Cybercrime – So wird die Praxis zur Trutzburg

Team muss an einem Strang ziehen

Es muss nicht immer die Phishingmail sein, über die sich Cyberkriminelle Zugang zur Praxis-IT verschaffen. Es lauern noch mehr Fallen. Um die Praxis zur Cyber-Trutzburg zu machen, geben IT-Experten Handlungsempfehlungen zur Umsetzung der IT-Sicherheitsrichtlinie. Der Fokus liegt dabei auf der Situation in der individuellen Praxis.

Zahnarztpraxen sind im deutschen Gesundheitswesen die Vorreiter in puncto Digitalisierung. Das digitale Herz der Praxis ist das Praxisverwaltungssystem (PVS), in dem die Patientenakten samt Dokumentation geführt werden. Über Schnittstellen werden Daten mit anderen Systemen ausgetauscht, aber auch eigenständige KI-Lösungen übertragen Daten in das PVS. Wie Experten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erläutern, mache gerade die Verarbeitung dieser sensiblen Daten die Praxen zu attraktiven Zielen für Cyberkriminelle. Hinzu komme, dass in den Praxen in der Regel mehrere Personen auf vernetzte Geräte zugreifen können. Das vergrößere die Angriffsfläche zusätzlich.

„Kommt es zum Datenverlust oder werden Daten durch Ransomware verschlüsselt, hat das unmittelbare Folgen für den Praxisbetrieb. Behandlungen verzögern sich und das Vertrauen der Patientinnen und Patienten kann leiden. Hinzu kommen ein erheblicher organisatorischer Aufwand, unter Umständen lange Ausfallzeiten und möglicherweise finanzielle Schäden", heißt es in dem aktuellen Selbst-Check, den das BSI Praxisteams an die Hand gibt, um die Anforderungen der aktuellen IT-Sicherheitsrichtlinie nach § 390 SGB V besser einzuordnen und IT-Sicherheit im Praxisalltag schrittweise zu etablieren.

Zentraler Bestandteil des sechsseitigen Serviceheftes ist ein Fragenkatalog, der über mehrere Themenbereiche abklopft, wie gut die Praxis bereits aufgestellt ist und wo noch Handlungsbedarf besteht. Das beginnt mit dem Komplex der Mitarbeiter und Zuständigen. Hier wird zum Beispiel gefragt, ob jedes Teammitglied eigene Zugangsdaten hat. Zu jeder Frage gibt es erste Tipps. In diesem Fall lautet die Handlungsempfehlung: „Vergeben Sie ein eigenes Benutzerkonto für jede Person. Damit lassen sich Zugriffe besser steuern und nachvollziehen." Ein weiterer Punkt adressiert Regeln für Fremdpersonal in den Praxen. Der Tipp: „Lassen Sie Dienstleister nur dort arbeiten, wo es nötig ist. Legen Sie fest, wer sie begleitet, und nutzen Sie kurze Standardvereinbarungen zur Vertraulichkeit."

Die sichere Kommunikation wird unter dem Aspekt beleuchtet, wie Praxisleitung und Team mit Schulungen zur IT-Sicherheit umgehen. In puncto Aktualität der IT-Systeme geht es zum Beispiel um die Frage, wie mit Updates verfahren wird, aber auch darum, ob veraltete Hard- und Software ohne Sicherheitsupdate in Betrieb ist. „Verschaffen Sie sich einen Überblick über alle eingesetzten Systeme. Prüfen Sie regelmäßig, ob diese noch vom Hersteller unterstützt werden. Veraltete Systeme sollten ersetzt oder sauber abgeschottet werden", raten die BSI-Profis.

Breiten Raum nehmen auch die Datensicherung und der Schutz von Geräten ein. Werden in der Praxis regelmäßig Back-ups vorgenommen und wer ist dafür zuständig? Werden die Back-ups auch regelmäßig getestet? „Testen Sie die Wiederherstellung regelmäßig, wenn möglich auf einem Testsystem. Ein Back-up schützt nur dann, wenn es sich im Ernstfall auch zurückspielen lässt", rufen die Experten in Erinnerung. Außerdem müssen Praxisteams Datensicherungen vor unbefugtem Zugriff schützen. Back-ups sollten physisch gesichert und möglichst verschlüsselt werden. Auch Zugriffe auf Geräte und Software sollten abgesichert sein, verlassene PC-Arbeitsplätze gesperrt werden.

Zunehmend sind auch Cloud-Dienstleister im Gesundheitswesen unterwegs und werben zum Beispiel bei Zahnarztpraxen für die Datenauslagerung in ihren virtuellen Speicher. Das ist nicht ohne Risiko für die Praxis. Denn: Werden Sozial- oder Gesundheitsdaten in der Cloud verarbeitet, muss der Anbieter laut BSI über ein aktuelles C5-Testat verfügen. Der Tipp der Experten: „Beugen Sie für den möglichen Ausfall des Systems vor und prüfen Sie im Zweifel Zertifizierung, Speicherort, Gerichtsbarkeit und Erreichbarkeit des Anbieters."

Zur Erinnerung: Die IT-Sicherheitsrichtlinie, die KBV, KZBV und BSI zusammen erarbeitet haben, setzt neben einer strukturierten Einarbeitung neuer Teammitglieder vor allem auf die Einhaltung der technischen Basissicherheit, die durch Updates, Datensicherung, Zugriffsschutz, E-Mail-Sicherheit und die Prüfung von Cloud-Diensten gewährleistet wird.

Matthias Wallenfels