Sicherheitsbedarf von IoT-Anwendungen

Die Digitalisierung ist die Basis für das Wohlergehen unserer Informations- und Wissensgesellschaft. Denn diese eröffnet für alle Branchen und Unternehmensgrößen enorme Wachstumschancen und führt dazu, die Effizienz zu steigern und Kosten zu reduzieren. Zudem wird künftig der Wertschöpfungsanteil der IT in allen Produkten und Lösungen zunehmend größer.

Ein bedeutender Bereich der Digitalisierung ist das Internet of Things (IoT), bei dem physische Objekte (Dinge) mehr Intelligenz bekommen sowie über das Internet verknüpft werden und Daten austauschen. Prognosen zeigen, dass im Jahr 2025 weltweit bereits 75 Mrd. IoT-Geräte im Internet sind. Aus diesem Grund ist es notwendig, sich mit diesem Thema auseinanderzusetzen und vor allem aus unterschiedlichen Perspektiven der IT-Sicherheit und Vertrauenswürdigkeit zu diskutieren.

Einen ersten Überblick dazu bietet der Artikel „IoT – die unterschätzte Gefahr für IT-Sicherheit". Er legt die grundsätzliche Gefahr unsicherer IoT-Geräten bezüglich der Nutzung von DDoS-Angriffen auf die Internet-Infrastrukturen dar. Doch es bestehen bei Weitem mehr Angriffsvektoren – wie im Artikel „Die Sicherheitslage im IoT-Umfeld" beschrieben. Aber die Lage ist nicht hoffnungslos – es gibt bereits Lösungsansätze wie die Beiträge „Automotive Security mit der On-Board Telematics Platform (OTP)" und „Digitalisierung der industriellen Dinge" zeigen. Denn mithilfe von Virtualisierung und Hardware-Sicherheitsmodulen wie dem TPM kann zukünftig ein höherer Level an IT-Sicherheit im IoT-Bereich erreicht werden. Des Weiteren gehören dazu auch grundsätzliche Maßnahmen, etwa die Etablierung eines Europäischen Standards, gegen den die IoT-Systeme bezüglich deren Sicherheit getestet werden können, wie im Artikel „Die Sicherheitslage im IoT-Umfeld" dargestellt.

Doch IoT ist nicht nur ein Thema für die Industrie. Der Artikel „Chancen und Risiken von Smart Home" erklärt, welche Möglichkeiten eine smarte Umgebung eröffnet, aber setzt sich ebenso kritisch damit auseinander, welche Risiken dabei auftreten können. Dabei wird auch diskutiert, ob wir diese Anwendungen überhaupt nutzen wollen und was getan werden muss, damit eine grundsätzliche Akzeptanz in die digitale Zukunft geschaffen werden kann.

Tatsächlich spielt beim Thema IoT der Datenschutz eine wichtige Rolle. Die hier relevanten Aspekte werden in den Artikeln „Wann ist ein IoT-Gerät datenschutzrelevant?" und „Datenschutz im Internet der Dinge" beleuchtet und zudem erläutert, warum diese in den Anwendungen von Anfang an zu berücksichtigen sind.

Doch letztendlich müssen die Produkte und Dienste auch vom Nutzer akzeptiert werden. Warum Vertrauenswürdigkeit eine essentielle Voraussetzung für die Nutzung von innovativen Technologien, Anwendungen und Diensten wie IoT ist, beschreibt der Grundsatzartikel „Vertrauen – ein elementarer Aspekt der digitalen Zukunft". Denn nur ein transparentes, verantwortliches und vertrauenswürdiges Handeln von Unternehmen schafft langfristig Akzeptanz beim Kunden.

In einem weiteren Beitrag im Heft befasst sich Sven Braun mit „Kontrollen risikoreicher Anwendungen" im nichtöffentlichem Bereich.

Zum Schluss wünsche ich Ihnen viel Freude und interessante Erkenntnisse beim Studium der Beiträge dieser DuD-Ausgabe. Auch über ein Feedback würden wir uns sehr freuen.

Norbert Pohlmann