ten zu können. Hierbei sollen vor der Stilllegung der Computer personenbezogene Daten extrahiert werden können.

Die grundlegende Beurteilung der Hintergründe von Terrorismus- und Kriminalitätsbekämpfung ist eine langfristige Aufgabe. Deren Umsetzung in technische und rechtliche Maßnahmen muss aber darüber hinaus allgemeinen Grundsätzen und rechtlichen Anforderungen der IT-Sicherheit, des Datenschutzes und der Wahrung der Privatsphäre Genüge tun. Die derzeit vorliegenden Dokumente beinhalten einen Richtervorbehalt, die Maßnahmen sind damit im Rahmen der Gewaltenteilung formal strengen Beschränkungen unterworfen. Damit dieser Richtervorbehalt jegliche nicht genehmigten Zugriff verlässlich verhindert, ist von klaren Voraussetzungen und Annahmen auszugehen: Die Annahme, dass eine Schwachstelle nur von einer staatlichen Stelle entdeckt und anschließend ausgenutzt wird, ist falsch. Gleiches gilt für die Annahme, dass Backdoors nicht entdeckt und geöffnet werden.

Folgerichtig ist jede nicht behobene Schwachstelle eine Gefährdung für Wirtschaft und Gesellschaft. Die Erfahrung zeigt, dass bei staatliche Stellen bekannte und genutzte Schwachstellen nur eine geringe Halbwertszeit bis zu deren Offenlegung und deren unerwünschte Nutzung durch Dritte haben. Der Wikileaks Vault7 Dump als nur ein sehr prominenter Leak in einer Reihe von Veröffentlichungen beinhaltet staatliche genutzte Schwachstellen, die oft noch langfristig ausnutzbar sind. Die Ransomware-Attacke WannaCry basierte auf einer in Windows erkannten Schwachstelle, die von der NSA aktiv fünf Jahre ausgenutzt wurde und deren Details erst nach Diebstahl von Informationen über die zugrundeliegende Schwachstelle und damit offensichtlich zu spät an Microsoft übermittelt wurden.

Die Entfernung solcher Sicherheitsrisiken zum Schutz der Bürger auch bei allgemeinem Bekanntwerden solcher Gefahren hingegen ist schwierig. Oft ist sie weder technisch noch organisatorisch machbar, da die Nutzungsdauer (und damit die Ausnutzungsdauer von bekannt gewordenen, gewollten wie ungewollten Sicherheitslücken) deutlich länger als der Wartungszeitraum ist, in dem Hersteller Sicherheitsupdates, neue Firmware oder Systemversionen bereitstellen. Nicht zuletzt ist auch der Zugang zu diesen Systemen aus vielen Gründen nicht direkt oder nur mit hohem Aufwand möglich.

Da die geplante Regelung die volle Bandbreite von Geräten umfasst, die der private, aber nicht zuletzt auch der kommerzielle oder staatliche Anwender in praktisch allen Lebens- und Arbeitsbereichen nutzt, sind auch praktisch alle von diesen Systemen verarbeiteten Daten in Gefahr.

Zu betrachten sind exemplarisch nur etwa die Informationen, die heute einem typischen Smartphone anvertraut werden, ergänzt um die kleinen und großen Geheimnisse, die ein intelligenter Sprachassistent, das vernetzte Auto und das Smart Home (inklusive der Überwachungskameras) über uns wissen. Eine Beurteilung der oben beschriebenen Initiative mit Blick auf eine Ausspähung dieser Informationen durch unerwünschte Dritte jenseits staatlicher Aktivitäten sollte damit grundlegend auf Basis der Grundsätze, Erkenntnisse und Best Practices von IT-Sicherheit, Compliance und dem Schutz der Privatsphäre der betroffenen Personen erfolgen.

Matthias Reinwarth

1.3.4 Telematik

Dirk Schlimm von Geotab zur Sicherheit von Telematikplattformen

„Vernetzte Autos eröffnen zahlreiche Vorteile wie erhöhte Sicherheit, größere Effizienz und Komfort. Flottenmanager (z.B. Betreiber von Autovermietung, Leasinggesellschaften oder Logistikfirmen) haben anhand unzähliger Daten wie GPS, Benzinverbrauch und Fahrverhalten den Status ihrer Autos immer im Blick. Diese Daten werden auf einem Standard Diagnose-Interface, dem On-Board-Diagnostic (OBD) Port gesammelt und bereitgestellt. Dieser ist somit ein wichtiger Bestandteil des vernetzten Fahrens.

Andererseits führt der Anschluss von Fahrzeugen an das Internet zu industrieweiten Diskussionen über den Aspekt der Cyber-Sicherheit. Betreiber von Telematik-Plattformen müssen bei deren Konfiguration dem Sicherheitsaspekt eine hohe Priorität einräumen, um ihren Kunden Datenschutz gewährleisten zu können. Hierzu empfiehlt es sich, Industrierichtlinien und Standards (wie SAE, ISO, IEEE oder ASAM) einzubeziehen. Des Weiteren müssen die Datenschutzmaßnahmen der lokalen Gesetzgebung entsprechen und die Daten der Fahrer ausreichend schützen.

Flottenmanager sind einerseits auf den direkten Zugriff auf die operativen Daten ihrer Fahrzeuge angewiesen, andererseits müssen diese stets sicher sein. Daher sollten sie Datenplattformen nutzen können, die genau die Daten erhebt, die sie auch brauchen und persönliche Daten der Fahrer auf einem Minimum halten. Außerdem empfiehlt sich ein Sicherheitsprogramm mit „Best of Breed“-Lösungen, welche für die einzelnen Bereiche die für sie besten Lösungen beinhalten. Denn datengetriebene Mobilität ist nicht möglich, wenn die Sicherheit der Daten nicht gewährleistet ist.“

Dirk Schlimm

Dirk Schlimm,
Executive Vice
President, Geotab
Advisory Boards