Die Sicherheit von Patientendaten hat Priorität

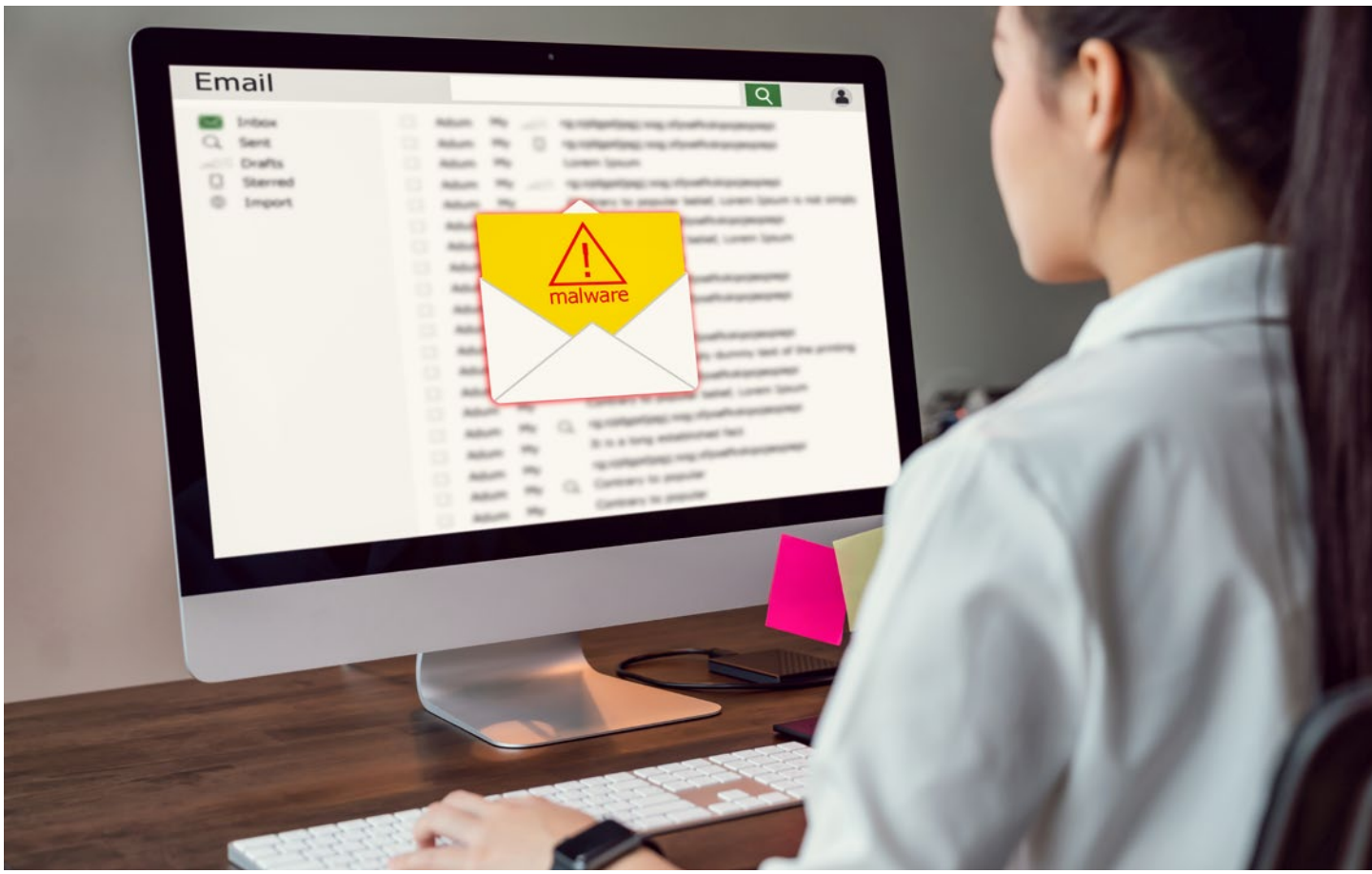
Auch kleine Unternehmen wie Zahnarztpraxen können **Opfer eines Hackerangriffs** werden. IT-Sicherheitsexperte Uwe Gempp erklärt im Interview, wie Praxisinhaber die Sicherheit der Patientendaten verbessern können.

Interview: Andrea Renggli, Redaktion SDJ; Foto: Istock

Uwe Gempp, im Frühling wurden im Kanton Neuenburg in mehreren Arztpraxen Computer gehackt und Patientendaten gestohlen. Die Angreifer drohten, die Daten zu veröffentlichen, und erpressten die Praxisinhaber. Wie kann es sein, dass eine kleine Einzelpraxis ins Visier von Hackern gerät?
Auch kleine Firmen sind häufig von solchen Angriffen betroffen. Die Hacker suchen nicht zielgerichtet, sondern automatisiert und rund um die Uhr nach Schwachstellen. Hat der Angreifer einmal Zugang zum System, prüft er, welche Opfer einen grossen Gewinn versprechen. Bei einem Zahnarzt oder Arzt vermutet man eine hohe Zahlungsbereitschaft: einerseits, weil er ein vergleichsweise hohes Einkommen hat, und andererseits, weil die Veröffentlichung von Patientendaten dem Ruf der Praxis schadet.

Offenbar haben die betroffenen Praxen alle die gleiche Software für elektronische Patientenakten verwendet. Wie kann ich mich informieren, ob eine Software sicher ist?
Als Laie ist das schwierig zu beurteilen. Sie können aber den Hersteller ihrer Praxissoftware fragen, welche Sicherheitsmassnahmen er regelmässig durchführt, um Schwachstellen zu erkennen und zu beheben. Es gibt entsprechende Zertifizierungen, die bekannteste ist die Normreihe ISO/IEC-27000. Fragen Sie nach einem entsprechenden Nachweis.

Wie soll man nach einem Angriff reagieren?
Das kommt auf den konkreten Fall an. Sobald man feststellt, dass der Computer



Je mehr Daten digital abgelegt werden, umso grösser ist die Gefahr, dass Hacker sie zu Geld machen wollen.

Zur Person

Uwe Gempp ist seit Anfang 2022 Security Officer bei der Health Info Net AG (HIN). Das Unternehmen schützt Patientendaten in der digitalen Welt und ist für Gesundheitsfachpersonen in der Schweiz der Standard für sichere Kommunikation und den vertrauensvollen Umgang mit sensiblen Daten. Uwe Gempp ist als CSO und IT-Architekt zuständig für die Informationssicherheit bei HIN. Er kann auf langjährige Berufserfahrung in der IT zurückgreifen.

gehackt wurde, muss das System abgeschaltet und vom Netz getrennt werden. So fliessen nicht noch mehr Daten ab. Der Praxisinhaber soll den Vorfall auf jeden Fall beim Nationalen Zentrum für Cybersicherheit (NCSC) melden (www.ncsc.admin.ch). Dort erhalten Betroffene Informationen und Unterstützung.

Wie soll man auf Geldforderungen reagieren?
Wir empfehlen, der Erpressung nicht nachzugeben, sondern Anzeige bei der Polizei zu erstatten. Einerseits unterstützt man mit der Zahlung die Hacker, da jede Zahlung die Attraktivität der Angriffe für Hacker erhöht und Mittel für weitere Attacken bereitstellt. Andererseits ist eine Lösegeldzahlung keine Garantie dafür, dass Daten wiederhergestellt bzw. vom Hacker nicht veröffentlicht werden. Die Angriffe werden oft kombiniert, Hacker dringen ins System ein und verschlüsseln die Dateien auf dem Computer, nachdem sie versendet wurden. Gegen ein Lösegeld versprechen sie, dem Opfer den Schlüssel zu geben, um die Daten zu entschlüsseln. Falls das Opfer darauf nicht eingeht, folgt eine weitere Forderung, damit die gestohlenen Daten nicht veröffentlicht werden. Auch wenn man auf diese Forderung eingeht, hat man keine Gewissheit darüber, was mit den Daten geschieht.

Welche Massnahmen kann ich selbst treffen, um gar nicht erst erpresst zu werden?
Das Wichtigste ist der IT-Grundschutz (siehe Kasten). Dazu gehören organisatorische und technische Massnahmen, aber auch ganz grundlegende Fragen: Ist die Software auf aktuellem Stand? Werden regelmässig Security-Updates gemacht? Ist der Virenscanner aktuell? Sind meine Passwörter sicher genug? Werden regelmässige Back-ups durchgeführt?

Und wie schütze ich mich vor Verschlüsselungstrojanern, die die Dateien auf dem Computer verschlüsseln?
Der beste Schutz ist ein regelmässiges Back-up. Dabei speichert man eine Sicherheitskopie auf einem externen Gerät. Es ist auch ratsam, ein Stand-by-Gerät einzurichten; zum Beispiel einen Laptop, der nicht am Praxisnetz angeschlossen ist. So kann der Praxisbetrieb nach einer Attacke auf den Hauptcomputer weitergeführt werden, falls dieser abgeschaltet werden muss. Schliesslich ist es empfehlenswert, Kontakt zu einem IT-Dienstleister zu haben, den man im Fall eines Angriffs anrufen kann. Damit erspart man sich zusätzlichen Stress und erhält schneller Unterstützung.

In der Praxis stehen nebst dem Computer auch andere vernetzte Geräte. Ist ein Angriff auf das IT-System über solche mit dem Internet verbundene Geräte möglich?
Ja, das ist möglich. Medizinische Geräte von renommierten Herstellern sind weniger gefährdet, da die Sicherheit ihrer Geräte für die Hersteller hohe Priorität hat. Problematisch sind aber günstige Geräte aus dem Handel, über die man beispielsweise in der Praxis Musik abspielt oder Kameras zur Überwachung in der Nacht betreibt. Diese Geräte sollten nicht ans Praxisnetzwerk angeschlossen werden, weil die Hersteller der Sicherheit häufig keine ausreichende Priorität einräumen und bekannte Schwachstellen nicht schliessen. Die Geräte können über ein separates Netzwerk angeschlossen werden, was bei den meisten Internetroutern auch unterstützt wird. Informationen dazu gibt das NCSC: www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-iot.html.

Kann man den IT-Schutz in der Zahnarztpraxis selbst umsetzen, oder braucht es zwingend eine Fachperson dazu?
Den IT-Grundschutz können die meisten Praxisinhaber selbst umsetzen, dazu muss man kein Informatiker sein. Es genügt, mit dem Betriebssystem vertraut zu sein und vorhandene Checklisten zu nutzen (z.B. IT-Grundschutz der SSO, siehe Kasten, oder www.hin.ch/blog/schutz-cyberattacken). Viele Zahnärztinnen und Zahnärzte haben jedoch wenig Zeit, sich mit IT-Fragen zu befassen, und schreiben dem Thema weniger Priorität zu als ihrer Kernkompetenz, der optimalen Behandlung der Patienten. Ich finde es jedoch wichtig, dass man sich bewusst ist: Der Computer ist ein wichtiges Arbeitsgerät in jeder Praxis, er gehört ebenso zur Ausrüstung wie der Behandlungsstuhl. Deshalb sollte jeder Praxisinhaber darauf achten, auch beim Computer auf Qualität und Sicherheit zu achten.

Die Digitalisierung im Schweizer Gesundheitswesen wird weiter zunehmen. Welche Gefahren birgt diese Entwicklung?
Je mehr Daten digital abgelegt werden, umso grösser ist die Gefahr, dass Hacker sie zu Geld machen wollen. Das Risiko eines Angriffs wird deshalb definitiv zunehmen. Die Digitalisierung bietet den grossen Nutzen einer besseren Vernetzung und damit einer effizienteren Gesundheitsversorgung. Dieser Entwicklung können wir uns nicht entziehen. Vielmehr müssen wir lernen, mit dem Gefahrenpotenzial umzugehen, indem wir der Datensicherheit eine grosse Bedeutung einräumen und für die Herausforderungen sensibilisiert sind.

IT-Grundschutz der SSO

Im Rahmen einer Kooperation mit der FMH bietet die SSO ihren Mitgliedern eine Broschüre mit Empfehlungen zum IT-Grundschutz an. Die Publikation unterstützt SSO-Praxisinhaberinnen und -inhaber beim Aufbau und Erhalt des Datenschutzes und der Datensicherheit im Betrieb. Die Broschüre und ein Poster zum IT-Grundschutz sind erhältlich im Mitgliederbereich (Cockpit) der Website der SSO (unter «SSO Dokumente» > «Zahnarztpraxis»).