Vernetztes Spielzeug

Wenn Cyber Security zum kritischen Faktor wird

Bei Sicherheitsvorfällen, z. B. durch Cyber-Angriffe, drohen Herstellern vernetzter Geräte drastische Strafen. Nigel Stanley und Mark Coderre, Experten für Cyber Security bei TÜV Rheinland, geben strategische Empfehlungen, wie sich Sicherheitsschwachstellen von IoT-Geräten möglichst vermeiden lassen.

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 aufregende 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, mit denen sich die Vorteile des Internets und des World Wide Webs umfassend nutzen lassen. Bis 2020 gehen die Marktforscher von Gartner von mehr als 20,4 Mrd. vernetzter Geräte aus.

Medizingeräte sind ein gutes Beispiel dafür, dass das Leben von Patienten und Ärzten durch die Ausstattung mit IoT-Funktionalität verbessert werden kann. Allerdings hat so mancher Hersteller seine Geräte recht übereilt an das IoT angepasst, ohne die damit verbundenen Probleme rund um Cyber Security zu beachten bzw. sie zu lösen. Schwachstellen wie

- 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,
- 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. Eine der bekanntesten Vorfälle im Gesundheitswesen stammt aus 2015. Seinerzeit warnte die US-amerikanische Bundesbehörde für Arzneimittel und Medizinprodukte, Federal Drug Agency (FDA), vor dem Hospira Symbiq Infusion System. Über das Krankenhausnetzwerk hätte ein unautorisierter Dritter die Infusionspumpe unter seine Kontrolle bringen und die verabreichte Dosis verändern können. Konkrete Vorfälle waren nicht bekannt. Vom Markt genommen wurde das Symbiq Infusion System dennoch, weil auch noch andere Schwachstellen aufgetreten waren.

Rückrufaktion auf dem deutschen Markt

Ein schnelles Aus für ein Produkt gab es in in der jüngsten Vergangenheit auch auf dem deutschen Spielzeugmarkt: 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 erwiesen sich als ungesichert und

Wissen, wie sich Sicherheitsschwachstellen von IoT-Geräten verringern lassen: Mark Coderre (li.) und Nigel Stanley vom TÜV Rheinland.

konnten laut Endbenutzer-Lizenzvertrag an Dritte weitergeleitet werden. Das Produkt wurde auf Basis des US-amerikanischen Bundesgesetzes Espionage Act vom Markt genommen. Bei einem anderen Vorfall waren 2017 zwei Millionen Sprachaufzeichnungen von Kindern, die von Cloud-Pet-Stofftieren aufgenommen wurden, aufgrund einer unsicheren Datenbank zeitweise online für jedermann zugänglich.

Unnötig zu erwähnen, dass es sich stets mindestens um geschäftskritische Imageschäden 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 das Akronym für einen inhärenten Risiko-Bewertungs-Ansatz, den TÜV Rheinland entwickelt hat und der für „Dependancy“ (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 daher unbedingt eine DICE-Bewertung durchlaufen – und zwar auf Basis eines strategischen Plans. Die Qualifizierung, ab welchem Punkt Sicherheit zu einem wichtigen oder kritischen Faktor für Endverbraucher und die eigene Marke wird, ist auf jeden Fall vital.

Konsequenzen aus den Prüfungen ziehen

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, 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. Compliance allein macht ein Produkt noch nicht sicher. Erst wenn Hersteller die mit Cyber-Sicherheit verbundenen Bedrohungen monitoren und daraus 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 Cyber Security von IoT-Geräten enthält das Whitepaper unter dem Titel „Herausforderungen im Internet of Things (IoT)“ (unter www.tuv.com/c2f/downloads).