Healthcare digital: Welche Regeln für die Cybersicherheit gelten

Gesundheits-Apps, elektronische Patientenakte und vernetzte Medizinprodukte: Digitale Produkte treiben die Entwicklung auch im Gesundheitssektor. IT-Sicherheit wird umso wichtiger. Doch welche Vorgaben zu beachten und welche Nachweise zu erbringen sind, ist für Anbieter und Betreiber oft nicht leicht zu überblicken. Die folgenden Ausführungen sollen bei der Orientierung helfen.

Die Digitalisierung des Gesundheitssektors entwickelt sich dynamisch: Digitale Produkte erobern den Markt. Künstliche Intelligenz hält Einzug, Innovationen in Bereichen wie Pflege, Medizin, Gentherapie oder Nanotechnologie sind weitere Treiber. Gleichzeitig ist die Markteinführung neuer Healthcareprodukte an strenge IT-Sicherheitsbestimmungen gebunden – zu Recht, da sie äußerst sensible Daten zu Gesundheit und Leben von Menschen berühren oder die Therapie beeinflussen.

Kritische Infrastrukturen: Die KRITIS-Verordnung

Besondere Anforderungen an die IT-Sicherheit gelten bereits für bestehende Einrichtungen des Gesundheitswesens, sofern sie vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als Kritische Infrastrukturen klassifiziert sind. Im Gesundheitssektor betrifft das nicht nur die stationäre medizinische Versorgung, sondern auch die Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten, verschreibungspflichtigen Arzneimitteln, Blut- und Plasmakonzentraten sowie die Laboratoriumsdiagnostik ab einer bestimmten Größe. Die jeweiligen Schwellenwerte sind in der BSI-Kritisverordnung definiert. Als Richtgröße gilt hier der Regelschwellenwert von 500 000 von der Einrichtung versorgten Personen.

Laut BSI-Gesetz (§ 8a) müssen die jeweiligen Betreiber nach Stand der Technik angemessene organisatorische und technische Vorkehrungen treffen, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer maßgeblichen informationstechnischen Systeme, Komponenten oder Prozesse zu vermeiden. Gegenüber dem Bundesamt ist die IT-Sicherheit alle zwei Jahre durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nachzuweisen. Zusätzlich kann das BSI auch selbst Sicherheitsüberprüfungen durchführen oder durchführen lassen. Bei Nichteinhaltung der gesetzlichen Vorgaben drohen empfindliche Geldstrafen.

Ausweitung der Verordnung auf alle Krankenhäuser: KRITIS „light“

Seit Januar 2022 gelten diese IT-Sicherheitsvorgaben nicht nur für stationäre medizinische Einrichtungen im Sinne der KRITIS-Verordnung, sondern für alle Krankenhäuser. Auch wenn die Nachweispflicht gegenüber dem BSI hier entfällt, müssen Betreiber im Ernstfall mit Schadensersatzforderungen und Haftungsrisiken rechnen. Daher sollten die im Sozialgesetzbuch V (§ 75) hinterlegten Anforderungen in jedem Fall umgesetzt und wie gefordert alle zwei Jahre an den aktuellen Stand der Technik angepasst werden. Orientierung bieten dabei die branchenspezifischen Sicherheitsstandards für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus.

Wann immer also in Krankenhäusern und Einrichtungen der Kritischen Infrastruktur neue Systeme oder Komponenten innerhalb der Kernfunktionen eingesetzt werden, sind diese auch unter KRITIS-Sicherheitsaspekten zu bewerten und in die Prüfprozesse einzubeziehen.

Datensicherheit: Ein Ziel – unterschiedliche Verfahren

Der Schutz der für das Gemeinwesen wichtigen Kritischen Infrastrukturen ist aber nur ein Aspekt der IT-Sicherheit im Gesundheitswesen. Da die Sicherheit der sensiblen Daten auch im Alltagsbetrieb jederzeit gegeben sein muss, sind in allen betroffenen Bereichen Cybersicherheitsanforderungen, Zulassungsvoraussetzungen und Prüfprozesse zu definieren und laufend auf dem aktuellen Stand der Technik zu halten. Die gesetzlichen Rahmenbedingungen dafür sind im Sozialgesetzbuch zusammengefasst. Als nationale Behörde für Cybersicherheitszertifizierung ist das BSI die zentrale Instanz. Allerdings – und das macht es für Antragsteller schwierig zu überblicken – gibt es nicht den einen Prüf- oder Zertifizierungsprozess für die IT-Sicherheit von Gesundheitsprodukten. Die IT-Sicherheitsprüfungen erfolgen immer in Absprache mit dem BSI oder durch das Bundesamt selbst, sind aber in die jeweiligen Zulassungsprozesse der verschiedenen Services eingegliedert. Zuständig sind jeweils unterschiedliche Institutionen: etwa die Gesellschaft für Telematik für Anwendungen in der Telematikinfrastruktur oder das Bundesinstitut für Arzneimittel und Medizinprodukte für digitale Gesundheitsanwendungen, netzwerkfähige Medizinprodukte und Pflegegeräte. Dazu im Folgenden einige Erläuterungen.

Telematikinfrastruktur: Mehrstufige Prüfprozesse

Zu den Herausforderungen im Healthcaresektor gehört die komplexe Struktur aus Betreibern, Leistungserbringern, Kostenträgern und Versicherten. Die Digitalisierung bietet die Chance, die einzelnen Akteure neu zu vernetzen, die Kommunikation und Abläufe dadurch erheblich zu beschleunigen und zu verbessern. Basis dieser neuen digitalen Vernetzung ist in Deutschland die Telematikinfrastruktur (§ 306 SGB). Dienste wie die elektronische Patientenakte oder der E-Medikationsplan setzen auf dieser

interoperablen Kommunikations- und Sicherheitsarchitektur auf. Für Aufbau und Weiterentwicklung der Telematikinfrastruktur (TI) ist die Gesellschaft für Telematik (gematik) verantwortlich, zu deren Aufgaben auch die Definition und Durchsetzung verbindlicher Standards für Dienste, Komponenten und Anwendungen gehört.

Bei der IT-Sicherheitsbewertung arbeitet die gematik eng mit dem BSI zusammen. Dazu werden alle TI-Komponenten und Dienste in einem mehrstufigen Prüfungsverfahren gemeinsam mit den Anbietern umfangreichen Tests unterzogen, bevor Sicherheitsevaluationen oder genaue Sicherheitsgutachten erstellt werden. Die einzelnen Anforderungen sind in sogenannten Produktsteckbriefen für die Zulassung der Anbieter in Anbietersteckbriefen hinterlegt.

Auch nach der Zulassung wird der sichere und störungsfreie Betrieb überwacht. Eine unberechtigte Nutzung der Telematikinfrastruktur wie auch die Nichtmeldung von Störungen oder Sicherheitsmängeln kann mit hohen Geldstrafen bis zu 300 000 € geahndet werden.

Videosprechstunde – Anbieter von Videodiensten

Während neue TI-Dienste, wie die elektronische Patientenakte (ePA), sicher noch etwas Zeit benötigen, um auch beim Versicherten anzukommen, sind mit Beginn der Pandemie die Nutzerzahlen für andere digitale Dienstleistungen förmlich explodiert: 1,4 Mio. Videosprechstunden wurden allein im ersten Halbjahr 2020 durchgeführt. Im Jahr 2019 waren es dagegen erst knapp 3 000. Voraussetzung für eine Teilnahme als Videodienstanbieter ist die Erfüllung aller Anforderungen an die technischen Verfahren. Die Anforderungen an Anbieter, Teilnehmer und Vertragsärzte wurden in einer entsprechenden Vereinbarung der Kassenärztlichen Bundesvereinigung und des Spitzenverbandes Bund der Krankenkassen festgelegt.

Unter anderem muss die Kommunikation zwischen Patient und Arzt bzw. Pflegekraft durch eine Ende-zu-Ende-Verschlüsselung gesichert sein und der Videodienst darf keine schwerwiegenden Sicherheitsrisiken aufweisen. Die nötigen Nachweise und Zertifikate zur IT-Sicherheit sind in der Vereinbarung im Einzelnen aufgeführt, Vorlagen für die Bescheinigungen und der Fragebogen mit Prüfkriterien in der Anlage hinterlegt.

Digitale Gesundheitsanwendungen: Die App auf Rezept

Deutschland bietet seit 2020 als erstes Land überhaupt digitale Apps auf Rezept. Diese digitalen Gesundheitsanwendungen (DiGA) sind definiert als Medizinprodukte niedriger Risikoklassen zur Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten oder zur Erkennung, Behandlung, Linderung oder Kompensierung von Behinderungen und Verletzungen. Die Hauptfunktion muss dabei auf digitalen Funktionen basieren (§ 33a SGB). Voraussetzung für eine Kostenübernahme durch die Krankenkassen ist die Aufnahme im Verzeichnis des Bundesinstituts für Arzneimittel und Medizinprodukte (BfArM).

Für diese Beantragungen wurde ein dreimonatiges Fast-Track-Verfahren aufgesetzt. Die entsprechenden Formulare sind zusammen mit einem Leitfaden über die Website des BfArM abrufbar. Grundsätzliche Vorgaben zur Datensicherheit sind in der Digitalen Gesundheitsanwendungen-Verordnung (§ 4) beschrieben. Dazu gehört u. a. ein Informationssicherheitsmanagementsystem auf Basis des BSI-Standards 200-2: IT-Grundschutz-Methodik. Hilfestellung bietet zudem die Technische Richtlinie des BSI zu Sicherheitsanforderungen an digitale Gesundheitsanwendungen.

Regulierungsbedarf bei vernetzten Medizinprodukten

Regulierungsbedarf besteht derzeit noch bei netzwerkfähigen Medizinprodukten. Anders als bei den rein digitalen Gesundheitsanwendungen sind Digitalfunktionen hier meist als Ergänzungen zur bestehenden medizinischen Grundfunktion integriert. Daraus ergibt sich ein äußerst breites und heterogenes Anwendungsspektrum. Zum Teil sind die IT-Sicherheitsanforderungen auch schwieriger zu adressieren, denn diese Netzwerkfunktionen werden häufig über Drittanbieter zugekauft und sind noch nicht bei allen Unternehmen auch in die Qualitätssicherungsprozesse eingebunden. Gleichwohl sind sie als Anbieter haftbar.

Grundlegende Anforderungen an Cybersicherheitseigenschaften von Medizinprodukten wurden erstmals in der EU-Verordnung 2017/745 über Medizinprodukte definiert, die in Deutschland durch das Medizinprodukterecht-Durchführungsgesetz (MPDG) umgesetzt wird. Bei der Umsetzung dieser – recht allgemein gehaltenen – Vorgaben zur IT-Sicherheit helfen Richtlinien und Verfahrensanleitungen wie:

- Guideline der Medical Device Coordination Group
- Leitfaden zur Nutzung des MDS2 (Manufacturer Disclosure Statement)
- Herstellerempfehlung zu Cybersicherheitsanforderungen an netzwerkfähige Medizinprodukte

Das BSI hat die Cybersicherheit vernetzter Medizinprodukte untersucht und in seinem Abschlussbericht dazu auch die anstehenden Aufgaben formuliert.

Die Weiterentwicklung der Regulatorik zur IT-Sicherheit bleibt eine wichtige Aufgabe. Es geht neben der IT-Sicherheit bestehender Produkte vor allem auch darum, Innovationen zum Durchbruch zu verhelfen und ihre schnelle und sichere Markteinführung zu fördern.

Anschrift des Verfassers

Randolf Skerka, SRC – Security Research & Consulting GmbH, Emil-Nolde-Str. 7, 53113 Bonn

www.daskrankenhaus.de (Online-Volltext-Version)