Software als Medizinprodukt: Sicherheit ist überlebenswichtig

Daniel Reichle

Sicherheit ist bei Software immer ein zentrales Thema. Bei Software im Gesundheitswesen kommt eine ganz neue Dimension hinzu. Hier hat die Gesetzgebung noch Lücken zu schliessen.

Die Digitalisierung hat im Gesundheitswesen längst Einzug gehalten. Betroffen sind nicht nur Systeme zum einfacheren Austausch bzw. zur Zentralisierung von Patientendaten (z.B. elektronisches Patientendossier in der Schweiz). Elektronische Geräte, wie sie Spitäler und Arztpraxen immer öfter einsetzen, sind zunehmend vernetzt. Zudem werden softwaregesteuerte Geräte vermehrt zum alltäglichen Begleiter von Patienten, z.B. in Form von Insulinpumpen oder implantierten Herzschrittmachern. Solche Geräte bringen dem Patienten einen immensen Mehrwert, erweitern aus Sicht der Cybersicherheit jedoch die Angriffsfläche.

Während Software von Systemen, die Patientendaten verarbeiten, vor allem Anforderungen des Datenschutzgesetzes erfüllen muss – bzw. der DSGVO bei Verarbeitung von Daten von EU-Bürgern oder HIPAA für den Einsatz in den USA –, ist es mit dem Schutz persönlicher Daten bei Software in medizinischen Geräten noch lange nicht getan. Denn eine Schwachstelle in der Software, die z.B. eine Insulinpumpe oder einen Herzschrittmacher steuert, kann für den Patienten lebensbedrohlich sein.

Software als Medizinprodukt

Die Anforderungen an die Sicherheit und Zuverlässigkeit von Software in medizinischen Geräten sind offensichtlich. In einem stark regulierten Bereich wie der Gesundheitsbranche liegt die Vermutung nahe, dass die Softwareentwicklung je nach Kritikalität der Anwendung regulatorischen Auflagen untersteht. Dies entspricht jedoch nur teilweise den Tatsachen. Obschon es nicht an gesetzlichen Bestimmungen und dazugehörigen Normen für die Zulassung von Software als Medizinprodukt mangelt [1], wird dabei jedoch das Thema Cybersicherheit kaum je explizit berücksichtigt. Die Folgen dieser Unterlassung waren in der Vergangenheit mehrfach zu beobachten: Cyberangriffe auf IT-Systeme, z.B. von Spitälern, mit dem Ziel, Geld zu erpressen.

Wie steht es um die Gesetzgebung?

In der EU ist 2017 die neue Verordnung über Medizinprodukte (Medical Device Regulation, MDR [2]) in Kraft getreten, die 2020 die Medizinprodukterichtlinie 93/42/EWG (Medical Device Directive, MDD) ersetzen wird. Diese EU-Richtlinien werden im Rahmen der bilateralen Verträge auch im schweizerischen Recht umgesetzt (v.a. über die Medizinprodukteverordnung MepV [3]). Die MDR bringt diverse Verschärfungen der Anforderungen an die Zulassung von Medizinprodukten mit sich, die Softwareprodukte zum Teil direkt betreffen. Die für die Softwareentwicklung relevante Norm IEC 62304 («Health software – Software life cycle processes») enthält im Moment keine Anforderungen an Cybersicherheit, wird aber wohl in der nächsten Version entsprechende Anforderungen beinhalten. Die aktuellen Anforderungen ergeben sich vor allem aus den Vorgaben für das Risikomanagement (IEC 14971), die ein angemessenes Sicherheitskonzept verlangen.

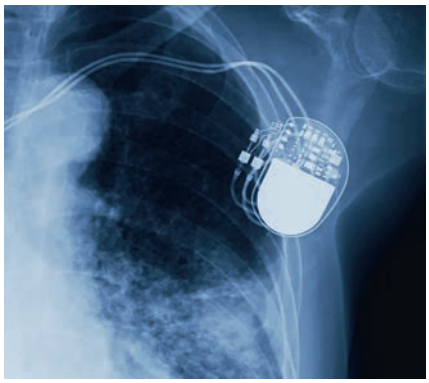
Daniel Reichle hat an der ETH das Studium zum diplomierten Informatik-Ingenieur absolviert und diverse Weiterbildungen in Informations- und IT-Sicherheit besucht. Er verfügt über 14 Jahre Erfahrung in der Software- und Informationssicherheits-Branche. Daniel Reichle arbeitet heute als Principal Information Security Engineer bei AdNovum.

Kontaktadresse:
Daniel Reichle
Principal Information Security Engineer
CO Security Consulting
AdNovum Informatik AG
Röntgenstrasse 22
CH-8005 Zürich
Tel: +41 44 272 61 11
E-Mail: daniel.reichle@adnovum.ch

In den USA hat die zuständige Gesundheitsbehörde FDA mehrere Richtlinien zum Thema Cybersicherheit für die Entwicklung von Medizinprodukt-Software veröffentlicht, wie zum Beispiel die Guideline «Content of Premarket Submissions for Management of Cybersecurity in Medical Devices», die zurzeit überarbeitet wird. Dabei ist die FDA [4] daran interessiert, Stakeholder einzubeziehen, um die Richtlinie möglichst effizient zu gestalten.

Fazit

Die regulatorischen Auflagen für Cybersicherheit bei der Entwicklung von Software im Gesundheitswesen nehmen tendenziell zu. Die in den Richtlinien beschriebenen Massnahmen entsprechen weitgehend den bekannten Prinzipien eines Secure Software Development Lifecycle, wo Security als integraler Teil des gesamten Softwareentwicklungsprozesses verstanden wird. Anzuführen wären hier Risikoanalysen, Berücksichtigung von Security Requirements, Secure Design, Secure Development und Security Testing. Diese Prinzipien sollten auch in der Entwicklung von IoT-Lösungen ohne Bezug zum Gesundheitswesen angewendet werden. Da dies leider (noch) keine Selbstverständlichkeit ist, gibt es bereits erste Gesetze, die die IoT- Sicherheit generell reglementieren [5].



Autor: © Choo / Fotolia

Referenzen

[1] Software als Medizinprodukt betrifft sowohl embedded Software in medizinischen Geräten, als auch standalone Software, welche z.B. der Diagnose von Krankheiten dient.

[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L:2017:117:FULL&from=DE

[3] https://www.admin.ch/opc/de/classified-compilation/19995459/index.html

[4] U.S. Food and Drug Administration https://www.fda.gov

[5] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=20172018oSB327

ifi news

Neues aus dem IfI

Renato Pajarola

Liebe Alumni

Ein neues Jahr bedeutet, dass sich für das IfI neue Herausforderungen und Optionen eröffnen. An dieser Stelle möchte ich erst einmal auf die bisherigen Erfolge hinweisen wie neue Projekte, Ehrungen und Medienpräsenz.

Das Projekt «Advanced Visual and Geometric Computing for 3D Capture, Display, and Fabrication» (EVOCATION) hat eine beträchtliche finanzielle Unterstützung erhalten. Das Projekt realisiere ich zusammen mit Kollegen der Universität Rostock, dem Centro di Ricerca, Sviluppo e Studi Superiori in Sardegna (CRS4), dem Consiglio Nazionale delle Ricerche {CNR), der TU Wien, des Fraunhofer IDG, von Holografika und Gexcel. Es wird erwartet, dass der 3D-Markt in naher Zukunft boomt und darauf abzielt, ein führendes europaweites Doktorandenkolleg zu schaffen. Das IfI kann auch auf erfolgreiche Paper Awards zurückblicken. Maria J. Puri und Lorenz Hilty erhielten für ihren Beitrag «ICT-Enabled Sharing Economy and Environmental Sustainability – a Ressource-oriented Approach» den Best Paper Award an der Konferenz Enviro-Info 2018. Das prämierte Paper schafft

Fortsetzung auf Seite 14