Ohne Security keine KI

Warum Cybersecurity der Schlüssel für KI-Anwendungen in der Medizintechnik ist

© designbyfreepik

Ein KI-gestützter OP-Roboter, ein intelligentes Monitoring-System oder eine vernetzte Bildgebung kann klinische Abläufe heute spürbar verbessern. Solange die Systeme vertrauenswürdig funktionieren. Doch genau hier zeichnet sich auch die größte Bedrohungslage ab: Aus dem Gesundheitswesen gingen zwischen Mitte 2023 und Mitte 2024 141 Meldungen zu erheblichen IT-Störungen oder -Ausfällen beim BSI ein. Gleichzeitig spricht das BKA bundesweit von zwei bis drei schweren Ransomware-Angriffen pro Tag.

KI in der Medizintechnik braucht sichere Daten

KI-Modelle sind nur so gut wie die Daten, mit denen sie trainiert und betrieben werden. In der Medizintechnik entsteht daraus ein Zielkonflikt: Für leistungsfähige Anwendungen wie automatisierte Patientenüberwachung oder Medikamentenpläne werden hochwertige Daten benötigt. Gleichzeitig sind Gesundheitsdaten aber besonders schützenswert.

Mit dieser Thematik beschäftigt sich Sebastian Peralta Friedburg, Experte für Cybersecurity, KI und Software-Entwicklung beim Technologieunternehmen TQ. Der Systemanbieter für Electronics Engineering und Manufacturing Services verfügt über ein mehr als 300-köpfiges Team erfahrener Entwickler, die unter anderem Hersteller dabei unterstützen, Cybersecurity von Anfang an zu denken und so ihre Systeme – von der Embedded-Lösung über die Gerätesoftware bis hin zur Cloud Anwendung – gemeinsam abzusichern.

Repräsentativ, gut strukturiert und nachvollziehbar

Peralta Friedburg erläutert: „Damit erhobene Daten für das Training von KI-Modellen geeignet sind, müssen sie repräsentativ, gut strukturiert und nachvollziehbar sein.“ Werden ungeeignete oder fehlerhafte Trainingsdaten verwendet, kann dies zu verzerrten Modellen und falschen Entscheidungen führen mit potenziellen Auswirkungen auf medizinische Diagnosen oder Behandlungsprozesse. Ebenso entscheidend ist daher, wer Zugriff auf diese Daten hat und wie dieser kontrolliert wird. Ohne klare Zugriffsregelungen steigt das Risiko von Manipulationen, Datenlecks oder sogar gezielten Cyberangriffen, die kritische Systeme beeinträchtigen können.

Die drei Schutzziele der Informationssicherheit

Für die Datensammlung und -verarbeitung in KI-basierten Medizinanwendungen gelten deshalb besondere Anforderungen, die sich entlang der klassischen Schutzziele der Informationssicherheit strukturieren lassen. Erstens **Integrität**: Daten müssen integer und vor Manipulation geschützt sein. Falsche Daten können ein KI-System gefährlich verzerren und zum Beispiel zu falschen Vorhersagen führen. Zweitens **Vertraulichkeit**: Der Zugriff auf Patientendaten muss strikt kontrolliert und abgesichert sein. Sensible Informationen dürfen nur von autorisierten Personen eingesehen oder verarbeitet werden und sollten möglichst anonymisiert oder pseudonymisiert vorliegen. Drittens **Verfügbarkeit**: Daten, Dienste und Geräte müssen jederzeit erreichbar sein und zugleich vor Ausfällen, Sabotage und Ransomware geschützt werden.

Ganzheitliche Sicherheitsmaßnahmen

Welche Maßnahmen sind also aus Sicht von TQ notwendig, um eine sichere Datensammlung zu gewährleisten? „Wir unterscheiden hier in drei Kategorien: technische, organisatorische und regulatorische. Nur durch ein stimmiges Zusammenspiel von allen kann wirksame Sicherheit erreicht werden“, beschreibt Peralta Friedburg weiter. Zu den technischen Grundlagen gehören Ende-zu-Ende-Verschlüsselung bei Übertragung und Speicherung sowie Pseudonymisierung oder Anonymisierung, damit Daten für KI-Anwendungen nutzbar bleiben, ohne direkten Personenbezug offenzulegen.

TQ-Systems GmbH
info@tq-group.com
www.tq-group.com

Rollenbasierte Zugriffsmodelle und klare Verantwortlichkeiten regeln, wer welche Daten sehen oder verarbeiten darf; Zero-Trust-Ansätze ergänzen dies, indem jeder Zugriff konsequent geprüft wird – unabhängig davon, von welchem Netz, System oder Benutzer er kommt. Besonders kritisch sind zudem Schnittstellen: Werden medizinische Daten zwischen Systemen ausgetauscht, sollten ausschließlich standardisierte und abgesicherte APIs mit klar geregelter Authentifizierung und Autorisierung eingesetzt werden. Nur so lässt sich verhindern, dass unsichere Integrationen entstehen oder sensible Daten durch fehlerhafte Implementierungen unkontrolliert abfließen.

Organisatorisch sorgen Audits, Trails und Monitoring dafür, dass Datenzugriff nachvollziehbar bleibt und Anomalien früh erkannt werden. Ergänzend sind klar definierte Zugriffsrechte und rollenbasierte Berechtigungskonzepte essenziell. So lässt sich sicherstellen, dass sensible Informationen nur von autorisierten Personen eingesehen oder verarbeitet werden.

Schulungen für Klinik- und IT-Personal sorgen für einen sicheren Umgang mit Daten oder Cyberrisiken. Ebenso wichtig sind Incident-Response-Pläne: Sie sollten nicht nur dokumentiert sein, sondern regelmäßig geübt werden, damit im Ernstfall klar definiert ist, wie Systeme isoliert, Schäden begrenzt und der Betrieb strukturiert wiederhergestellt wird.

Auch regulatorisch besteht ein klarer Rahmen, der „Privacy and Security by Design“ voraussetzt. Im Medizinprodukterecht wird IT-Sicherheit zunehmend als verbindlicher Bestandteil vernetzter Medizinprodukte verankert. So definieren die MDR sowie die Norm IEC 81001-5-1 konkrete Anforderungen an die Cybersecurity von Medizinprodukten, während die DSGVO unter anderem das Prinzip der Datenminimierung festschreibt. Hinzu kommen allgemeine Vorgaben für vernetzte Produkte wie der Cyber Resilience Act (CRA) und – je nach Gerätetyp – die Radio Equipment Directive (RED). Hersteller müssen damit Security nicht nur umsetzen,

© *designbyfreepik*

sondern auch nachvollziehbar dokumentieren und über den gesamten Produktlebenszyklus pflegen.

Security by Design mit DevSecOps

Mit KI steigt die Veränderungsgeschwindigkeit: „Cyberbedrohungen entwickeln sich ständig weiter, leistungsfähigere KI-Modelle kommen hinzu und damit auch neue regulatorische Anforderungen“, warnt der Software-Experte. „Deshalb haben wir uns in der Entwicklung bei TQ dem ganzheitlichen Ansatz des Secure Software Development Lifecycle verschrieben.“ Konkret nutzt das Unternehmen ein DevSecOps (Development, Security, Operations) Framework. Hierbei handelt es sich um ein kontinuierliches Entwicklungs- und Betriebsmodell, was Cybersecurity als laufenden Prozess und nicht als einmaligen Zyklus versteht. Praktisch bedeutet das: Security-Anforderungen werden früh in Architektur und Design verankert, Security-Tests werden in Build- und Testketten automatisiert, und der Betrieb wird durch Schwachstellenmanagement, geregelte Update-Prozesse und kontinuierliches Monitoring flankiert, um das System stetig zu verbessern.

Warum sich Security früh lohnt

Neben Patientensicherheit und Compliance spricht ein weiteres Argument für „Security early“: Kosten. Je später Schwachstellen gefunden und behoben werden, desto teurer wird es technisch, organisatorisch und im Zulassungsprozess. Genau hier setzt das „Shift-left“-Prinzip an, was auch vom Technologieführer angewendet wird: Sicherheitsanforderungen, Tests und Prüfungen werden im Entwicklungsprozess bewusst nach vorne verlagert, also bereits in Architektur, Design und frühe Entwicklungsphasen integriert, statt erst am Ende vor der Zulassung oder im Feldbetrieb adressiert zu werden. Das reduziert Risiken, erhöht die Qualität, verhindert Rework und unangenehme Überraschungen bei den Zulassungen. Als Ergebnis reduziert sich die Time-to-Market, auch wenn die Planung und Entwicklungsphase in erster Instanz länger und aufwendiger werden.

End-to-End-Expertise bei TQ

KI in Medizinanwendungen eröffnet große Chancen, geht jedoch zugleich mit hohen Anforderungen an Sicherheit, Rechenleistung und regulatorische Konformität einher. Um diese Komplexität beherrschbar zu machen, empfiehlt es sich, auf erfahrene Partner mit entsprechender Expertise zu setzen.

TQ begleitet als zuverlässiger Systemanbieter Hersteller über den gesamten Produktlebenszyklus hinweg – angefangen bei Requirements Engineering oder Anforderungserklärungen bis hin zu Beratungsworkshops. Kunden profitieren dabei besonders von der engen interdisziplinären Zusammenarbeit (Cybersecurity, KI, Software etc.) und dem 360-Grad-Ansatz des Unternehmens. Dazu gehören nämlich neben der ganzheitlichen Entwicklung auch eine umfassend zertifizierte Fertigung, ein akkreditiertes Prüflabor und After-Sales-Services inklusive Obsoleszenz Management für nachhaltige, resiliente Elektronik.

„Bei TQ verfügen wir nicht nur über die notwendigen Kapazitäten, sondern auch über mehr als 30 Jahre Erfahrung und zahlreiche erfolgreiche Medizinprojekte, um in einem so anspruchsvollen Umfeld wie der Medizintechnik sichere Systeme zu entwickeln“, betont Sebastian Peralta Friedburg. ◄