IT-SECURITY IST VERTRAUENSSACHE!

Die Datensicherheit gestaltet sich sowohl für Privatpersonen wie auch für Unternehmen deutlich schwerer als gedacht. Viele Kunden wissen nicht, welchen Herstellern und Konzernen sie Zugang zu ihren sensiblen Daten geben sollen.

Allein in den letzten zwei Jahren war jedes zweite Unternehmen in Deutschland von Hackerangriffen betroffen. Das gab das für Fragen rund um Cybersecurity zuständige Bundesamt für Sicherheit in der Informationstechnik (BSI) bekannt. Durch Attacken wie WannaCry und Petya konnten Internet-Kriminelle tagelang die Produktion in Unternehmen lahmlegen. Große Konzerne verzeichnen mittlerweile tausende solcher Angriffe pro Tag. Kommt nur ein einziger davon durch, drohen Schäden in Millionenhöhe. Hinzu kommt der immaterielle Schaden. Wie nach realen Einbrüchen sind die Betroffenen verunsichert. Welche Daten und Rechner nach einem Angriff noch sicher sind, ist unklar.

Friedhelm Pickhard
Vorsitzender der Geschäftsführung von ETAS.

friedhelm.pickhard@etas.com

Maßnahmen gegen das Aufhebeln von Türen und Fenstern sind allgemein verständlich. Im Gegensatz dazu ist IT-Security für Laien meist ein Buch mit sieben Siegeln. Sie können weder die Methoden der Hacker noch die Gegenmaßnahmen nachvollziehen. Letztlich sind IT-Nutzer auf das Know-how von Security-Spezialisten angewiesen. Eine Zielscheibe für Hacker können auch moderne Fahrzeuge werden. Sie sind ein Teil der vernetzten Welt und somit genauso angreifbar wie Rechner. Mit der Einbindung des Internets in Autos ist auch deren IT angreifbar. Wenn Cyberkriminelle Funktionen in Fahrzeugen manipulieren, hat das weitreichende Folgen. Die Sicherheit von Menschen wird gefährdet und die wirtschaftliche Stabilität des betroffenen Fahrzeugherstellers kann davon geschädigt werden. Schließlich können Kunden sich nicht mehr sicher sein, welchem Hersteller sie noch vertrauen.

Mit der IT-Security im Fahrzeug steht und fällt der Erfolg von Geschäftsmodellen rund um vernetzte Services. Sie ist essentiell für die Reputation der gesamten Branche. Dafür müssen die Hersteller die Sicherheit der Kundendaten in den Fahrzeugen garantieren können. Deshalb suchen OEMs und Zulieferer den Schulterschluss mit Security-Experten, um im Wettlauf gegen die Hacker die Nase vorn zu behalten. Hier sind holistische Ansätze, also solche, die das ganze System betrachten, gefragt: IT-Security beginnt mit den Planungen vor der Entwicklung eines Modells. Sie sichert nicht nur sämtliche Produktionsabläufe ab, sondern auch den Fahrzeugbetrieb in Kundenhand. Erst nachdem die kryptografischen Schlüssel aus dem Fahrzeug gesichert wurden, endet die IT-Security mit der Verschrottung.

Security-Partner haben Zugriff auf geschützte Bereiche und sensible Daten. Fahrzeughersteller und Zulieferer müssen sich demnach fragen, wen sie so tief in ihre Strukturen und Prozesse blicken lassen. Mancher IT-Security-Anbieter hat sich zuletzt zu seinen Wurzeln in Geheimdienstkreisen bekannt und teils sogar damit geworben. Andere rekrutieren Mitarbeiter dort. Angesichts des Mangels an IT-Spezialisten ist das nachvollziehbar, jedoch bleiben die Akteure undurchschaubar. Ob solche Partner keine eigene Agenda verfolgen und sensible Daten in ihren Händen sicher sind, kann nicht gewährleistet werden. IT-Security ist Vertrauenssache! Gerade in diesem Bereich sollten Partnerschaften auf gemeinsamen Werten aufbauen. OEM und Zulieferer tun gut daran, ihre Partner gründlich zu prüfen. Denn nicht nur IT-Netzwerke von Fahrzeugen bieten Angriffsfläche, sondern auch die Organisationen ihrer Hersteller.