Pressemitteilung

Medizinprodukte und In-vitro-Diagnostika 6. September 2023

TÜV SÜD fordert EU-weite Norm für Cybersecurity-Tests

München. TÜV SÜD fordert die Ausgestaltung der Vorgehensweise bei den verpflichtenden Penetrationstests für Medizinprodukte und In-vitro-Diagnostika (IVD) und veröffentlicht dazu ein neues White Paper. Weder die regulatorischen Vorgaben der EU noch die zugehörigen Guidance-Dokumente enthalten bislang konkrete Leitlinien. Eine zugehörige Norm sollte künftig klären, was, wo, wie und in welchem Umfang zu prüfen ist. So lässt sich gewährleisten, dass netzwerkfähige Produkte im Sinne der Patienten auch tatsächlich cyber-sicher sind.

Jan Küfner
Senior Product Specialist (SPS)
Cybersecurity

Dr. Abtin Rad
Global Director Functional Safety,
Software and Digitization

Dr. Alexander Stock
Projektleiter IVD-Prüfungen
TÜV SÜD MHS

„Noch fehlen zum Beispiel genaue Aussagen darüber, ob es eine geringere Prüftiefe für Medizinprodukte und IVDs mit geringerem Risiko geben sollte, obwohl dies ja nahe liegt“, sagt Jan Küfner, Senior Product Specialist für Cybersecurity bei TÜV SÜD. Muss zum Beispiel bei einer Software für jedes Release ein vollständiger Penetrationstest erfolgen? Wie sind Ethernet und Bluetooth-Verbindungen zu prüfen? Wann ist Fuzzing überhaupt erforderlich und in welchem Umfang? Beim Penetrationstest simulieren sogenannte Ethical Hacker einen IT-Angriff auf ein Medizinprodukt oder IVD. So finden sie Schwachstellen, bevor diese von Dritten ausgenutzt werden. Beim so genannten Fuzzing provozieren die Prüferinnen und Prüfer Fehlverhalten von Software, indem sie zufällige, teils

manipulierte Daten einspeisen. Das von TÜV SÜD veröffentlichte White Paper geht bestehenden Lücken anhand konkreter Fragen aus Sicht von Herstellern und Unternehmen auf den Grund. Diese Fragen sollten verbesserte Standards in Zukunft beantworten.

EU-Verordnungen wie die Medical Device Regulation (MDR) für Medizinprodukte und die In-Vitro Diagnostics Regulation (IVDR) machen zwar Vorgaben zur Cybersecurity. „Aber der zugehörigen europäischen Leitlinie MDCG 2019-16, die die Anforderungen an den Prozess klären soll, fehlen entscheidende Details. Gleiches gilt für die internationale Norm IEC 81001-5-1, die sich mit IT-Sicherheit im Software-Lebenszyklus befasst“, sagt Dr. Abtin Rad, Experte für Cybersicherheit und Künstliche Intelligenz bei TÜV SÜD. „Die von der EU für das kommende Jahr angekündigte Harmonisierung bietet die Chance, anhand einer einheitlichen EU-Norm die teils bestehenden länderspezifischen Standards zu vereinheitlichen.“

Prüfumfang bei dynamischer Bedrohungslage klären

Weil sich die IT-Werkzeuge weiterentwickeln und neue Software oder Updates neue Schwachstellen generieren können, wandelt sich die Bedrohungslage ständig. So unterstützt Künstliche Intelligenz nicht nur die Medizinerinnen und Mediziner, sondern auch die Angreifer. Um in kürzester Zeit große Mengen an medizinischen Daten zu analysieren, müssen Ultraschallgeräte oder Hämoglobinzähler zudem digital vernetzt werden. Das wiederum bietet eine größere Angriffsfläche für Cyberattacken.

Unsichere Produkte bergen Risiken für die Patientensicherheit, die Datensicherheit und den Datenschutz. Bei manipulierten Daten besteht zudem die Gefahr von falschen Diagnosen und Therapieansätzen oder einer Gefährdung der öffentlichen Gesundheit, etwa bei Fehleinschätzungen zum Infektionsgeschehen. Eine verweigerte oder verzögerte Marktzulassung, Entschädigungszahlungen und Imageschäden wären weitere Folgen.

TÜV SÜD-Expertinnen und Experten übernehmen unter anderem Schwachstellenanalysen, Penetrationstests oder so genannte Fuzzing-Kampagnen. Dabei greifen sie auf ein weltweites Netzwerk von Pentest-Laboren[1] zurück. Um stets das Patientenrisiko im Fokus zu halten, konzentrieren sich die Pentest-Experten von TÜV SÜD auf Medical Devices und IVDs. In dieser Hinsicht bieten klassische Cybersecurity-Methoden nicht immer passgenaue Lösungen. Auf Basis der ermittelten Risiken können Unternehmen maßgeschneiderte Lösungen für Netzwerke, mobile oder Web-Anwendungen entwickeln. Mittels seiner Vorgehensweise verkürzt der Prüfdienstleister die Time-to-Market für IVDs und Medical Devices deutlich. Dr. Alexander Stock, Projektleiter IVD-Prüfungen bei TÜV SÜD: „Dabei arbeiten wir vernetzt mit unseren Kolleginnen und Kollegen in Singapur, Japan, Indien, China und den USA. In

[1] München, Singapur, Shanghai, Tokio, Bangalore, Pune, Michigan, San Diego.

Cybersicherheits-Trainings schult TÜV SÜD zudem externe Experten zur Zweckbestimmung von Medizinprodukten oder den unterschiedlichen landesspezifischen regulatorischen Anforderungen."

TÜV SÜD White Paper:

Cybersicherheit von Medizinprodukten – die Lücke in den aktuellen EU-Verordnungen:

- https://www.tuvsud.com/de-de/wissenswert/white-paper/whitepaper-cybersecurity-medizinprodukte
- https://www.tuvsud.com/de-de/-/media/de/product-service/pdf/whitepaper/whitepaper-cybersecurity-de.pdf

Weitere Infos: https://www.tuvsud.com/de-de/dienstleistungen/cyber-security/cyber-security-assessments/penetrationstests/it-penetrationstest

Hinweis für Redaktionen: Die Pressemeldung und die Bilder von Jan Küfner, Dr. Abtin Rad und Dr. Alexander Stock in reprofähiger Auflösung gibt es im Internet unter www.tuvsud.com/presse.

Pressekontakt:

Dirk Moser-Delarami TÜV SÜD AG Unternehmenskommunikation Westendstr. 199, 80686 München	Tel. +49 (0) 89 / 57 91 – 15 92 Fax +49 (0) 89 / 57 91 – 22 69 E-Mail dirk.moser-delarami@tuvsud.com Internet www.tuvsud.com/de

Im Jahr 1866 als Dampfkesselrevisionsverein gegründet, ist TÜV SÜD heute ein weltweit tätiges Unternehmen. Mehr als 26.000 Mitarbeiter sorgen an über 1.000 Standorten in rund 50 Ländern für die Optimierung von Technik, Systemen und Know-how. Sie leisten einen wesentlichen Beitrag dazu, technische Innovationen wie Industrie 4.0, autonomes Fahren oder Erneuerbare Energien sicher und zuverlässig zu machen. www.tuvsud.com/de