Spies: USA: Gesetz gegen gehackte Autos: Spy Car Act	ZD-Aktuell 2015, 04153

USA: Gesetz gegen gehackte Autos: Spy Car Act

Dr. Axel Spies ist Rechtsanwalt bei Morgan Lewis & Bockius in Washington DC und Mitherausgeber der ZD.

Aktuell wird in der deutschen und in der amerikanischen Presse breit berichtet, dass es Hackern gelungen ist, sich in die Software eines Jeep Cherokee einzuklinken und während der Fahrt u. a. dessen Bremsen und Lenkung zu manipulieren. Dies wirft Fragen nach der Sicherheit von Fahrzeugsystemen insgesamt auf und ruft den Gesetzgeber auf den Plan. Die Probleme betreffen einen Teilbereich des Internet of Things.

Senator *Ed Markey* (D-Mass), der seit vielen Jahren besonders für mehr Datenschutz/Privacy in den USA kämpft, hat deshalb zusammen mit seinem Amtskollegen *Blumenthal* am 21.7.2015 einen Gesetzesentwurf vorgelegt. Ziel des geplanten Gesetzes, das sich selbst als „Security and Privacy in Your Car Act of 2015“ oder kurz als SPY Car Act of 2015 bezeichnet, ist es, den Verbraucher in Bezug auf sein Fahrzeug vor Sicherheitsrisiken und Verletzungen der Privatsphäre zu schützen.

Der SPY Car Act gibt den Herstellern von Fahrzeugen gewisse „Cybersecurity Standards“ für Betriebssoftware, auf die unautorisierte Fremdzugriffe möglich oder zumindest denkbar sind, vor, die sie einhalten müssen. So müssen die Fahrzeughersteller ihre Systeme z. B. hinsichtlich aller Zugriffsstellen umfassend vor Hackerangriffen absichern. Der von den Herstellern zu gewährleistende Test-Standard ist hoch: „The measures … shall be evaluated for security vulnerabilities following best security practices, including appropriate applications of techniques such as penetration testing.“ Zudem soll, für den Fall eines erfolgreichen Hacker-Angriffs, zumindest die kritische Software, die die Steuerung des Autos bedient, von der restlichen Betriebssoftware des Wagens getrennt werden, um die Sicherheit im Straßenverkehr zu gewährleisten. Die Software des Autos soll daneben auch die während des Betriebs gesammelten Daten aufzeichnen und speichern, um das System dauerhaft auf Sicherheitslücken überprüfen zu können.

Weiter muss jedes Auto, das zukünftig in den Anwendungsbereich des SPY Car Act fällt, über eine „Cyber-Anzeige“, ein sog. Cyber Dashboard, verfügen, das den Verbraucher über die vorinstallierten Schutz- und Abwehrmaßnahmen des Systems gegen Hackerangriffe und die Gewährleistung der Datensicherheit informiert. Zudem muss die Datenaufzeichnung durch das Fahrzeugsystem transparent erfolgen und dem Verbraucher Zugriff auf die gespeicherten Daten ermöglichen. Ein vergleichbarer Ansatz eines Cyber Dashboard und einer transparenten Datenaufzeichnung wird in Deutschland u. a. für zukünftige fahrerlose Fahrzeuge vorgeschlagen (vgl. zuletzt *Sörup/Marquardt*, ZD 2015, 310 ff.)

Insgesamt bleibt der Entwuf zum SPY Car Act an vielen Stellen sehr unbestimmt und verzichtet auf genaue Definitonen von verwendeten Rechtsbegriffen. So wird von den Herstellern verlangt, die „besten Sicherheitssysteme“ zu installieren, „angemessene Maßnahmen“ zu treffen, um Angriffe auf das Fahrzeug zu verhindern, und das Fahrzeug mit der „Fähigkeit, Angriffe umgehend zu ermitteln, zu melden und zu stoppen“, auszustatten. Der Fahrer soll die Option bekommen, die Sammlung von Fahrzeugdaten zu

verhindern oder zu beenden, womit wohl ein Opt-out gemeint ist. Ob damit auch Standortdaten der Fahrzeuginsassen gemeint sind, ist nicht klar.

Entsprechende Sicherungsmaßnahmen für die eigene Betriebssoftware zu treffen, dürfte schon im Interesse der Hersteller liegen. Die angedrohten Strafen (US-$ 5.000,- pro Einzelfall) bei Verletzung der Pflichten aus dem SPY Car Act könnten sich allerdings schnell summieren, abgesehen von der Möglichkeit des Schadensersatzes in den USA im Wege der Zivilklage. Ob und wann der Spy Car Act im *Senat* beraten wird, ist noch offen. Da sich bislang noch kein Unterstützer aus den Reihen der Republikanischen Partei gefunden hat, könnte das Projekt in den Ausschüssen stecken bleiben. Selbst wenn es dazu kommt, dürfte die Umsetzung durch die *Federal Trade Commission (FTC)* und die *National Highway Traffic Safety Administration (NHTSA)* geraume Zeit in Anspruch nehmen. Die Untersuchungen könnten einige Zeit in Anspruch nehmen. Es gibt z. B. das schwer lösbare Problem von WLANs, die mit Fahrzeugen kommunizieren. Diese könnten gehackt werden und dann die vorbeifahrenden Fahrzeuge mit Malware infizieren (sog. Zombie-Problem). Erpressungen wäre damit Tür und Tor geöffnet.

Die Sicherheitsorgane und die Polizeibehörden haben sich noch nicht zu der Gesetzesmaßnahme geäußert. Vermutlich besteht ein lebhaftes Interesse dieser Behörden, ein Fahrzeug von außen durch einen Software-Eingriff (möglicherweise direkt vom Polizeiauto aus) lahmlegen zu können. Die in US-Filmen und -Serien so beliebten Verfolgungsfahrten dürften dann der Vergangenheit angehören.

Weiterführende Links

Vgl. auch *Sörup/Marquardt*, ZD 2015, 310; *Lüdemann*, ZD 2015, 247 und *ÖBVwG* ZD 2015, 318 m. Anm. *Trieb*