Mehr Cybersicherheit für Medizinprodukte

MIT ZUNEHMENDER Komplexität vieler Medizinprodukte und deren digitaler Anwendungs- und Vernetzungsmöglichkeiten steigt die Gefahr möglicher Angriffe durch Unbefugte. Mehr Cybersicherheit tut not.

Die Digitalisierung schreitet rasant voran: Software ist mittlerweile Kernbestandteil vieler Medizinprodukte. Großgeräte wie Kernspintomographen verfügen über spezifische Anwendungsprogramme, Implantate wie Herzschrittmacher können umfassend individuell programmiert werden. Patientendaten werden telemedizinisch an behandelnde Ärztinnen und Ärzte versendet, Geräte können aus der Ferne aktualisiert und konfiguriert werden. Und mit der Einführung von Apps als digitale Gesundheitsanwendungen (DiGA) vergüten die gesetzlichen Krankenkassen mittlerweile auch Medizinprodukte, die gänzlich ohne Hardware auskommen. Doch bei allem Fortschritt gilt: Jede Schnittstelle birgt prinzipiell das Risiko, als Einfallstor für Schadsoftware genutzt zu werden.

Was ist Cybersicherheit?

»Cybersicherheit« bezeichnet den Schutz von Informationssystemen mit dem Ziel, die Vertraulichkeit, Verfügbarkeit und Integrität (Fehlerfreiheit) von Daten und Prozessen sicherzustellen – ein Ziel, das für die Gesundheitsversorgung von entscheidender Bedeutung ist: Denn hochsensible Patientendaten sind vertraulich und müssen für Unbefugte unzugänglich sein. Für Leistungserbringende müssen sie bei Bedarf zuverlässig zur Verfügung stehen. Eine Verfälschung der Daten könnte für lebenswichtige Therapieentscheidungen ebenso fatale Folgen haben wie ein unbefugter Eingriff in die Funktionalität von Hochrisikoprodukten wie Herzschrittmachern.

Lange Zeit wurde die Cybersicherheit von Medizinprodukten vernachlässigt. Erst die europäische Medizinprodukteverordnung 2017/745 (MDR), die seit Mai 2021 gilt, fordert nun unter anderem bereits während der Softwareentwicklung eine Cybersicherheitsbetrachtung nach dem Stand der Technik, also dem aktuell bekannten Stand der technischen Entwicklung.

Ein einheitliches Dokument, das diesen Stand konkretisiert, fehlt derzeit jedoch, auch existieren nur wenige Vorgaben zur Umsetzung. Um den wachsenden Herausforderungen an die Cybersicherheit bei Gesundheitssoftware gerecht zu werden, wurde Ende 2021 die Norm IEC 81001-5-1 veröffentlicht. Sie formuliert konkrete Sicherheitsvorgaben – von der Entwicklung bis zur Überwachung nach dem Inverkehrbringen. Eine Harmonisierung der Norm, also ein Abgleich mit den rechtlichen Anforderungen der MDR, ist erst für 2024 geplant. Bis dahin müssen Hersteller aus einer Vielzahl von Richtlinien und Normen passende Cybersicherheitsanforderungen selbst festlegen. Dies kann dazu führen, dass das Schutzniveau von Produkt zu Produkt stark variiert.

Schwachstellen auf der Spur

Im Rahmen des Projekts *Manipulation von Medizinprodukten* (ManiMed, veröffentlicht im Jahr 2020) untersuchte das Bundesamt für Sicherheit in der Informationstechnik (BSI), die zentrale Cybersicherheitsbehörde in Deutschland, stichprobenartig verschiedene Medizinprodukte auf Sicherheitslücken in der Cybersicherheit. Hierzu zählten unter anderem vernetzte Herzschrittmacher und Kardioverter-Defibrillatoren (ICD), Insulinpumpen, Beatmungsgeräte, Infusions- und Spritzenpumpen sowie Patientenmonitore.

Bei elf Systemen namhafter Hersteller konnten insgesamt mehr als 150 Schwachstellen zur Cybersicherheit identifiziert werden. Dabei zeigte sich, dass die Hersteller unterschiedlich auf das Auffinden von Schwachstellen reagierten: Einige kommunizierten offen und bemühten sich professionell um die Behebung der Sicherheitslücken, andere akzeptierten die Schwachstellen, wenn sie nur wenig kritisch erscheinen.

Rechtlich obliegt die Risikobewertung der Schwachstellen gänzlich dem Hersteller. Selbst wenn eine Cybersicherheitslücke nachgewiesen wird, ist der Hersteller gesetzlich gemäß europäischer Medizinprodukteverordnung nur dann verpflichtet, dies als sogenanntes Vorkommnis der zuständigen Behörde zu melden, wenn er darin ein schwerwiegendes Patientenrisiko sieht.

Bei dem Projekt räumte nur einer von elf Herstellern ein, dass sein Medizinprodukt, eine Insulinpumpe, Sicherheitslücken aufwies, die Auswirkungen auf die Patientensicherheit hatten. Angreifer hätten die Pumpe entsperren, die Pumpenkonfiguration ändern, einen Insulinbolus verabreichen und die maximale tägliche Insulindosis ändern können.

Der Hersteller meldete diese Schwachstellen der zuständigen Bundesbehörde, dem Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM), das die Sicherheitsmitteilung in seine Datenbank einstellte. Die übrigen im Bericht genannten Sicherheitslücken wurden ohne Meldung ans BfArM behoben. Für Sicherheitsmeldungen zur Cybersicherheit von Medizinprodukten hat das BfArM auf seiner Homepage eine eigene Rubrik eingerichtet.

Wo drohen welche Gefahren?

Jedes Jahr veröffentlicht das BSI einen sektorenübergreifenden Bericht zur IT-Sicherheitslage in Deutschland, in dem zahlreiche Vorfälle ausgewertet werden. Der Lagebericht 2022 zeigt deutlich, dass die Gefährdungslage im Cyber-Raum aktuell so hoch ist wie nie zuvor. Insbesondere Angriffe mit Ransomware (Schadsoftware, die für Erpressungen verwendet wird) haben zugenommen. Beispielsweise wurde ein internationales Medizintechnologie-Unternehmen im September 2021 Opfer eines solchen Angriffs. Unternehmensdaten seien zwar nicht abgeflossen, Datenübertragungen zu Teilen der Vertriebs- und Produktionsnetzwerke mussten aber eingestellt werden.

Zu Prüfungszwecken versuchen Sicherheitsexperten ebenfalls gezielt von außen in Systeme einzudringen. Mithilfe solcher »Penetrationstests« werden den Unternehmen dann die entsprechenden Sicherheitslücken aufgezeigt. Ein Team des Kollektivs *zerforschung* hat im Juni 2022 einen Bericht über zwei medizinische Apps veröffentlicht, die auch als DiGA gelistet sind. Über die Sicherheitslücken eines Behandlungsprogramms bei Depressionen und einer Anwendung zur Unterstützung Brustkrebserkrankter konnten mehr als 20 000 Datensätze ausgelesen werden, darunter E-Mail-Adressen, Passwörter und Diagnosen. Mittlerweile konnten die Sicherheitslücken geschlossen werden. Doch zeigen die Fälle, wie wichtig gesetzliche Nachbesserungen sind.

Um als DiGA von den Krankenkassen vergütet werden zu können, durchlaufen medizinische Apps einen Zulassungsprozess beim BfArM. Bei der Cybersicherheit stützt sich das BfArM zum Teil auf die Selbstauskunft der Hersteller. Schrittweise wird nun gesetzlich nachgebessert: Bis zum 1. August 2024 müssen verschiedene Sicherheitsmaßnahmen von unabhängigen Stellen geprüft und zertifiziert werden.

Hohe Anforderungen an die Cybersicherheit sind umso mehr gefordert, wenn es um telemedizinische Versorgungsangebote geht, die lebenserhaltende Produkte wie zum Beispiel Kardioverter-Defibrillatoren beinhalten. Neue Entwicklungen, wie die Verwendung von patienteneigenen Smartphones als Kommunikationsschnittstelle zwischen Implantaten und den Servern der Gerätehersteller, bringen neue Risiken mit sich, die angemessen berücksichtigt werden müssen.

Wie (cyber)sicher sind Medizinprodukte?

Auch wenn Patientenschäden infolge eines gezielten Cyber-Angriffs auf ein Medizinprodukt bisher nicht bekannt sind, haben Angriffe auf die Systeme von Einrichtungen und Herstellern bis heute bereits Behandlungen behindert und Patientendaten offengelegt. Der Lagebericht des BSI zeigt, dass die Angriffe zunehmen und die Angreifer kreativer werden. Man kann nur vermuten, dass es sich bei den bislang bekannt gewordenen Schadensfällen zu Medizinprodukten – wie auch in anderen Bereichen – um die Spitze des Eisbergs handelt. Umso wichtiger ist es, dass die Gesetzgebung zeitnah klare Vorgaben schafft, ein hohes Cybersicherheitsniveau verpflichtend vorschreibt und dabei die verbindliche Meldung entsprechender Vorkommnisse berücksichtigt. Nur wenn Schwachstellen schnell und transparent kommuniziert werden und alle Akteure mit gebündelter Fachexpertise zusammenarbeiten, kann beim Wettrennen um die Cybersicherheit von Medizinprodukten ein Vorsprung vor Angreifern aufgebaut werden.

Le Nguyen, M.Sc., ist Fachmitarbeiter im Team Medizinprodukte beim Medizinischen Dienst Bund.
l.nguyen@md-bund.de