Zeitschrift für Datenschutz – ZD
www.zd-beck.de

Chefredakteurin
Anke Zimmer-Helfrich

Redaktion:
Marianne Gerstmeyr
Katharina Losso

Herausgeber:
RA Prof. Dr. Jochen Schneider
Prof. Dr. Thomas Hoeren
Prof. Dr. Martin Selmayr
RA Dr. Axel Spies
RA Tim Wybitul

Wissenschaftsbeirat:
Isabell Conrad
Dr. Oliver Draf
Dr. Stefan Hanloser
Dr. Helmut Hoffmann
Prof. Dr. Gerrit Hornung
Prof. Dr. Jacob Joussen
Thomas Kranig
Dr. Thomas Petri
PD Dr. Andreas Popp
Prof. Dr. Alexander Roßnagel
Dr. Christian Schröder
Dr. Jyn Schultze-Melling
Prof. Paul M. Schwartz
Thorsten Sörup
Prof. Dr. Jürgen Taeger
Florian Thoma
Prof. Dr. Marie-Theres Tinnefeld

Axel Spies

Europa: Wer hat Angst vor dem US-Patriot Act?

ZD-Aktuell 2012, 03062

Die „European Cloud" ist für diverse Anbieter von Cloud-Dienstleistungen in Europa ein gutes Verkaufsargument. Die bei ihnen abgespeicherten personenbezogenen Daten, so heißt es, würden den EU-Raum nicht verlassen und könnten deshalb von US-Regierungsstellen nach dem US-Patriot Act nicht gespeichert werden. Die Vertreter der US-Cloud-Anbieter beklagen sich über diese aus ihrer Sicht unfaire Vermarktungsstratgie zu Gunsten der European Cloud.

So forderte die *Information Technology and Innovation Foundation* am 23.7.2012 anlässlich einer gut besuchten Anhörung zu Cloud Computing im *US-Senat* Taten von der *US-Regierung* gegen die aus ihrer Sicht unfairen Anwürfe aus der EU gegen US-Cloud-Anbieter: „Strong U.S. leadership is needed to combat trade practices that other countries are using to block foreign competitors." Der Vertreter der *Business Software Alliance* (*BSA*) legte in der Anhörung wie folgt nach: „Far too often they would do so by throwing up protectionist barriers aimed to hurt international cloud providers and by adopting policies that would chop the cloud into country-sized pieces."

Der US-Patriot Act hat schon häufiger Anlass zu teils schriller Polemik in Europa gegeben. Schon der martialische Untertitel des Gesetzes wirkt auf viele Europäer abschreckend: „Uniting and Strengthening America by Providing Approriate Tools Required to Intercept and Obstruct Terrorism Act of 2001." Das Ziel des Gesetzes ist, nach der Katastrophe von 9/11 der *US-Regierung* vereinfachte Möglichkeiten zu geben, Zugang zu Telefon, E-Mail und anderen elektronischen Datenträgern zu erhalten, um die nationale Sicherheit bei der Terroristenbekämpfung zu schützen. Von der Befugnis wird praktisch regelmäßig Gebrauch gemacht. *Gordon Frazer*, der Geschäftsführer von *Microsoft UK*, hatte am 28.6.2011 für einige Aufregung in Europa mit seiner Bemerkung gesorgt, er könne nicht garantieren, dass die auf Microsoft-Servern gespeicherten Daten, wo immer sie sich befinden, nicht in die Hände der *US-Regierung* gelangen: *Microsoft* sei als US-Gesellschaft an US-Recht gebunden – gleich wo sich die Daten befinden. Besonders kritisch scheinen eine Reihe von Mitgliedern des *EU-Parlaments*, angeführt von der niederländischen Abgeordneten *Sophie in 't Veld*, gegen den Patriot Act eingestellt zu sein.

Im Prinzip nichts Neues

Der US-Patriot Act ist nicht das erste US-Gesetz, das den US-Behörden erlaubt, Zugang zu Daten zu erhalten, die in einer Cloud gespeichert sind. Diese Möglichkeit gewährte schon der Foreign Intelligence Surveillance Act (FISA) aus dem Jahre 1978, auf dem der Patriot Act basiert. FISA sah schon vor dem Patriot Act vor, dass die Sicherheitsbehörden mittels einer Anordnung eines Sondergerichts (*FISA Court*) eine sog. FISA-Order erhalten konnten, um an bestimmte Dokumente zu gelangen. Neu war, dass durch Titel II des Patriot Act diese Befugnisse auf fast alle denkbaren Beweisstücke zur Terrorismusbekämpfung ausgedehnt wurden. Außerdem enthält Sec. 215 des Patriot Act eine sog. Gag-Provision, sodass der Empfänger der FISA-Order über die Order und ihren Inhalt umfänglich schweigen muss. Ein Anbieter von Cloud-Dienstleistungen ist demnach nicht befugt, seine Kunden zu unterrichten, dass das *FBI* bestimmte Daten nach dem Patriot Act angefordert hat.

In der Praxis spielen die FISA-Orders eine geringe Rolle. Weitaus wichtiger als die FISA-Orders sind die National Security Letters (NSLs) – Anordnungen der Beschlagnahme von bestimmten Dokumenten direkt durch die Behörde (*FBI*, *CIA* etc.) – ohne die vorherige Einschaltung eines Gerichts. Auch die NSLs sind im Prinzip nicht neu und wurden schon vor dem Patriot Act z.B. bei der Prüfung der Zuverlässigkeit von US-Personal (Background Check) genutzt. Titel V des Patriot Act hat den Anwendungsbereich der NSL allerdings erheblich ausgeweitet. Für die Anbieter von elektronischer Kommunikation ist die relevante Vorschrift 18 U.S.C. § 2709.

Es genügt nach diesen Vorschriften, dass die angeforderten Daten relevant für die Aufdeckung von internationalem Terrorismus oder ausländischer Spionage sind und der Chef des *FBI Field Office* die Not-

wendigkeit des NSL zertifiziert. Dementsprechend ist der Gebrauch der NSLs in den USA stark angestiegen: Nach einem Schreiben des *US-Justizministeriums* an den *US-Kongress* v. 29.4.2011 zu urteilen, soll das *FBI* über 24.000 NSLs im Jahr 2010 verschickt haben. Auch für die NSLs gilt das Schweigegebot (Gag-Order). 2006 hat der *US-Kongress* im Reauthorization Act eine Bestimmung in den Patriot Act eingefügt, dass gegen die NSLs im Prinzip der Rechtsweg offen steht und diese Möglichkeit dem Empfänger auch mitzuteilen ist. Auch ist der Umfang der mit über NSLs angeforderten Daten gesetzlich beschränkt: Der Inhalt der Kommunikation wird nach dem Gesetz mit NSLs nicht abgefragt. In der genannten Vorschrift 18 U.S.C. § 2709 sind folgende Daten für die Abfrage aufgelistet: „Name, Adresse, Dauer des Dienstes und Rechnungsunterlagen für die Orts- und Ferngespräche" – worauf sich das *FBI* aber wohl in vielen Fällen, wie in der Presse berichtet wurde, in der Praxis nicht beschränkt hat.

Gerichtliche Überprüfung der NSLs – nicht einfach

Gerichtsverfahren gegen ausgefertigte und zugestellte NSLs sind in der Praxis nicht einfach, weil das *FBI* in aller Regel argumentiert, dass aus Gründen der Nationalen Sicherheit die NSLs geheim bleiben müssen, um Terroristen keine Hinweise auf Ermittlungen oder die Ermittlungstaktik zu geben. Eine Reihe von Verfahren auf Aktenzugang nach dem Freedom of Information Act (FOIA) sind von Gerichten abschlägig beschieden worden. Besonders beachtenswert ist ein Verfahren, das derzeit beim *Kalifornischen Bundesgericht für den Nördlichen Bezirk* anhängig ist: Eine im TK-Bereich tätige Gesellschaft in Kalifornien legte gegen einen NSL gerichtliche Beschwerde ein. Das *FBI* erhob Widerklage u.a. mit dem Argument, dass die Gesellschaft allein schon durch das Einreichen der Beschwerde nationale Sicherheitsinteressen der USA verletze. Die Verfassungsmäßigkeit des NSL dürfe das *Gericht* nicht prüfen, da das *FBI* insoweit Immunität genieße. Das *US-Justizministerium* gibt zu dem laufenden Verfahren keinen Kommentar ab. Der Name der Gesellschaft ist in den öffentlich zugänglichen Gerichtsdokumenten geschwärzt, aber es scheint sich um die in San Francisco ansässige Gesellschaft *Credo* zu handeln. Die Gesellschaft gibt ebenfalls wegen der genannten Schweigevorschrift (Gag-Order) keine Auskunft. Das *Gericht* hat trotz der Intervention des *FBI* den Disput zur Entscheidung angenommen. Wann dieser Fall endgültig entschieden wird, steht noch nicht fest.

Konsequenzen

Aus europäischer Warte ist festzuhalten, dass das Problem der Datensammlung nach dem Patriot Act beim Cloud Computing nicht einfach dadurch gelöst wird, dass die Daten in einer European Cloud abgespeichert werden. Das US-Recht geht von der sog. Personal Jurisdiction aus, sodass es im Prinzip nicht darauf ankommt, wo auf der Welt sich die Prozesspartei oder der Zeuge gerade aufhält und wo die Beweismittel belegen sind. Ebenso kommt es nicht darauf an, wo sich die Daten befinden, wenn eine Vorlageanordnung (Subpoena) der Partei rechtskräftig zugestellt wird. Eine EU-Gesellschaft mit einem Büro in den USA könnte deswegen mit einem NSL oder einer FISA-Order konfrontiert werden, selbst wenn sich die Daten in einer EU-Cloud befinden. Eine andere Möglichkeit für die US-Behörden besteht darin, sich gewünschten Informationen über den Mutual Legal Assistance Treaty (MLAT) zwischen der EU und den USA (2003) aus der EU zu besorgen. Es heißt, dass die EU die Kooperation mit den USA in Fällen der Terrorismusbekämpfung im Wege des MLAs so gut wie nie verneint.

Schließlich müssen sich die Kritiker des Patriot Act in der EU darüber im Klaren sein, dass es auch in den EU-Ländern weitgehende rechtliche Möglichkeiten für die Sicherheitsbehörden gibt, an Daten zur Terrorismusbekämpfung heranzukommen. Ein kürzlich veröffentlichtes Rechtsgutachten einer namhaften internationalen Kanzlei gelangt zum selben Ergebnis. In der EU gibt es überdies die (für Deutschland derzeit vom *BVerfG* MMR 2010, 356, ausgesetzte) Vorratsdatenspeicherung zur Verbrechensbekämpfung in bestimmten Fällen, die in den USA derzeit keinen Gegenpart hat. Eine automatische Speicherung von Daten und Weiterleitung an die Behörden ist vom US Patriot Act nicht vorgesehen. Eine länderübergreifende Lösung des Datenzugangs für die Sicherheitsbehörden wäre in der Tat wünschenswert (so auch *Brookman* im Editorial der ZD 9/2012, S. 401).

■ Vgl. *Spies*, ZD-Aktuell 2012, 02957.

Dr. Axel Spies
ist Rechtsanwalt in der Kanzlei Bingham McCutchen LLP in Washington DC und Mitherausgeber der ZD.

EU-Kommission: Freier Zugang zu wissenschaftlichen Daten

ZD-Aktuell 2012, 03030

Die *EU-Kommission* hat konkrete Vorschläge zur Vollendung des Europäischen Forschungsraums – eines Binnenmarkts für Forschung und Innovation in Europa – vorgelegt. Damit soll die wissenschaftliche Zusammenarbeit von europäischen Forschern, Forschungseinrichtungen und Unternehmen über Grenzen hinweg vereinfacht und die Wettbewerbsfähigkeit der Mitgliedstaaten erhöht werden.

Ergänzend zu den Vorschlägen stellt die *Kommission* eine Initiative vor, um öffentlich geförderte Forschung in Europa frei zugänglich zu machen. Der umfassendere und schnelle Zugang zu wissenschaftlichen Artikeln und Daten soll es für Forscher und Unternehmen leichter machen, die Ergebnisse öffentlich geförderter Forschung zu nutzen. Durch einen freien Zugang würden wichtige Durchbrüche schneller erreicht werden, wodurch letztlich die Wettbewerbsfähigkeit gesteigert würde.

Bis 2016 sollen 60% der veröffentlichten Ergebnisse der in Europa öffentlich geförderten Forschung frei zugänglich sein. So würde die Innovationskapazität der EU gestärkt werden und die Bürger kämen rascher in den Genuss der Vorteile wissenschaftlicher Entdeckungen. Die jährlichen Forschungsinvestitionen i.H.v. € 87 Mrd. würden auf diese Weise rentabler. In einem ersten Schritt will die *Kommission* den freien Zugang zu wissenschaftlichen Veröffentlichungen als allgemeinen Grundsatz im Programm „Horizont 2020", dem Forschungs- und Innovationsförderprogramm der EU für den Zeitraum 2014–2020, verankern. Ab 2014 müssen alle Artikel, die mit Hilfe der Förderung durch „Horizont 2020" zu Stande gekommen sind, zugänglich sein.