Qualitätsring Medizinische Software

Stellungnahme des QMS e.V. vom 12.12.2024

im Rahmen einer Benehmensherstellung zum KBV-Entwurf einer Richtlinie nach § 390 SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit

1. Grundsätzlich sieht der QMS e.V. die vorliegende Fassung der Richtlinie nach §390 SGB V als gelungenen nächsten Schritt auf dem Weg zu mehr IT-Sicherheit in KV-Praxen an. Gleichwohl wollen wir mit den nachfolgenden Punkten zur Verbesserung der Richtlinie beitragen.

2. Wesentliche Bedrohungen für die Sicherheit von KV-Mitgliedspraxen aus Sicht des Betriebs der Informationstechnik entstehen durch den physischen Zugang zu den IT-Systemen oder zu den Datensicherungen und mehr noch durch den Anschluss der IT-Systeme an Kommunikationsnetze. Die Bedrohungen bestehen in der Kompromittierung von Patientendaten oder Betriebsgeheimnissen oder in Betriebsstörungen oder -unterbrechungen, die durch eine fehlende Verfügbarkeit von Daten oder Systemen entstehen und die auch längere Zeit andauern können. KV-Mitglieder sind für die Sicherheit ihrer Betriebsstätte selbst verantwortlich. Da sie in der Regel nicht allein einen ordnungsmäßigen IT-Betrieb sicherstellen können, bedienen sie sich grundsätzlich externer Dienstleister, die im Rahmen eines entsprechenden Vertrags die IT-Sicherheit garantieren sollen. Wegen individuell differierender Notwendigkeiten für IT-Sicherheitsmaßnahmen bei den einzelnen Praxen macht es wenig Sinn, wenn in der Richtlinie versucht wird, Details zu regeln; es ist zielführender, sich auf die Expertise der beauftragten Unternehmen zu verlassen.

3. Die Richtlinie der KBV kann Ärztinnen und Ärzten sowie Psychotherapeutinnen und Psychotherapeuten dabei helfen, geeignete Verträge mit IT-Dienstleistern abzuschließen. Darüber hinaus können Awareness-Maßnahmen und Schulungen das Bewusstsein der Praxisverantwortlichen verbessern und außerdem aufzeigen, was in Verträgen mit Dienstleistern geregelt werden sollte. Für kleine und mittlere Praxen wäre es auch hilfreich, wenn mögliche Inhalte solcher Verträge konkret, etwa in Muster-Verträgen, beschrieben würden.

4. Außerdem könnten stichprobenhaft bei einzelnen Praxen durchgeführte IT-Sicherheits-Audits (neben der Abstellung gefundener Mängel) in der Form hilfreich sein, dass die Erkenntnisse daraus in allgemeine Awareness-Maßnahmen oder Schulungen einfließen könnten.

5. Folgende Details sollten in der Richtlinie geregelt werden:

    - IT-Systeme oder an IT-Systeme angebundene Geräte, für die keine Updates mehr verfügbar sind, sollten nur ohne Netzverbindung mit dem übrigen IT-Netz oder mit einer besonderen Netzabsicherung betrieben werden.

    - Sicherheitsanforderungen sollten nicht für ein bestimmtes Betriebssystem oder bestimmte Endgeräte formuliert werden, sondern in generischer Form. Das bedeutet konkret, dass die Punkte 30 bis 35 der Anlage 1, Punkte 5 bis 8 der Anlage

2 und Punkte 4 bis 12 der Anlage 3 zu einem Zielobjekt („Mobile Endgeräte“ o.ä.) zusammengefasst werden sollten.

- Die Anforderungen an die IT-Sicherheit in Arztpraxen werden sich durch den Betrieb der IT-Infrastruktur nach den Prinzipien einer TI 2.0 verändern; hierauf sollte zu gegebener Zeit bei einer Fortschreibung der Richtlinie eingegangen werden.