Institut für Sicherungssysteme iSS

WITTE AUTOMOTIVE

# Risikomodellierung digital vernetzter Zugangsmöglichkeiten am Beispiel Mobile-Access-Systeme für Fahrzeuge

Die zunehmende Digitalisierung stellt die Automobilbranche vor allem durch neue Ziele in der Prozessautomatisierung vor große Herausforderungen und disruptive Veränderungen. Neben autonomem Fahren beschäftigt die Unternehmen insbesondere auch die digitalisierte Regelung des physischen und logistischen Zugangs zu Fahrzeugen. Bereits existierende Strategien und Organisationsstrukturen müssen aufgrund dessen nicht nur hinterfragt, sondern ggf. auch vollständig umgedacht werden.

Die Vernetzung durch den Einsatz von IoT-Devices in modernen Systemen verändert sowohl das Alltags- als auch Geschäftsleben des Menschen. Der digitale Support wird unter anderem durch die Multifunktionalität von Smartphones beschleunigt. Neueste Entwicklungen automobiler Sicherungssysteme verfolgen den Ansatz, dass ein über eine App des Smartphones generierter Code für das Öffnen des Fahrzeugs die Funktion des Fahrzeugschlüssels als Zugangsmittel in neuen Use-Cases ersetzen kann. Das Potenzial mobiler Anwendungen ist zum einen immens und zum andern ein Impulsgeber für die technologische Akzeptanz der Digitalisierung in der heutigen Gesellschaft, wobei insbesondere standardisierte Kommunikationsschnittstellen wie das etablierte Bluetooth den Gebrauch von Smartphones und Wearables alltags- und geschäftstauglich machen. Digitale Zugangssysteme für das Automobil führen zu einer Revolution des Produktangebots. Neben modernen Car-Sharing und Flottenmanagement-Systemen wird die flexible private Nutzung von Mobile Access zunehmend nachgefragt, wobei über das Smartphone Zugangsberechtigungen an Dritte vergeben werden können.

Die wachsende Marktdurchdringung von IoT und Industrie 4.0 bringt neue Chancen und Geschäftsmodelle, aber auch neue Gefahren mit sich. Zunehmende digitale Vernetzung erfordert die Berücksichtigung von IT-Security und Datenschutz in immer mehr Lebensbereichen. Sicherungssysteme, die physische Sicherungsfunktionen erfüllen, verbinden durch diese Entwicklung die Disziplinen *Physical Security* und *IT-Security* bzw. auch *Embedded Security.* Gleichzeitig ist eine erhöhte Sensibilität für das Thema Sicherheit zu beobachten, was auch auf eine subjektiv empfundene Zunahme globaler Bedrohungen zurückgeführt werden kann.

Klassische Risikobetrachtungen, die neue Chancen und Geschäftsmodelle den Gefahren der Digitalisierung gegenüberstellen, beschränken sich meist auf die Rolle der IT-Sicherheit und des Datenschutzes in den betroffenen Unternehmen und Geschäftsprozessen (siehe z.B. [Lün]). Sicherheitstechnologien und hier insbesondere Sicherungssysteme bringen aber zusätzliche, z.B. auch technologieimmanente und soziotechnische Risikofaktoren mit sich, die bei der Implementierung neuer Produkte und Geschäftsmodelle betrachtet werden sollten. So bedingt z.B. die durchaus derzeit noch zunehmende digitale Oligopolisierung einen relativ großen Einfluss weniger Akteure (z.B. Apple) auf die Kompatibilität und damit Zukunftsfähigkeit von Sicherheitstechnologien. Subjektive Kundenperspektiven, die die Sicherheitswahrnehmung betreffen, sind darüber hinaus ein entscheidender soziotechnischer Faktor für die Akzeptanz.

Im Rahmen eines Promotionsvorhabens sollen die entscheidenden Risikofaktoren eines vernetzten Sicherungssystems identifiziert und unter Berücksichtigung sowohl der Produktperformance (IT- und Physical Security) als auch technologieimmanenter und soziotechnischer Faktoren zu einem Gesamtmodell entwickelt werden, das einen wichtigen Beitrag zur Bewertung innovativer Sicherheitsprodukte und Geschäftsmodelle leisten kann. Die Risikobewertung soll am Beispiel Mobile-Access für Fahrzeuge (Flinkey-System der Firma WITTE Digital) durchgeführt werden.

[Lün] Lünendonk - Trendstudie 2016 „IT - Security und Risk Management 2016 ”