Medizintechnik-Geräte/Cybersecurity

Ab wann wird IT-Sicherheit zum kritischen Faktor für den Patienten?

von Nigel Stanley und Mark Coderre (Experten für Cybersecurity, TÜV Rheinland)

Geräte, Systeme und Prozesse – immer mehr ist über das Internet der Dinge (IoT) vernetzt. Zugleich ist es für viele Nutzer normal, persönliche Informationen gegen vermeintlich „kostenlose Dienste" zu tauschen. Für Hersteller sind die so generierten Verbraucher- und Nutzerdaten zunehmend ein eigener Wert und Basis für neue Geschäftsmodelle. Im Falle von Sicherheitsvorfällen drohen inzwischen allerdings drastische Strafen. Wie sicher ist zurzeit das IoT? Wie lassen sich Sicherheitsschwachstellen von vernetzten Medizingeräten so weit wie möglich vermeiden? Eine Bestandsaufnahme.

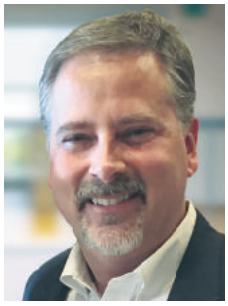
Der sinnvolle Einsatz von IoT-Geräten und damit erhobenen Daten kann unseren Lebensstandard und die Produktivität der Herstellung verbessern. Mit den zahlreichen Möglichkeiten von Big-Data-Analysen, bei denen Daten gezielt auf nützliche Informationen untersucht werden, eröffnen sich neue und vielversprechende kommerzielle Möglichkeiten.

Grundlage für diese neuen Geschäftsmodelle ist das Internet of Things (IoT) oder auch Internet der Dinge. Immer mehr Hersteller bieten Produkte oder Services an, mit denen sich die Vorteile des Internets und des World Wide Web umfassend nutzen lassen. Bis 2020 geht das US-Marktforschungsunternehmen Gartner von weltweit mehr als 20,4 Mrd. vernetzten Geräten aus.

Hersteller von Medizingeräten haben bereits früh erkannt, dass das Leben von Patienten und Ärzten durch die Ausstattung von Geräten mit IoT-Funktionalität verbessert werden kann. Gute Beispiele dafür sind die zahlreichen Blutzucker-Messgeräte, die per Smartphone gesteuert werden und Daten via Internet übermitteln.

Allerdings hat so mancher Hersteller von Medizingeräten seine Geräte recht übereilt an das IoT angepasst, ohne die damit verbundenen Probleme rund um Cybersecurity zu beachten bzw. sie zu lösen. Die folgenden in diesem Zusammenhang aufgeführten Schwachstellen sind da lediglich die Spitze des Eisbergs:

Nigel Stanley.



Mark Coderre.

- mangelhafte oder fehlerbehaftete Soft- bzw. Firmware, die die Sensibilität und Integrität medizinischer Daten bzw. Funktionen nicht adressiert,
- falsch konfigurierte Netzwerkdienste mit unverschlüsselter Übertragung von Patientendaten,
- die Verwendung schwacher Passwörter oder eine zu weitreichende Vergabe von Berechtigungen für nicht privilegierte Benutzer, die als Einfallstore für Hacker dienen können.

Einer der bekanntesten Vorfälle im Gesundheitswesen stammt aus dem Jahr 2015. Seinerzeit warnte die US-amerikanische Bundesbehörde für Arzneimittel und Medizinprodukte, Federal Drug Agency (FDA), vor dem Hospira-Symbiq-Infusionssystem. Über das Krankenhausnetzwerk hätte ein nicht autorisierter Dritter die Infusionspumpe unter seine Kontrolle bringen und die verabreichte Dosis verändern können. Konkrete Vorfälle waren jedoch nicht bekannt geworden.

Vom Markt genommen wurde das Symbiq-Infusionssystem dennoch, weil auch noch andere Schwachstellen zutage getreten waren.

Risikobewertung als Teil der Prophylaxe

Unnötig zu erwähnen, dass es sich mindestens um einen geschäftskritischen Imageschaden handelte. Was ist Unternehmen zu raten, die solche Fälle vermeiden möchten?

Einer der ersten Schritte ist die Integration des IoT-Cyber-Risikos in das Risiko-Register des Unternehmens und die Durchführung einer DICE-Bewertung für

alle geplanten Produkte und Services. DICE ist ist das Akronym für einen inhärenten Risiko-Bewertungs-Ansatz, den TÜV Rheinland entwickelt hat und der für „Dependency“ (Abhängigkeit), „Impact“ (Auswirkungen), „Complexity“ (Komplexität) und „Ecosystem“ (Ökosystem) steht. Entscheidend für die Bewertung eines Systems, Prozesses oder Gerätes gemäß der DICE-Kriterien ist, dass angemessene und kostengünstige Maßnahmen zur Risikobewältigung implementiert werden. Alle Produkte und Services sollten eine DICE-Bewertung durchlaufen, und zwar auf Basis eines strategischen Plans. Die Festlegung darauf, ab welchem Punkt Sicherheit zu einem wichtigen oder kritischen Faktor für Endverbraucher und die eigene Marke wird, ist auf jeden Fall essenziell.

Darüber hinaus können Prüfungen und Zertifizierung von IoT-Services einen qualifizierten Nachweis darüber leisten, dass Hersteller personenbezogene Daten ihrer Kunden gut schützen und für den Kunden transparent verarbeiten.

TÜV Rheinland etwa bietet ein Produkt- und ein Service-Zertifikat an, mit dem Produkthersteller sowie Systemanbieter zeigen können, dass ihr Angebot entsprechend den Anforderungen der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) geprüft wurde.

In den IoT-Prüfungen bewertet TÜV Rheinland u. a., inwieweit Prozesse und Maßnahmen implementiert sind, um Sicherheitsvorfällen vorzubeugen und gegebenenfalls angemessen reagieren zu können.

Dynamischer Entwicklung Rechnung tragen

Compliance allein macht ein Produkt noch nicht sicher. Erst wenn Hersteller die mit Cybersicherheit verbundenen Bedrohungen und Risiken monitoren und daraus entsprechende Konsequenzen ziehen, können sie sich auf ihre Produktinnovationen konzentrieren – in der Gewissheit, alle erforderlichen Maßnahmen ergriffen zu haben, die der dynamischen Entwicklung auch wirklich Rechnung tragen.

Mehr Infos über das DICE-System und eine Checkliste der wichtigsten Empfehlungen für Hersteller rund um die Cybersecurity von IoT-Geräten enthält das Whitepaper „Herausforderungen im Internet of Things (IoT)“ von TÜV Rheinland. Link zum Download: https://www.tuv.com/landingpage/de/c2f/meta-navigation/downloads/ oder https://goo.gl/A88pSr