Marco Buschmann MdB
Generalsekretär der FDP NRW
Düsseldorf, 05.07.2013

Fünf Fragen und Antworten zu PRISM & Tempora

Was bedeuten PRISM und Tempora?

Auf Grundlage des US-Auslandsüberwachungsgesetzes erfasst der US-Geheimdienst National Security Agency (NSA) mit dem nun bekannt gewordenen Programm PRISM Verbindungsdaten und Inhalt, etwa von Mails, Internettelefonie, sozialen Netzwerken, Chats und Videokonferenzen sowie Zugangsdaten und im Netz gespeicherte Inhalte von Nicht-US-Bürgern.
Anordnungen der geheimen FISA-Gerichte können alle Unternehmen mit Sitz in den USA treffen, darunter auch AOL, Apple, Facebook, Google, Microsoft, Skype, Yahoo, YouTube. Zudem wurde bekannt, dass US-Sicherheitsbehörden aufgrund geheimer Anordnungen die Verbindungsdaten von Telefonaten anlasslos speichern können.

Nach Informationen des früheren NSA-Mitarbeiters Edward Snowden soll mit Tempora der britische Geheimdienst Government Communications Headquarter (GCHQ) direkt an den Netzknoten und den großen Glasfaserkabeln, durch die gebündelt alle digitalen Datenströme zusammenlaufen, anlasslos alle Verbindungs- und Inhaltsdaten von Telefonnutzung wie auch von Mails, Websites und anderer Internetkommunikation überwachen. Diese werden dann für mindestens dreißig Tage gespeichert und ausgewertet. Abgefischt würden alle Daten, die über diese Knoten und Kabel laufen, was ca. 95% der Kommunikation Europas ausmacht.

Ist auch Deutschland betroffen?

Ja. Fast alle der Unternehmen, deren Daten von PRISM erfasst werden, bieten ihre Dienste und Produkte auch in Deutschland an und haben teilweise Millionen Nutzer. Durch Tempora sind ebenfalls Millionen Deutscher betroffen, weil fast die gesamte Internet- und Telefonkommunikation abgehört wird. Damit wird die private wie auch geschäftliche Kommunikation auch der deutschen Bürgerinnen

und Bürger wie auch Unternehmen vollumfänglich erfasst – von Telefongesprächen über SMS bis zu Mails und Profilen in sozialen Netzwerken.

Machen deutsche Nachrichtendienste etwas Ähnliches?

Nein, das ist ihnen nicht erlaubt. Der deutsche Auslandsnachrichtendienst Bundesnachrichtendienst (BND) ist dem Bundeskanzleramt fachlich unterstellt und wird vom Parlamentarischen Kontrollgremium des Bundestags kontrolliert. Zwar gehört zu den Aufgaben des BND auch die sogenannte strategische Fernmeldeaufklärung. Dabei darf der BND auf Grundlage des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G10-Gesetz) zur Auslandsaufklärung bestimmter außen- und sicherheitspolitisch relevanter Gefahrenbereiche (wie internationaler Terrorismus) unter engen Voraussetzungen einen begrenzten Teils der gebündelt übertragenen internationalen Telekommunikationsverkehre erfassen. Im Gegensatz zu den amerikanischen und britischen Programmen werden – und darin besteht der entscheidende Unterschied – jedoch nur Treffer, d.h. aufgrund von Anhaltspunkten verdächtige Kommunikation, gespeichert. Zudem darf der BND – anders als etwa der britische Geheimdienst GCHQ – keine Wirtschaftsspionage betreiben. Über die Maßnahmen nach dem G10-Gesetz wird jährlich ein Bericht veröffentlicht. Der deutsche Inlandsnachrichtendienst, das Bundesamt für Verfassungsschutz, hat überhaupt nicht derartige Befugnisse.

Was will die FDP?

Die FDP lehnt jede verdachtsunabhängige Überwachung von Internet- und Telefonkommunikation entschieden ab.
Für uns ist ganz klar, dass nicht alles, was technisch geht, auch rechtlich erlaubt sein darf. Nicht die technische Machbarkeit setzt die Grenzen des Rechtsstaats, sondern unsere Verfassung und die Grundrechte.
Aufklärung ist nach wie vor notwendig: Daher hat die liberale Justizministerin Leutheusser-Schnarrenberger sich bereits an ihre amerikanischen und britischen Kollegen gewandt. Wirtschaftsminister Rösler hat einige der von PRISM betroffenen Unternehmen befragt. Die Bundesregierung hat der britischen wie amerikanischen Botschaft einen Fragenkatalog zugesandt.

Außenminister Westerwelle hat außerdem mit seinem amerikanischen Amtskollegen John Kerry telefoniert und eine zügige Aufklärung der im Raum stehenden Spionagevorwürfe gefordert.
Die Bundesregierung soll nun eine ressortübergreifende Projektgruppe einrichten, die alle rechtlichen und politischen Möglichkeiten auf europäischer und internationaler Ebene prüft, um derartigem Treiben ausländischer Nachrichtendienste einen Riegel vorzuschieben.
Von der gesamten Bundesregierung fordern wir, gegenüber den USA und Großbritannien klar zum Ausdruck zu bringen, dass der Kampf gegen den Terrorismus nicht rechtfertigt, grundlegende Freiheiten - wie das Recht auf Privatheit - aufzugeben, nur weil der technologische Fortschritt dies heute einfach macht.

Die Europäische Kommission muss nun in den seit langem stockenden Verhandlungen über ein allgemeines Datenschutzabkommen zwischen den USA und der EU den Druck erhöhen. Sie muss für einen Abschluss kämpfen, der das Recht auf informationelle Selbstbestimmung schützt, allen Betroffenen Rechtsschutz garantiert und Transparenz in die Datensammelaktivitäten des NSA bringt.
Die zuständigen Landesdatenschutzbeauftragten sind aufgefordert, die Unternehmen mit US-amerikanischen Konzernmüttern oder amerikanischen Tochterunternehmen zu prüfen, um zu klären, ob und in welchem Umfang Daten deutscher Nutzer an die NSA weitergegeben wurden.

Was kann jeder selbst tun, um seine Daten zu schützen?

Der beste Datenschutz ist Datenvermeidung. Alles, was man nicht ins Internet stellt, kann auch keiner dort finden und speichern. Aber es wäre natürlich fatal, wenn die Menschen aus Angst vor Überwachung von nun an darauf verzichten, an der Informationsgesellschaft teilzuhaben. Menschen dürfen nicht ihr Recht auf Privatheit einbüßen, wenn sie bei sozialen Netzwerken ihre Daten einstellen. Kein Staat hat das Recht, anlasslos alle Daten zu sammeln und lückenlose Profile von Menschen zu erstellen.
Deutsche Unternehmen, die ausländischem Recht nicht unterliegen, können von fremden Nachrichtendiensten nicht gezwungen werden, Daten herauszugeben. Wer vertrauliche Unterlagen im Internet speichert, sollte darauf achten, wo die Dienstanbieter sitzen und wo deren Server stehen. Allerdings schützt dies nicht vor etwaigem Abfischen an den Glasfaserkabeln direkt, da davon Daten auch während des Transports vom eigenen Rechner auf einen Server und wieder zurück erfasst werden.
Datensicherheit und Datenschutz gehen Hand in Hand. Wer seine Daten verschlüsselt, schützt diese auch vor unbefugter Kenntnisnahme. Verschlüsselungstechnologien für Mails, eigene Datenspeicher wie Festplatten oder auch für einzelne Dokumente wie z.B. PGP (Pretty Good Privacy) kann jeder einfach im Internet finden und herunterladen und auf seinen Geräten installieren.

Unternehmen sollten dafür Sorge tragen, dass gerade die mobilen Geräte, die ihre Mitarbeiter nutzen, geschützt sind. Nicht nur kann man Laptops verschlüsseln, es gibt auch viele Angebote für eine Verschlüsselung der Mobilfunkkommunikation, die auch für kleine und mittlere Unternehmen angeboten werden.

Anonymes Surfen im Internet wird möglich durch Dienste wie das TOR-Netzwerk (The Onion Router), das die Identität beim Internetsurfen verschleiert. Die Installation auf dem eigenen Rechner ist einfach für jedermann möglich. Mittels TOR-Apps kann man auch mit mobilen Geräten anonym surfen.

V.i.S.d.P.: Marco Buschmann, FDP NRW, Sternstraße 44, 40479 Düsseldorf