Prüfung der Cybersecurity von IVD-Medizinprodukten

Categories : Allgemein

Date : 6. Juni 2023

Komplexe Systeme mit unterschiedlichen Schnittstellen, die potenziell angreifbar sind, resultieren aus der zunehmend digitalen Vernetzung der medizinischen Infrastruktur. Nach der IVDR müssen Hersteller die Cybersecurity vor Inverkehrbringen nachweisen. Die Übergangsfristen für bereits zertifizierte Produkte laufen gestaffelt ab 26. Mai 2025 ab. Aufgrund der begrenzten Zahl an Benannten Stellen kann es bei den Konformitätsbewertungsverfahren jedoch zu Engpässen kommen. TÜV Süd unterstützt mit umfangreichen Prüf- und Testing-Services und stellt neue Whitepaper zur Verfügung.

„Das Thema betrifft alle Geräte, die mit einem Netzwerk verbunden werden können. In Krankenhaus-Laboren und -Stationen existieren zahlreiche IVD-Medizinprodukte, die mit Medizinprodukten und Informationssystemen vernetzt sind“, sagt Dr. Alexander Stock, Project Manager IVD Medical Device Testing bei TÜV Süd. „Ein unbefugter Zugriff kann neben dem Verlust vertraulicher Daten vor allem die Patientensicherheit und sogar die öffentliche Gesundheit gefährden.“ Die Manipulation von Testdaten kann zu einer falschen Diagnose und somit zu einer falschen Therapie führen, aber auch zu Fehlschlüssen beispielsweise bei der Einschätzung zum Infektionsgeschehen in einer Pandemie. Hersteller und Betreiber von unsicheren Geräten müssen neben den finanziellen Risiken auch mit Imageschäden rechnen.

Wettrennen um die Patientensicherheit

Cybersecurity-Risiken sollten frühzeitig und kontinuierlich über den gesamten Produktlebenszyklus berücksichtigt werden – von der Entwicklungsphase, über die Herstellung, Installation und Wartungsphase. Der Grund dafür ist, dass täglich neue Schwachstellen gefunden und veröffentlicht werden, die IVD-Geräte angreifbar machen können. Diese Sicherheitslücken kommen zum Beispiel aus Modulen oder Bibliotheken von Programmiersprachen und Betriebssystemen. Als Folge müssen die Hersteller kontinuierliche Risikoanalysen betreiben, permanent Updates für ihre Geräte anbieten, sie auf dem neuesten Stand halten und gegebenenfalls kurzfristig reagieren.

IVD-Geräte erfordern die gleiche Cybersecurity-Betrachtung wie vernetzte Medizinprodukte. Das schließt Threat Modeling beziehungsweise Threat-Analyse ein – Verfahren zum Cybersecurity-Risikomanagement – mit dem Ziel, die Bedrohungen frühzeitig zu identifizieren und Maßnahmen davon abzuleiten. Die verpflichtende regulatorische Basis ist die IVDR, deren Annex I grundlegende Anforderungen an die Cybersecurity enthält. Weitere Hilfestellung bieten die so genannten MDCG-Leitlinien der Medical Device Coordination Group der EU, Positionspapier der Benannten Stellen, sowie die ISO 14971 für das Risikomanagement bei Medizinprodukten und die IEC 81001-5-1 für die sicherheitsbezogenen Aktivitäten im Software-Lebenszyklus.

TÜV Süd hat zusätzlich drei Whitepaper erarbeitet, von denen Hersteller und Betreiber profitieren: eines zur Cybersecurity von Medizinprodukten nach IEC 81001-5-1, einer Health-Software-Norm, und eines zum Produktstandard IEC TR 60601-4-5 für medizinisch-elektrische Geräte sowie ein aktuelles direkt zur Cybersecurity von IVD-Geräten und -Produkten.

Fünf-Stufen-Ansatz für Sicherheit

TÜV Süd verfügt über akkreditierte Prüflabore und bietet umfassende Prüfleistungen und Testing-Services für IVD-Geräte und -Produkte sowie produktindividuelle Cybersecurity-Tests. Je nach Stand des Produktes im Lebenszyklus umfasst das fünf Stufen: Training zu den Normen und regulatorischen Vorgaben, Early-Bird-Assessment, Fuzzing, Vulnerability Scanning und einen Penetration-Test (simulierter Cyberangriff).

TÜV Süd betreibt zudem das einzige akkreditierte Prüf- und Validierungslabor für die IEC TR 60601-4-5. Die Expertinnen und Experten kennen die unterschiedlichen länderspezifischen regulatorischen Anforderungen. Sie unterstützen Hersteller, ihre Geräte und Produkte sicher und zeiteffizient in Verkehr zu bringen und wissen auch um die Anforderungen an eine rechtssichere Dokumentation.

IVD-Geräte und Produkte, die bereits vor dem Geltungsbeginn der IVDR rechtmäßig in Verkehr gebracht wurden, dürfen derzeit unter bestimmten Voraussetzungen weiterhin befristet in Verkehr gebracht werden (IVDR, Artikel 110). Allerdings laufen die Übergangsfristen je nach Risikoklasse des Produkts bald ab: Für Risikoklasse D ist es der 26. Mai 2025, für Klasse C der 26. Mai 2026, für Klasse B und für Produkte der Klasse A, die in sterilem Zustand in Verkehr gebracht werden, der 26. Mai 2027.