Cyber-Security als Wettbewerbsvorteil bei IoT-Geräten

Qualifizierte Risiken

Das Internet of Things (IoT) oder auch Internet der Dinge erweist sich als Grundlage für neue und aufregende Geschäftsmodelle. Immer mehr Hersteller bieten Produkte oder Services, mit denen sich die Vorteile des Internets und des World Wide Webs umfassend nutzen lassen. Folgender Beitrag beschreibt den aktuellen Status Quo der Cyber-Security bei IoT-Geräten und gibt strategische Empfehlungen, wie sich Sicherheitsschwachstellen von IoT-Geräten so weit wie möglich verringern lassen.

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. Dadurch wird den Betroffenen der Umgang mit Diabetes etwas erleichtert. Allerdings hat so mancher Hersteller von Medizingeräten seine Geräte recht übereilt an das IoT angepasst, ohne die damit verbundenen Probleme rund um Cyber-Security zu beachten beziehungsweise sie zu lösen. Schwachstellen wie

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

sind da nur die Spitze des Eisbergs. 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 unautorisierter Dritter die Infusionspumpe unter seine Kontrolle bringen und die verabreichte Dosis verändern können. Konkrete Vorfälle waren glücklicherweise nicht bekannt. Vom Markt genommen wurde das Infusionssystem dennoch, weil auch noch andere Schwachstellen aufgetreten waren.

Ein schnelles Aus für ein Produkt gab es in der jüngsten Vergangenheit auch in Deutschland: 2017 wurde eine Spielzeugpuppe aufgrund von Sicherheitsbedenken verboten. Die My Friend Cayla-Puppe verwendete eine Spracherkennungstechnologie über einen Service mit Sitz in den USA. Die Daten aus den Tonaufnahmen erwie-

sen sich als ungesichert und konnten laut Endbenutzer-Lizenzvertrag an Dritte weitergeleitet werden. Bei einem anderen Vorfall waren 2017 zwei Millionen Sprachaufzeichnungen von Kindern, die von CloudPet-Stofftieren aufgenommen wurden, aufgrund einer unsicheren Datenbank zeitweise für jedermann online zugänglich.

Bei Sicherheitsvorfällen drohen Geräteherstellern inzwischen drastische Strafen, ganz zu schweigen von den Reputationsschäden. Was ist Unternehmen zu raten, die derlei vermeiden möchten? Auf jeden Fall Cyber-Security aktiv managen: Einer der ersten Schritte ist die Integration des IoT-Cyber-Risikos in das Risikoregister des Unternehmens und die Durchführung einer Risikobewertung für alle geplanten Produkte und Services, wie sie etwa der TÜV Rheinland mit DICE entwickelt hat. DICE steht für einen inhärenten Risikobewertungsansatz, der die Faktoren „Dependency" (Abhängigkeit), „Impact" (Auswirkungen), „Complexity" (Komplexität) und „Ecosystem" (Ökosystem) mit einbezieht. Entscheidend für die Bewertung eines Systems, Prozesses oder Gerätes gemäß der DICE-Kriterien ist, dass angemessene und kostengünstige Maßnahmen zur Risikobewältigung implementiert werden. Die Risikobewertung sollte einem strategischen Ansatz folgen: Die Qualifizierung, ab welchem Punkt Sicherheit zu einem wichtigen oder kritischen Faktor für Endverbraucher und die eigene Marke wird, ist auf jeden Fall vital.

Darüber hinaus können Prüfungen und Zertifizierungen von IoT-Services einen qualifizierten Nachweis darüber leisten, dass Hersteller personenbezogene Daten ihrer Kunden gut schützen und für den Kunden transparent verarbeiten. Hier gibt es Service-Zertifikate, mit denen Produkthersteller sowie Systemanbieter zeigen können, dass ihr Angebot entsprechend den Anforderungen der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) geprüft wurde. TÜV Rheinland etwa bewertet in seinen IoT-Prüfungen unter anderem, inwieweit Prozesse und Maßnahmen implementiert sind, um Sicherheitsvorfällen vorzubeugen und gegebenenfalls angemessen reagieren zu können.

Fazit: Compliance allein macht ein Produkt noch nicht sicher. Erst wenn Hersteller die mit Cyber-Sicherheit verbundenen Bedrohungen und Risiken überwachen 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. ■

NIGEL STANLEY / MARK CODERRE,
Experten für Cyber Security bei TÜV Rheinland