PRESSEMITTEILUNG

TeleTrusT – Bundesverband IT-Sicherheit e.V.:

'PRISM' und die Konsequenzen

Anwenderschutz / IT-Mittelstandsförderung / Nationale Sicherheitsstrategie: Zieht die Bundesregierung jetzt die richtigen Schlussfolgerungen?

Berlin, 12.06.2013 – Der TeleTrusT – Bundesverband IT-Sicherheit e.V. sieht die aktuelle Diskussion über das Überwachungssystem "PRISM" als Gelegenheit, insbesondere die Vorteile von Lösungen 'made in Germany' in den Blickpunkt zu rücken und fordert die Bundesregierung auf, jetzt zu handeln.

Aktuellen Medienberichten zufolge erheben US-Behörden, namentlich die National Security Agency, im Rahmen des Programms "PRISM" bzw. "Upstream" in erheblichem Umfang und routinemäßig Daten aus der Kommunikationsüberwachung von Nutzern großer amerikanischer Internet-Dienste. Für IT-Sicherheitsexperten ist diese Erkenntnis weder überraschend noch neu, allenfalls die offenkundige Dimension.

Die USA sammeln Daten mit der zunächst legitimen Motivation, sich vor terroristischen Anschlägen zu schützen. Der zugrundeliegende "Patriot Act" hat bereits kurz nach den Anschlägen vom 11.09.2001 den dortigen Behörden großen Spielraum beim Zugriff auf Daten von Internetnutzern eingeräumt. Unklar war bisher, in welchem Umfang US-Dienste diese eingeräumten Rechte tatsächlich nutzen.

Deutsche Behörden, Unternehmen und private Anwender sollten sich fragen, welche Konsequenzen sie ziehen. Ob nämlich der Zugriff auf Daten zielführend und welcher rechtliche Rahmen dabei einzuhalten ist, bestimmen amerikanische Institutionen. Deutschen Institutionen, Unternehmen und privaten Nutzern bleibt ein Mitbestimmungsrecht offensichtlich verwehrt, wenn man von der Möglichkeit der Nichtnutzung der marktdominierenden Internetdienste absieht. Ebenso verborgen bleibt, in welchen Verwendungskontext die erhobenen Daten geraten.

Behörden sind in der besonderen Pflicht, vertrauenswürdige Anbieter auswählen, z.B. mit deutscher Sicherheitszulassung oder Zertifizierung. Privatanwender haben die Option, einheimische Mailkommunikationsdienstleister zu nutzen, vorausgesetzt, es gelingt diesen, das durch die jetzigen Vorgänge insgesamt gestörte Vertrauen aufzubauen. IT-Sicherheit ist dabei das entscheidende Element.

TeleTrusT kritisiert in diesem Zusammenhang, dass seit zwei Jahren erfolglos ein Datenschutzabkommen zwischen der EU und den USA verhandelt wird. TeleTrusT unterstützt die europäische Forderung, wonach US-Partner zwei Grundbedingungen akzeptieren müssen:
- Klagemöglichkeiten für EU-Bürger vor US-Gerichten geben
- Verpflichtung von US-Firmen, die in der EU tätig sind, sich an die in der Datenschutzrichtlinie vorgesehenen hohen Standards zu halten.

TeleTrusT sieht sich in der Vermutung bestätigt, dass sensible Daten in Servern US-amerikanischer Anbieter nicht sicher im Sinne des hiesigen Datenschutzverständnisses bzw. Fernmeldegeheimnisses sind. TeleTrusT empfiehlt deshalb mit Nachdruck mindestens bei Cloud-Speicherung und vertraulicher Kommunikation den Einsatz von Technologie deutscher oder europäischer Anbieter, die dem Bundesdatenschutzgesetz bzw. dem Fernmeldegeheimnis oder einer gleichartigen Rechtsqualität unterliegen oder zumindest dem Datenschutzniveau auf EU-Ebene. Zusätzlich sollten adäquate Verschlüsselungsverfahren eingesetzt werden. Auch hier gibt es zahlreiche Lösungen deutscher Anbieter.

Erfreulicherweise wird die Entwicklung von IT-Sicherheitstechnologien in Deutschland seit längerem durch Förderprogramme unterstützt. "IT Security made in Germany" genießt weltweit einen guten Ruf. Was gele-

gentlich fehlt, ist die Anerkennung durch die breite Öffentlichkeit. Amerikanische Anbieter nutzen vor allem hier den Vorteil eines starken Heimatmarktes.

Der überwiegende Teil der IT-Sicherheitsindustrie in Deutschland besteht aus mittelständischen Unternehmen oder hochspezialisierten Start-ups. Die Bundesregierung hat jetzt die Gelegenheit, unter Beweis zu stellen, dass ihr Mittelstands- und Innovationsförderung auch auf diesem Gebiet wichtig sind.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik hat durch seine bisherige Evaluierungs- und Zulassungspolitik einen wichtigen Beitrag für die Stärkung der deutschen IT-Sicherheitsindustrie geleistet. Dieser Weg erscheint aus Sicht von TeleTrusT richtig.

Prof. Dr. Norbert Pohlmann, TeleTrusT-Vorsitzender: "Auch zukünftig müssen exzellente Lösungen 'made in Germany' gefördert werden. Verwaltung und Industrie müssen sich hier als Partner verstehen. Eine gesunde und leistungsfähige IT-Sicherheitsindustrie ist für Deutschland von nationaler und politisch-strategischer Bedeutung."

TeleTrusT – Bundesverband IT-Sicherheit e.V., Dr. Holger Mühlbauer, Geschäftsführer, Chausseestraße 17, 10115 Berlin, Tel.: +49 30 /40054310, holger.muehlbauer@teletrust.de
www.teletrust.de