IT-Grundschutz in der Arztpraxis nicht vernachlässigen

Reinhold Sojer

Dr. rer. biol. hum., Leiter Digitalisierung/eHealth, FMH

Im Schweizer Gesundheitswesen werden jährlich schätzungsweise 1,5 Millionen Gigabyte Daten verarbeitet. Zusätzlich entstehen in der Schweiz jedes Jahr etwas mehr als 300 Millionen Seiten Papier mit medizinischen Daten von Patientinnen und Patienten. 76 000 Gigabyte der Daten fallen allein in Hausarztpraxen an, welche die Krankengeschichten der Patientinnen und Patienten zunehmend elektronisch verwalten [1]. So wie physische Datenablagen vor unbefugtem Zugriff geschützt werden müssen, sind auch digitale Daten zu schützen, insbesondere vor dem Hintergrund zunehmender Vernetzung. Cyberangriffe auf Gesundheitsdaten oder auf die Infrastruktur einer Arztpraxis können das Tagesgeschäft einer Arztpraxis stark einschränken, einen finanziellen oder Reputationsschaden nach sich ziehen oder die Patientensicherheit gefährden. Der Gesetzgeber hat die in einer Praxis anfallenden Daten als besonders schützenswert eingestuft, die mit angemessenen technischen und organisatorischen Massnahmen zu schützen sind. Diese Massnahmen sollen das Risiko minimieren, dass Angreifer Schwachstellen ausnutzen, welche die Vertraulichkeit, die Verfügbarkeit oder die Integrität von Patientendaten gefährden. Das Schutzziel der Vertraulichkeit wird gefährdet, wenn zum Beispiel Patientendaten unverschlüsselt übertragen werden, wohingegen Systemausfälle die Verfügbarkeit von Daten bedrohen. Ein Angriff auf das Schutzziel der Verfügbarkeit muss dabei nicht zwangsläufig durch einen gezielten Angriff erfolgen, wie zum Beispiel durch den Verschlüsselungstrojaner Wanacry im Mai 2017, der mehr als 230 000 Computer in 150 Ländern infizierte. Anfang 2018 hat ein «simpler» Softwarefehler bei der Swisscom dazu geführt, dass über 5000 Arztpraxen mehrere Stunden lang telefonisch nicht erreichbar waren [2].

Um kritische Infrastrukturen wie Energie- und Wasserversorger oder Spitäler vor Cyberrisiken zu schützen, hat der Bund 2018 erstmals Minimalstandards erlassen. Für kleine und mittlere Unternehmen, insbesondere für Arztpraxen, existieren in der Schweiz bislang hingegen keine entsprechenden Standards. In einer Arztpraxis trägt die Ärztin oder der Arzt die gesamte Verantwortung, sowohl für die Sicherheit als auch für den Schutz der Daten wie auch für den Betrieb der ICT-Infrastruktur. Angesichts der in einer Arztpraxis zur Verfügung stehenden Ressourcen stellt diese Aufgabe eine Herausforderung für die Praxisinhaberinnen und Praxisinhaber dar.

Die FMH hat für ihre Mitglieder daher Minimalanforderungen zum IT-Grundschutz in der Arztpraxis erarbeitet, die helfen sollen, ein angemessenes Sicherheitsniveau zu erzielen und die Anforderungen des Datenschutzgesetzes zu erfüllen. Die Empfehlungen umfassen unter anderem Massnahmen zum Schutz vor Zugriff, zur Verwaltung von Benutzerrechten, zum Schutz des Netzwerkes oder zur Sensibilisierung der Mitarbeitenden. Die Umsetzung und Einhaltung der Massnahmen kann zwar keinen hundertprozentigen Schutz vor erfolgreichen Cyberangriffen bieten. Falls trotz allen Schutzmassnahmen ein Sicherheitsvorfall eintritt, kann dieser aber besser bewältigt werden, wenn die Praxisinhaberin und die Mitarbeitenden darauf vorbereitet sind.

Bildnachweis
Hahn + Zimmermann

Literatur

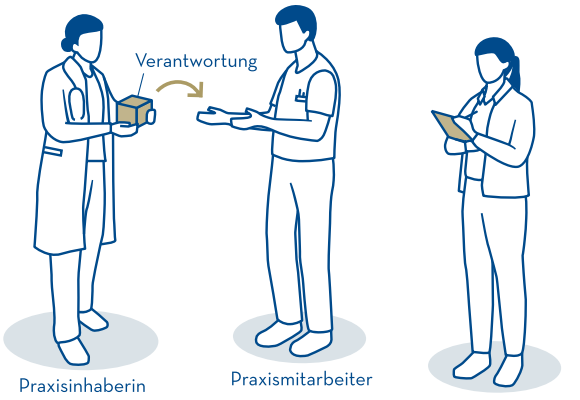
1 Swisscom Health, «Schweizer Gesundheitsdaten heute und morgen», 2017.
2 Die FMH hat in diesem Zusammenhang Empfehlungen erarbeitet, die unter https://www.fmh.ch/themen/ehealth/praxisinformatik.cfm#i134809 abgerufen werden können.

Die vollständigen Empfehlungen sind unter https://www.fmh.ch/praxisinformatik abrufbar.

Dr. Reinhold Sojer
Leiter Abteilung Digitalisierung/eHealth FMH
Elfenstrasse 18
Postfach 300
CH-3000 Bern 15
Tel. 031 359 12 04
reinhold.sojer[at]fmh.ch

Minimalanforderungen IT-Grundschutz für Praxisärztinnen und Praxisärzte

11 Empfehlungen

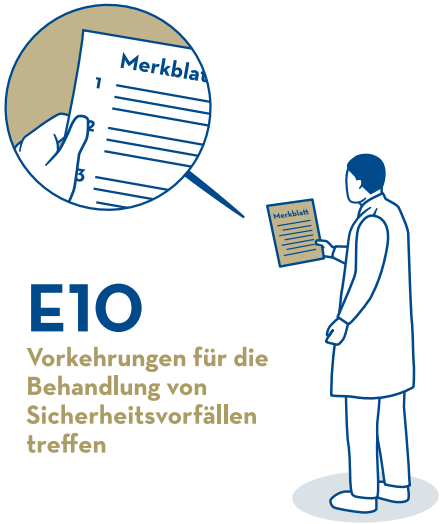


E1
Verantwortlichkeiten bestimmen und Vorgaben erlassen

E2
ICT-Mittel in ein Inventar aufnehmen

E3
Zugriffsschutz regulieren und Benutzerrechte verwalten

E11
Externe Dienstleister beauftragen und überwachen



E10
Vorkehrungen für die Behandlung von Sicherheitsvorfällen treffen