Das Netz der bewegten Dinge

Die Vernetzung der Dinge (Internet of Things oder kurz IoT) findet in vielen Bereichen statt, wie zum Beispiel der vernetzte Kühlschrank, der selbständig Lebensmittel bestellt, oder der Fernzugriff mittels Smartphone auf verschiedene Geräte, wie Überwachungskameras, Beleuchtung etc. Unlängst hat ein österreichischer Mobilfunkunternehmer in Kooperation mit einem Start-Up ein „smartes" Kuscheltier vorgestellt. Dieses ist mit Sensoren zur Temperatur-, Aktivitäts- und Atmungsmessung ausgestattet. Es ermöglicht den Eltern, somit den Vitalzustand des Kindes während des Schlafes zu überwachen[59]. Bei den genannten Beispielen handelt sich um statische Anwendungen des Internet of Things. Unter Netz der bewegten Dinge versteht man Geräte/Dinge, die vernetzt und zudem in irgendeiner Form in Bewegung sind, wie zum Beispiel Roboter oder (autonome) Fahrzeuge. Es handelt sich somit um ein eigenes Anwendungsfeld. In der Robotik könnte die Vernetzung z. B. über Cloud-Dienste zum Austausch gesammelter Daten, „Lernerfahrungen" bzw. Algorithmen genutzt werden. Interessante Anwendungsfelder für das Internet der bewegten Dinge ergeben sich vor allem im Bereich der Mobilität. Viele Neuwagen unterstützen bereits den SIM-Karten-Standard, Tendenz steigend. Das ermöglicht die Vernetzung der Fahrzeuge untereinander, aber auch zum Hersteller. Das ermöglicht einerseits Ferndiagnostik, Echtzeitnavigation und verschiedene Infotainment-Services. Weitere potentielle Vorteile ergeben sich über die Datensammlung des Mobilitätsverhaltens, welches für ein effizienteres Verkehrssystem genutzt werden könnte. Zugleich aber stellt sich die Frage, wie das Grundrecht auf informationelle Selbstbestimmung geschützt werden kann, vor allem Im Hinblick auf die Nutzung der Daten durch Dritte (Krieger-Lamina 2016). Die Vernetzung eröffnet zudem potentielle Einfallstore für HackerInnen, was gravierende Auswirkungen haben kann. 2015 haben zwei Hacker auf diese Gefahr hingewiesen. Sie haben es geschafft einen zwei Tonnen schweren SUV zu kapern. Es war ihnen somit möglich das Fahrzeug gänzlich zu steuern, angefangen bei der Klimaanlage hin zu Lenkbewegungen und sogar das Bremsen war möglich.[60] 2016 wiesen Hacker auf eine Sicherheitslücke eines Elektroautoherstellers hin. Sie konnten aus einer Entfernung von 19 km auf das Fahrzeug zugreifen. Nach einem Update wurde die Sicherheitslücke beseitigt[61]. Auch auf Österreichs Straßen sind bereits Fahrzeuge unterwegs, die vernetzt sind. Mit den genannten Beispielen kristallisieren sich neue Handlungsfelder im Bereich der IT-Sicherheit heraus. Die Relevanz ist auch seitens des VerbraucherInnenschutzes gegeben.

---

59 sticklett.com.

60 wired.com/video/hackers-wireless-jeep-attack-stranded-me-on-a-highway.

61 zdnet.de/88279165/tesla-model-s-sicherheitsforscher-hacken-elektroauto-aus-der-ferne/?inf_by=5a03063e681db8cf478b467d.

Zitierte Quellen

Krieger-Lamina, J., 2016, *Vernetzte Automobile. Datensammeln beim Fahren – von Assistenzsystemen zu autonomen Fahrzeugen. Endbericht*, 2016-08-31, Wien: Institut für Technikfolgen-Abschätzung (ITA): epub.oeaw.ac.at/ita/ita-projektberichte/2016-02.pdf.

(LC)