es gerade für medizinische Praxen so wichtig wie nie zuvor, **Daten ihrer Patienten und Mitarbeiter zu schützen.**

Text: Andrea Renggli, Redaktion SDJ; Foto: Pixabay

Gefälschte Werbeanzeigen, die auf betrügerische Websites führen, Phishing im Namen der SBB mit einem angeblichen Gewinnspiel, oder Betrug-E-Mails, die den Absender der Polizei tragen: In einer einzigen Woche im Herbst 2023 gingen beim Nationalen Zentrum für Cybersicherheit (NCSC) 1517 Meldungen zu Cybervorfällen in der Schweiz ein.
Das ist der höchste Wert in den vergangenen zwölf Monaten. In Wirklichkeit dürfte es sogar um ein Vielfaches mehr sein.
Wie kann man sich vor diesen allgegenwärtigen Angriffen oder Manipulationen schützen? Insbesondere in einer Zahnarztpraxis, wo besonders schützenswerte Daten der Patientinnen und Patienten gespeichert und bearbeitet werden?

Jedes verseuchte Gerät ist eine Gefahr im Internet

Ich frage nach bei einem Experten. Rolf Lanz ist Professor für Data Communication und IT Security an der Berner Fachhochschule. Einige Tage später ruft er mich an. Er habe meine E-Mail geöffnet und gelesen, obwohl er den Absender nicht kannte und ich ein Word-Dokument mitgeschickt hatte. Eine kurze Recherche habe aber ergeben, dass ich wohl tatsächlich die Person bin, die ich behaupte zu sein. Meine erste Lektion in Sachen Cybersicherheit: Keine E-Mail eines unbekannten Absenders öffnen, schon gar nicht, wenn ein Dokument angehängt ist. Auch normale Office-Dokumente können einen Virus enthalten, der den Computer infiziert, sobald das Dokument geöffnet wird. Falls nötig sollte man die Person kurz anrufen und fragen, ob die E-Mail tatsächlich von ihr stammt.

Der durch Angreifer verursachte Schaden wird Jahr für Jahr grösser. Jedes verseuchte Gerät kann durch Hacker missbraucht werden und ist somit eine Gefahr im Internet.

Das scheint mir für den beruflichen Alltag, in dem ich täglich Dutzende E-Mails verschicke und empfange, untauglich. Die Möglichkeit, per E-Mail unkompliziert und schnell miteinander zu kommunizieren, hat das Leben extrem erleichtert. Wo bleiben diese Vorzüge, wenn ich jeden unbekannten Absender zurückrufen soll?
Die digitale Kommunikation werde in Zukunft sehr viel aufwendiger werden, als sie bisher war, bestätigt Rolf Lanz. Denn: «Der durch Angreifer verursachte Schaden wird leider jedes Jahr immer noch deutlich grösser. Jedes verseuchte Gerät kann durch Hacker missbraucht werden und ist somit eine Gefahr im Internet, die durch einen korrekten Umgang mit den IT-Mitteln vermieden werden könnte.»

Das Restrisiko eines Angriffs abschätzen
Ein weiteres Beispiel für die aufwändigere Kommunikation ist die Zweifaktorauthentifizierung, die mittlerweile in vielen Systemen möglich oder gar vorgeschrieben ist. Weil wir im beruflichen Alltag mit verschiedenen Plattformen und Anbietern arbeiten, wird diese Sicherheitsmassnahme als zeitraubend und mühselig empfunden. Aber Rolf Lanz betont: «Für alle Systeme und Daten, auf die aus dem Internet zugegriffen werden kann, ist heute eine Zweifaktorauthentifizierung DER «Standard» und für geschäftliche Zwecke zwingend notwendig. Dies gilt insbesondere für die Gesundheitsdaten der Patienten.» Mit FIDO2 stünden aber bereits Techniken zur Verfügung, die den täglichen Umgang deutlich vereinfachten und gleichzeitig eine noch höhere Sicherheit gewährleisten könnten (siehe Kasten). FIDO2 ersetzt Passwörter bei der Anmeldung an Onlinediensten. Das Akronym steht für «Fast IDentity Online». Der Initialaufwand sei jedoch nicht zu unterschätzen, so Rolf Lanz.
Wo zieht man also die Grenze, um mit vernünftigem Aufwand und trotzdem sicher arbeiten zu können? Die allgemeine Empfehlung von Rolf Lanz lautet: Die IT-Sicherheit sollte so hoch sein, dass sie noch bezahlbar bleibt und dass das Restrisiko im Fall, dass ein Angriff geschieht, noch getragen werden kann.

Häufige Fehler
Das Öffnen von E-Mail-Anhängen unbekannter Herkunft sei einer der häufigsten Fehler, den Nutzerinnen und Nutzer im Zusammenhang mit IT-Sicherheit machen würden, weiss Rolf Lanz: Aber auch das Anklicken von Links in Spam-Mails, das Besuchen von zweifelhaften oder nicht für die Arbeitstätigkeit benötigten Websites oder das Ignorieren von aktuellen Updates und Softwareversionen der installierten Applikationen stehen seiner Erfahrung nach oft am Anfang einer Cyberattacke. Und weiter: «Geschäftliches und privates Arbeiten sollten unbedingt getrennt auf separaten und voneinander getrennten Accounts und Systemen verrichtet werden. Das heisst, die Geschäfts-PC mit den entsprechenden Accounts sind nicht dieselben wie die privaten Notebooks und Accounts.»
Verschärft wird das Problem, weil durch KI-Instrumente Spam-E-Mails immer glaubwürdiger dargestellt werden. Auch hier helfen laut Rolf Lanz einige simple persönliche Massnahmen: Spam-Mails sollten nicht geöffnet, sondern direkt gelöscht werden. E-Mail-Adressen von unbekannten Absendern soll man genau prüfen – nicht nur den angezeigten Namen des Senders, sondern die effektiv genutzte Absenderadresse (siehe Kasten). Das Unternehmen soll zudem alle E-Mails vor der Zustellung durch eine lokale Anti-Malware-Software (Virenscanner) prüfen lassen. Zusätzlich können E-Mails auch durch den Internet-Service-Provider geprüft werden. Diese Leistung ist aber kostenpflichtig.

Angriffe auf KMU können lukrativ sein
KMU, auch kleine Handwerks- und Dienstleistungsbetriebe, können laut Rolf Lanz lukrative Angriffsziele für Hacker sein. «Die Firmen verfügen teilweise über eine wenig professionell geführte IT-Infrastruktur und weisen daher oft bekannte Schwachstellen auf. Diese sind den Angreifern bekannt und lassen sich leicht für einen Angriff nutzen. Je dringender ein Betrieb auf eine funktionierende IT-Infrastruktur angewiesen ist, umso interessanter ist er für einen Erpressungsversuch, z. B. zum Zahlen eines Lösegeldes für die Freigabe der zuvor vom Angreifer verschlüsselten Daten durch Ransomware.»
Die in den Zahnarztpraxen gespeicherten Patientendaten seien für einen Angreifer ein speziell lohnendes Ziel, so der Experte. «Es handelt sich hierbei um besonders schützenswerte Gesundheitsdaten, die nicht in fremde Hände kommen dürfen. Sie eignen sich somit bestens für eine Erpressung. Der Hacker droht dazu mit der Veröffentlichung der gestohlenen Daten.»

Massnahmen zur Erhöhung der IT-Sicherheit
Als wesentliche Anforderungen an die Nutzer zur Erhöhung der IT-Sicherheit nennt Rolf Lanz folgende Massnahmen:
- lokales Netzwerk nur über eine korrekt konfigurierte Firewall mit dem Internet verbinden
- zeitgerechte Installation aller zur Verfügung stehenden Updates
- Nutzen von aktuellen Software-Versionen
- Tägliche Erstellung von Back-ups nach der 3-2-1-Regel (siehe Kasten)
- ausschliesslich persönliche Accounts verwenden
- keine allgemeinen Accounts, die von mehreren Personen genutzt werden
- Für die tägliche Arbeit keine Accounts mit Root- oder Admin-Rechten nutzen
- Die aktuelle IT-Sicherheit regelmässig (ca. jährlich) durch eine vertrauenswürdige Fachperson prüfen lassen und gegebenenfalls nachbessern.

Nützliche Links

Tipps vom NCSC für Unternehmen:
www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen.html

3-2-1-Regel für Backups:
www.synology.com/de-de/dsm/solution/data_backup

Informationen über die effektiv genutzte E-Mail-Absender-Adresse:
www.spamhaus.com/de/resource-center/source-code-bosartiger-e-mails/

Informationen über FIDO2:
www.forgerock.com/de/resources/whitepaper/go-passwordless-authenticate-securely