Cybersicherheit verliert ihren Schrecken

Weltweit ist eine Sensibilisierung der Regulierer für Cybersecurity zu erkennen. Doch wer kümmert sich um die Cybersicherheit für Medizinprodukte?

Hans-Otto von Wietersheim, Bretten

© THAWEERAT / adobe stock.com

Die fortschreitende Digitalisierung betrifft und beeinflusst nahezu alle Bereiche unseres täglichen Lebens. Überall dort, wo ein höherer Komfort und ein besseres „Nutzer-Erlebnis“ (User Experience, UX) dazu beitragen, das Leben zu verbessern oder zu erleichtern, werden sich die Digitalisierung und die damit verbundenen Anwendungen sehr schnell durchsetzen. Mit vernetzten Medizinprodukten können wichtige Diagnosedaten schnell übertragen, ausgewertet oder kontrolliert werden. Doch die Vernetzung der Medizintechnik bringt nicht nur Vorteile, sie birgt auch Risiken. Die hochsensiblen Daten von Patienten müssen sicher sein, d. h., sie müssen vor den täglich lauernden Cyberattacken geschützt werden. Zu den bedrohten Geräten gehören z. B. Implantate, Produkte zur Injektion, Infusion, Transfusion und Dialyse, humanmedizinische Instrumente, Software, Katheter, Herzschrittmacher, Dentalprodukte, Verbandstoffe, Sehhilfen, Röntgengeräte, Kondome, ärztliche Instrumente, Labordiagnostika, Produkte zur Empfängnisregelung sowie In-vitro-Diagnostika. Der unbefugte Zugriff auf ein Medizinprodukt kann zu schwerwiegenden Konsequenzen führen. Daher ist es besonders wichtig, dass Cybersecurity-Risiken sowohl in der Entwicklungsphase als auch bei der Installation und Beschaffung von Medizinprodukten berücksichtigt werden. Für die Zulassung von Medizinprodukten wird im Allgemeinen ein Plausibilitätsnachweis gefordert. Dieser ist naturgemäß schwer zu erbringen, wenn eine Maschine aufgrund maschineller Erfahrungen eine Dateninterpretation durch deep learning vorgenommen hat.

Nutzung nur mit Risikoanalyse

Die gesellschaftliche Akzeptanz zur Anwendung digitaler Dienste hat sich durch die Nutzung der mobilen Endgeräte entscheidend verändert bzw. befindet sich in einer Transformationsphase. Der Gebrauch von Chat- und Messaging-Diensten hat eine Dynamik erreicht, die nahezu jede Altersgruppe anspricht und in vielen Lebenslagen genutzt, sogar erwartet wird. Datenschutz spielt in der Wahrnehmung der Anwender, insbesondere bei den „Digital Natives“, eine untergeordnete Rolle. Speziell im Gesundheitswesen steht jedoch der Schutz der Daten an erster Stelle. Dieser Logik folgend wird eine sehr sichere Infrastruktur benötigt, die gegen kriminelle „Hackerangriffe“ immun ist. Die Sicherheitsinfrastruktur muss die Eigenschaft besitzen, Manipulationen sofort aufzudecken oder diese wenigstens so zu erschweren, dass ein Cyberangriff unwirtschaftlich ist und die gestohlenen oder manipulierten Daten wertlos sind. Es beansprucht somit die Möglichkeit, einerseits die Daten bereitzustellen und andererseits deren Schutz zu gewährleisten. Nur dann kann Vertrauen und die damit verbundene Akzeptanz in ein neues System erreicht werden. Dieses Vertrauensverhältnis zwischen Partnern kann nur dadurch erreicht werden, dass eine Vielzahl von Teilnehmern die Daten bzw. die damit verbundenen Transaktionen validieren, für korrekt befinden und erst nach einer gemeinsamen Abstimmung (Konsens) die Änderungen an den Daten vornehmen. Die Arzt-Patienten-Beziehung im medizinischen Umfeld kann nun analog zum Vertrauensverhältnis zwischen Partnern in einem IT-Netzwerk betrachtet werden, d. h. Patienten, Ärzte, Medizintechniker, Forschungseinrichtungen, Apotheken etc. agieren direkt mit- und untereinander.

Anforderungen leiten IoT

Vorbei sind die Zeiten, als Bedenken in Sachen Security und Datenintegrität die größten Hürden bei der Einführung von IoT waren. Die COVID-19-Pandemie und die damit einhergehenden Mobilitätsbegrenzungen, Kontaktverbote, Handy-Überwachungs-Apps sowie weitere Strategien zur Eindämmung von Infektionsketten hat in den vergangenen beiden Jahren zu einem eindeutigen Anstieg der Nutzung digitaler Anwendungen im öffentlichen und privaten Gesundheitswesen geführt. Verbesserte Daten-Analysen in der Forschung, Entwicklung und Prüfung von neuen Therapien, sowie das wachsende Potenzial der KI für im Eilverfahren entwickelte diagnostische Methoden und Impfstoffkandidaten, mündete ebenfalls in einer gestiegenen Nachfrage und Anwendung von digitalen Hilfsmitteln unter Ärzten, Patienten, Krankenhäusern, Forschern und Unternehmen. Der Einsatz technischer Innovationen wurde jedoch sowohl von sozioökonomischen und politischen Diskussionen als auch von munteren ethischen und rechtlichen Debatten begleitet. Themen wie Datenschutz, Cybersicherheit, Einwilligung, Transparenz, Diskriminierung, Eigentum und eine gerechte Verteilung und Zugang zu den digitalen Möglichkeiten spielen hierbei eine wichtige Rolle. Zutreffend ist diese Thematik auch für KI, KNN, Musterkennung und Robotik, die voneinander abhängen.

Sicherheit für IoT-Gestaltung

Nutzern von IoT-Lösungen im Gesundheitsbereich ist mitunter nicht bewusst, welcher Art von Datenverarbeitung sie zustimmen und welche Daten überhaupt erhoben werden. Die möglichen Bedrohungen und Angriffsvektoren sowie Datenschutzaspekte in IoT-Umgebungen sind nicht immer vollständig offengelegt. Existierende Maßnahmen werden in Fachkreisen zwar diskutiert, wie etwa die Einführung von technischen Richtlinien und Normen oder Zertifizierungsmöglichkeiten. Doch diese zielen darauf ab, verschiedene Ebenen der IoT-Architektur hinsichtlich Sicherheit und Datenschutz zu verbessern, vernachlässigen jedoch meist die Berücksichtigung von Emergenzen. Lösungen sind eindeutig durch eine Internetadresse (URL) identifizierbar und über das Internet ansprechbar – aber bei mangelnder Sicherheit auch leicht zu kompromittieren. Bislang ungesicherte Lösungen aus dem Bereich des IoT, vor allem Endverbrauchergeräte wie Fitnesstracker und andere Wearables, wurden oft als Angriffsplattform und Einfallstor in Netzwerke und Infrastrukturen missbraucht. Das sei einerseits darauf zurückzuführen, das Cybersecurity noch kein integraler Bestandteil der Produktentwicklung auf Herstellerseite sei, andererseits seien sich aber auch die Anwender der Wichtigkeit von Basis-Sicherheitsmaßnahmen, wie dem Ändern voreingestellter Hersteller-Passwörter, noch nicht bewusst. So hätten Angreifer leichtes Spiel.

Robotik für viele Fälle

Der Umgang mit Information ist den letzten Jahrzehnten in jedem Bereich exponentiell gewachsen und setzt heute völlig neue Denk- und Strukturansätze voraus, damit Menschen auch in der Zukunft mit der zunehmenden Informationsflut sinnvoll umgehen können. Allein in der Robotik manifestiert sich die Macht dieses Wandels, den die Informationstechnologie im letzten Jahrzehnt mit sich gebracht hat.

Ob Desinfektionsroboter für den Kampf gegen die Covid-19-Pandemie, Lernroboter, oder verschiedene Anwendungen in der Landwirtschaft: Es ist nicht zu übersehen, in wie vielen Lebensbereichen Robotik mittlerweile Einzug gehalten hat. Und es werden ständig mehr. Allerdings funktioniert eine energiegeladene Entwicklung nicht ohne Forschung, die Robotern neue Möglichkeiten eröffnet, und die hat im Jahr 2022 an Dynamik zugelegt. Für den Pflege- und Assistenzbereich arbeiteten Forscher beispielsweise and Robotern, die dank Drucksensoren gefühlvoll zugreifen können oder solchen, die beim Anziehen helfen. Bislang erstarren Assistenzroboter beispielsweise in der Pflege oft einfach, wenn ihre Bewegungssensoren eine drohende Kollision melden. Besser wäre es, wenn sie die eigene Bewegung anpassen würden. Genau das macht ein Roboter, den Forscher am Computer Science and Artificial Intelligence Laboratory (CSAIL) des Massachusetts Institute of Technology (MIT) so programmiert haben, dass er sich ähnlich bewegt wie ein Mensch. Er kann beispielsweise beim Anziehen einer Jacke helfen. „Die Entwicklung von Algorithmen, die körperliche Schäden verhindern, ohne die Effizienz unnötig zu beeinträchtigen, mit der die Roboter ihre Aufgabe erfüllen, war eine große Herausforderung“, sagt MIT-Doktorand Shen Li, der zu den Entwicklern der Software gehört. Der maschinelle Helfer müsse sich an die Menschen anpassen. Gleichzeitig müsse aber sichergestellt sein, dass er sein Gegenüber nicht verletzt. Ein strampelndes Kleinkind reagiere auf den Versuch, ihm ein Hemd anzuziehen, schließlich völlig anders als eine gebrechliche ältere Person oder ein Mensch mit Behinderung. „Unser Algorithmus berücksichtigt das“, so Li. Anfangs agiert der Roboter mit dem speziellen Algorithmus noch ein wenig unsicher, doch mit der Zeit lernt er dazu. „Dieses Forschungsergebnis lässt sich möglicherweise auf eine Vielzahl von Assistenzrobotern anwenden, die sie in die Lage versetzen, Menschen mit Behinderungen eine sicherere körperliche Unterstützung zu bieten“, so Zackory Erickson, Assistenzprofessor am Robotik-Institut der Carnegie Mellon University, der die Entwicklung seiner Kollegen begutachtete. Norwegische Forscher lehrten Robo-Vierbeiner, draußen ihren Gang gekonnt an den jeweiligen Untergrund anpassen, während die University of Cincinnati Robotern beibrachte, Türen zu öffnen und sich bei Bedarf selbst eine Steckdose zu suchen.