tieren – nicht mehr den schnellsten, technisch und ökonomisch besten Weg selbst suchen dürfen, sondern sich vielmehr an nationalen Grenzen zu orientieren hätten, steht im grundsätzlichen Widerspruch zu den fundamentalen Prinzipien des Internets, für deren Erhaltung und Fortentwicklung die Internet Society weltweit kämpft. Denn die Prinzipien der Offenheit, Transparenz und Neutralität sind es, wegen denen das Internet in seiner 45-jähriger Geschichte seine einzigartige gesellschaftliche und wirtschaftliche Bedeutung erlangen konnte. Vorschläge, die eine Re-Territorialisierung der Strukturen des Netzes und damit seine „Balkanisierung" erzwingen wollen, würden dagegen das Ende eines freien Internets einleiten und so zugleich auch die gesellschaftliche Fortentwicklung einer offenen, freien und demokratischen Gesellschaft behindern.

In die gleiche problematische Kategorie fallen unseres Erachtens Vorschläge, mit denen etwa Providern der Betrieb von Peering-Knoten untersagt werden soll. Ebenso, wenn der Grenzen von Staaten überschreitende Datenverkehr im Internet dadurch beschränkt werden soll, dass Daten verarbeitenden Unternehmen aus dem Ausland eine Residenzpflicht innerhalb der EU auferlegt, die Verarbeitung von Daten von EU-Bürgern ansonsten verboten wird, obwohl diese damit einverstanden sind. Oder gar Private zu Maßnahmen verpflichtet werden sollen, die sie gegenüber dem Staat, in dem sie niedergelassen sind, weder technisch, noch rechtlich erfüllen können.

Egal ob solche Vorschläge aus geschäftlichem Kalkül, einer offensichtlichen Konzept- und Hilflosigkeit gegenüber einer fortschreitenden Globalisierung oder mit Blick auf berechtigte Ziele der Datensicherheit oder des Datenschutzes gemacht werden, so sind es dennoch nach Überzeugung von ISOC.DE untaugliche Instrumente: Sie dienen im Ergebnis nicht dem Schutz der Freiheit der Menschen im Internet, sondern können vielmehr die Freiheit, die sie zu schützen vorgeben, letztlich nur beschränken, wenn nicht sogar beseitigen; ohne aber den Schutz der Menschen damit tatsächlich erhöhen zu können. In der aktuellen Diskussion um unzulässige Eingriffe staatlicher Nachrichtendienste in bürgerliche Freiheiten, sind es nämlich vorrangig Staaten, die zu einem anderen Verhalten finden und dazu mit Mitteln der Politik und des (Völker-) Rechts angehalten werden müssen. Politik, die um mehr Datenschutz und Datensicherheit ihrer Bürger im Verhältnis zu anderen Staaten besorgt ist, muss sich vorrangig politisch mit diesen Staaten auseinandersetzen.

Dagegen ist es weder das Internet in seiner grundlegenden Struktur, noch sind es die User oder andere privaten Stakeholder – auch nicht die Anbieter von Diensten oder Infrastrukturen des Internets – die für das problematische Handeln staatlicher Dienste verantwortlich wären. Auch wären sie gar nicht in der Lage, sich gegen staatliches Handeln auf dem Territorium eines Landes gegen das dortige Recht zur Wehr zu setzen. Firmen und Bürger im Internet zu Handlungen verpflichten zu wollen, die eigentlich Staaten betreffen und auch nur von ihnen zu erfüllen wären, sind daher aus unserer Sicht untaugliche Mittel. Aus diesem Grunde appelliert ISOC.DE sowohl im Hinblick auf die aktuellen Verhandlungen zwischen den Parteien einer künftigen Regierungskoalition, als auch mit Blick auf die laufenden Diskussionen der EU und dort insbesondere die geplante EU-Datenschutzgrundverordnung, bei der Verfolgung legitimer Ziele die tatsächliche Wirksamkeit und Folgen von Instrumenten sorgfältig abzuwägen, um unerwünschte Folgen zu vermeiden, die weder dem Bürger, noch seiner Freiheit und dem Internet dienlich sein können.

ISO/TS-Zertifizierung für SIM-Kartenlösung im Automobilbereich

Giesecke & Devrient (G&D) hat für die SkySIM®Argo in-car, die speziell für den Einsatz in Kraftfahrzeugen entwickelt wurde, die Zertifizierung nach der internationalen Norm ISO/TS 16949 erhalten. Gegenstand der umfangreichen Qualitätsprüfungen waren die entsprechenden Abläufe und Prozesse in den G&D-Kartenproduktionsstandorten im slowakischen Nitra und in München. Mit dieser Zertifizierung erfüllt G&D eine wesentliche Anforderung, welche die internationale Automobilindustrie an ihre Lieferanten stellt. Als Herzstück für automobile Vernetzungslösungen zeichnet sich die SkySIM Argo in-car nicht nur durch ihre besonders robuste Bauart aus. Sie unterstützt zudem die innovativen Subscription- und Life Cycle-Managementlösungen, die Giesecke & Devrient für seine Kartenlösungen bereithält.

Mit der Zertifizierung nach der Norm ISO/TS 16949 hat Giesecke & Devrient eine wichtige Hürde genommen, um ein erfolgreicher Zulieferer der internationalen Automobilindustrie zu werden. Diese auch als „Automobilstandard" bekannte ISO/TS-Norm fasst die speziellen Anforderungen der Automobilindustrie zusammen und soll sicherstellen, dass entsprechende Lieferanten einen sehr hohen Qualitätsstandard erfüllen. Die offizielle Überreichung des Zertifikats an G&D wird im Februar 2014 erfolgen.

Bei der SkySIM Argo in-car handelt es sich um ein Produkt aus dem M2M-Portfolio von Giesecke & Devrient. Diese SIM wurde speziell für den integrierten Einsatz in Kraftfahrzeugen entwickelt und ist nach AEC-Q100-Standard des AEC (Automotive Electronics Council) qualifiziert.

Die SkySIM Argo in-car arbeitet im Temperaturbereich von -40° bis +105° Celsius und zeichnet sich durch eine besonders hohe mechanische Robustheit aus.

Die SkySIM Argo in-car ist für die Verwendung neuester Netztechnologien wie 3G und 4G/LTE ausgelegt. Zudem nutzt das Produkt die Leistungen der aktuellen SIM-Karten-Betriebssysteme von G&D und erfüllt höchste Sicherheitsanforderungen. Die SIM-Karte unterstützt die innovativen Subscription-Management-Lösungen und das Life-Cycle-Management von G&D, so dass alle Voraussetzungen für eine zukunftssichere Langzeitverwendung in Fahrzeugen erfüllt sind.

T-Systems baut Sicherheitsportfolio zusammen mit RSA weiter aus

T-Systems und RSA, die Sicherheitssparte von EMC, bündeln im Kampf gegen Cyberangriffe ihre Kräfte. Mit der neuen Cybersecurity-Partnerschaft erweitert die Telekom-Tochter ihr eigenes Sicherheitsportfolio und kann Großkunden weitreichende Sicherheitslösungen bieten: von der Beratung über die Analyse bis hin zu dynamischem Schutz vor Angriffen. Ziel ist es, Cyberangriffe zielgerichtet und deutlich früher zu erkennen. Die Kombination aus moderner IT-Sicherheitstechnik, Expertenwissen und Zugriff auf Datenquellen wie konzerneigene Frühwarnsysteme ermöglicht den Aufbau neuer Sicherheitssysteme für Konzerne.

Die Cybersecurity-Partnerschaft mit RSA ist ein Baustein beim Aufbau der Business Unit Cyber Security. Die neue Geschäftseinheit bündelt ICT-Kompetenz und Sicherheits-Know-how des Te-