Schwachstellen erkennen – Angriffe abwehren

IT-Sicherheitsrichtlinie gibt Orientierungshilfe

IT-Sicherheit umfasst alle technischen und organisatorischen Maßnahmen zum Schutz digitaler Informationen vor Ausspähung, Manipulation und Verlust. Ein einziger falscher Klick kann ausreichen, um den Praxisbetrieb lahmzulegen: Termine sind nicht abrufbar, Patientendaten unzugänglich, Abläufe gestört. Was lange als theoretisches Risiko galt, gehört inzwischen zum Alltag vieler medizinischer Einrichtungen. Die im Januar 2026 eingeführte verbindliche IT-Sicherheitsrichtlinie gibt hier Orientierungshilfe.

Mit der fortschreitenden Digitalisierung wachsen die Chancen für eine bessere Versorgung ebenso wie die Risiken durch Cyberangriffe. Entsprechend müssen Sicherheitsmaßnahmen kontinuierlich angepasst, Schwachstellen frühzeitig erkannt und Angriffe effektiv abgewehrt werden. Die neue IT-Sicherheitsrichtlinie für Zahnarztpraxen verfolgt das Ziel, sensible Gesundheitsdaten zu schützen und gleichzeitig die Funktionsfähigkeit der Praxis sicherzustellen. IT-Sicherheit ist damit keine optionale Ergänzung, sondern eine zentrale Voraussetzung für verlässliche digitale Prozesse und einen stabilen Praxisbetrieb.

Gesetzliche Grundlage

Die IT-Sicherheitsrichtlinie für Arzt- und Zahnarztpraxen basiert auf dem gesetzlichen Auftrag gemäß § 390 SGB V und wurde im Rahmen des Digital-Gesetzes konkretisiert. KBV und KZBV sind verpflichtet, verbindliche Anforderungen zur IT-Sicherheit festzulegen, abgestimmt mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Die Richtlinie konkretisiert bestehende Pflichten aus Datenschutz-Grundverordnung (DSGVO) und Bundesdatenschutzgesetz (BDSG) und wird regelmäßig an den Stand der Technik sowie an die aktuelle Gefährdungslage angepasst. Die aktuelle Fassung gilt seit Juli 2025, neue Anforderungen sind seit Januar 2026 umzusetzen.

Die IT-Sicherheitsrichtlinie passt bestehende Vorgaben an aktuelle Bedrohungen und gesetzliche Anforderungen an. Dabei konkretisiert sie insbesondere die Praxisorganisation, den sicheren Umgang mit IT-Systemen sowie die Einbindung externer Dienstleister. Viele Maßnahmen sind nicht neu, werden jedoch verbindlicher geregelt, etwa in den Bereichen Dokumentation, Aktualisierung von Software und Datensicherung. Ziel ist es, den Schutz sensibler Gesundheitsdaten zu stärken und das Bewusstsein für IT-Sicherheit zu schärfen. Die Kassenzahnärztliche Bundesvereinigung schreibt dazu: „Für die Zahnärzteschaft bedeutet das mehrheitlich: business as usual. Die Richtlinie regelt nämlich weitestgehend das, was den Praxen auf Grundlage bisheriger Bestimmungen in der DSGVO und dem BDSG ohnehin bereits vorgeschrieben wird."

Die IT-Richtlinie differenziert die Anforderungen nach Größe, Ausstattung und Digitalisierungsgrad der Praxis. Maßgeblich ist die Anzahl der Personen, die ständig mit der Datenverarbeitung betraut sind, sowie die Komplexität der eingesetzten IT-Systeme. Dabei gilt: je höher das Risikopotenzial, desto umfangreicher die verpflichtenden Sicherheitsmaßnahmen. Entscheidend ist daher eine realistische Einordnung der eigenen Praxis, um die jeweils geltenden Anforderungen korrekt umzusetzen. Verantwortlich für die Datensicherheit der Praxis-IT ist der Inhaber, das gilt auch für den Internetanschluss.

Was ist neu?

Der Faktor Mensch

Ein Großteil erfolgreicher Cyberangriffe beginnt nicht mit Technik, sondern durch einen vom Menschen verursachten Fehler.

Eine unbedachte E-Mail, ein schwaches Passwort oder ein offener Bildschirm können schon ausreichen. Die Richtlinie setzt deshalb stark auf Schulung und Sensibilisierung. Neue Mitarbeitende müssen strukturiert eingearbeitet werden, inklusive klarer Vorgaben zum Umgang mit IT-Systemen und Patientendaten. Bestehendes Personal ist regelmäßig zu schulen – mindestens einmal jährlich.

Auch beim Ausscheiden von Mitarbeitern gelten klare Regeln: Zugänge müssen deaktiviert, Passwörter geändert und ausgegebene Geräte zurückgegeben werden. So werden unnötige Sicherheitslücken vermieden. Externe Dienstleister, Reinigungspersonal oder IT-Techniker sind Teil des Praxisalltages – und zugleich ein potenzielles Risiko. Die Richtlinie sieht deshalb verbindliche Vertraulichkeitsvereinbarungen sowie eine strikte Begrenzung von Zugriffsrechten vor. Fremdpersonal darf nur auf die Systeme zugreifen, die für die jeweilige Aufgabe zwingend notwendig sind.

Aktualität ist das A und O

Ein weiterer zentraler Baustein ist das konsequente Patch- und Änderungsmanagement. Systeme müssen regelmäßig aktualisiert werden. Veraltete Software oder Hardware, die keine Updates mehr erhält, darf nicht weiter betrieben werden – es sei denn, sie wird isoliert in einem separaten Netzwerk eingesetzt. Gerade in Zahnarztpraxen betrifft das häufig ältere medizinische Geräte, die weiterhin genutzt werden, aber besondere Schutzmaßnahmen erfordern. Ergänzend gilt seit Oktober 2025 die Pflicht, verfügbare Updates generell zeitnah zu installieren, um Sicherheitslücken schnell zu schließen.

Bereits seit 2021 und weitestgehend etabliert gelten für alle Zahnarztpraxen verbindliche IT-Sicherheitsanforderungen, die Schutzmaßnahmen für den Praxisalltag festlegen. Dazu gehört insbesondere der sichere Umgang mit Anwendungen: Apps sollen ausschließlich aus offiziellen Quellen bezogen, nicht mehr benötigte Anwendungen vollständig entfernt und Zugriffsrechte auf sensible Daten möglichst eingeschränkt werden. Vertrauliche Daten müssen durch verschlüsselte Verbindungen geschützt sein, etwa bei der Nutzung von Webanwendungen.

„Ständig mit der Datenverarbeitung betraut" bezeichnet im datenschutzrechtlichen Sinne alle Personen, die regelmäßig – unabhängig von Umfang oder Dauer – mit der Verarbeitung von Daten beschäftigt sind. Dazu zählen in der Regel sämtliche Mitglieder des Praxisteams sowie die Praxisinhaber, sofern sie mit dem Praxisverwaltungssystem, der Abrechnung oder anderen datenbezogenen Aufgaben arbeiten. Nicht einbezogen sind hingegen Personen ohne Zugang zu entsprechenden Systemen, etwa Reinigungskräfte. Unter Datenverarbeitung fällt das Erheben, Speichern, Bearbeiten, Weiterleiten oder Löschen von Daten – beginnend bereits bei der Terminvergabe oder dem Einlesen der elektronischen Gesundheitskarte.

Auch organisatorische Maßnahmen sind verpflichtend: Geräte sind nach der Nutzung zu sperren oder abzumelden, mobile Endgeräte durch sichere Zugangscodes zu schützen und Kamera sowie Mikrofon nur bei Bedarf zu aktivieren. Zudem sind ein aktueller Virenschutz einzusetzen und Wechseldatenträger regelmäßig auf Schadsoftware zu prüfen. Für die Praxis-IT ist eine strukturierte Dokumentation des Netzwerkes erforderlich.

Ein weiterer Schwerpunkt liegt auf der Datensicherung: Daten müssen regelmäßig nach einem festgelegten Plan gesichert werden. Bei Verlust mobiler Geräte sind umgehend Sperrmaßnahmen einzuleiten. Für Komponenten der Telematik-Infrastruktur (TI) gilt zudem, dass Updates zeitnah installiert und Administrationsdaten sicher, aber für den Praxisinhaber zugänglich aufbewahrt werden müssen.

Bietet die Praxis eigene Webdienste an, sind zusätzliche Schutzmaßnahmen wie der Einsatz einer Web Application Firewall sowie Mechanismen gegen unbefugte automatisierte Zugriffe erforderlich.

Und was, wenn es doch passiert?

Notfallplan für den Ernstfall

Ein Cyberangriff kann jederzeit erfolgen. Entscheidend ist dann, schnell und strukturiert zu reagieren. Die Richtlinie verlangt deshalb einen klar definierten Notfallplan.

Dieser sollte festlegen, wer im Ernstfall welche Aufgaben übernimmt, wie Systeme gesichert werden und wie der Betrieb wiederhergestellt werden kann. Vorbereitung reduziert Ausfallzeiten – und kann im Ernstfall existenzsichernd sein. Beispielsweise stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine IT-Notfallkarte „Verhalten bei IT-Notfällen" bereit.

Die Richtlinie macht deutlich, dass IT-Sicherheit kein einmaliges Projekt ist. Sie erfordert kontinuierliche Aufmerksamkeit, regelmäßige Anpassungen und die aktive Mitwirkung des gesamten Teams. Für Zahnarztpraxen bedeutet das: Strukturen prüfen, Maßnahmen umsetzen und das Thema dauerhaft im Blick behalten. Denn am Ende geht es nicht nur um Technik, sondern um Vertrauen, Verlässlichkeit und die Zukunft der eigenen Praxis.

Eileen Andrä
Leitung Telematik-Infrastruktur (TI)

Ausführliche Informationen zur IT-Sicherheitsrichtlinie: https://www.kzvb.de/digitalisierung-ti/sicherheit-datenschutz.

Die Richtlinie nach § 390 SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit finden Sie hier: https://www.kzbv.de/zahnaerzte/digitales/it-sicherheit/.