RECHT KOMMENTIERT

Neuer Best-Practice-Katalog für die IT-Sicherheit

Nach den Vorgaben der Datenschutz-Grundverordnung müssen die für die Datenverarbeitung Verantwortlichen technische und organisatorische Maßnahmen ergreifen, um ein angemessenes Schutzniveau der verarbeiteten personenbezogenen Daten zu gewährleisten. Das Bayerische Landesamt für Datenschutzaufsicht („BayLDA") hat am 27. Mai 2020 eine Best-Practice-Liste von Maßnahmen veröffentlicht, die Anforderungen an die IT-Sicherheit speziell bei medizinischen Einrichtungen beinhaltet (https://www.lda.bayern.de/media/best_practice_cybersicherheit_medizin_baylda.pdf). Hierdurch soll nach Auffassung des BayLDA „eine gesteigerte Sensibilisierung für sicherheitsrelevante Themen erreicht und aktiv ein störungsfreier Betrieb dieser Einrichtungen unterstützt werden". Der Katalog ist wie eine Checkliste aufgebaut und soll die medizinischen Einrichtungen, gleichgültig ob Arztpraxis oder Klinikum, in die Lage versetzen, die eigenen ergriffenen IT-Sicherheitsmaßnahmen auf den Prüfstand zu stellen.

Die Maßnahmen sind dabei weit gefächert. Sie umfassen Mittel, die etwa gegen Angriffe durch Schadsoftware und Trojaner implementiert sein können. Darunter fallen neben präventiven Instrumenten, wie z.B. einer regelmäßig aktualisierten Antiviren-Software, auch Anleitungen wie mit tatsächlichen Cyberattacken umgegangen werden soll. Dies kann durch klare Anweisungen an Beschäftigte zum Umgang mit Alarmmeldungen und einem Ablaufplan der IT-Administration bei Malware-Befall erfolgen. Die Best-Practice-Liste beinhaltet daneben auch Maßnahmen zum Passwortschutz, E-Mail-Sicherheit, Homeoffice-Arbeit sowie Fernwartung und Online-Zugriffsmöglichkeiten auf Laborergebnisse. Bei Letzteren wird beispielsweise eine Protokollierung der Zugriffe und regelmäßige Überprüfung derselben vorgeschlagen. Die Liste geht auch auf den Datenschutzbeauftragten („DSB") ein und fordert insoweit eine konsequente Einbindung des DSB bei Sicherheitsfragen. Zudem sollte eine ausreichende fachliche Qualifikation des DSB für sicherheitsrelevante Fragestellungen und Möglichkeiten zur Fortbildung für dieses Thema bestehen. Die aufgezählten Maßnahmen des Best-Practices-Katalogs sind nicht abschließend. Vielmehr kommt es auf die Situation im Einzelfall und die Datenverarbeitung der jeweiligen medizinischen Einrichtung an. Die Handreichung des BayLDA kann jedoch ein hilfreicher Anhaltspunkt für die Überprüfung der bestehenden IT-Sicherheitsmaßnahmen sein.

Johanna Clausen, Anwältin am Berliner Standort von Taylor Wessing, berät im Datenschutz, in urheber-, wettbewerbs-, IT- und fernabsatzrechtlichen Themen sowie in sonstigen technologierechtlich relevanten Fragestellungen.