FDP| 15.11.2013 - 15:30

Schnarrenberger formuliert 10 Thesen zur Cybersicherheit

Der 2. Cyber Security Summit der Münchner Sicherheitskonferenz und der Deutschen Telekom hat durch die NSA-Spähaffäre neue Dringlichkeit bekommen. Sabine Leutheusser-Schnarrenberger nutzte die Veranstaltung, um ihre Ablehnung der Vorratsdatenspeicherung zu bekräftigen. Jetzt hat sie nachgelegt und 10 Grundthesen zur Zukunft der Cybersicherheit formuliert.

Die Abhörmethoden des US-Geheimdiensts NSA und die wachsende Zahl von Sicherheitsattacken auf Computernetzwerke haben das Thema digitale Sicherheit ins Rampenlicht gerückt. Da kam der am Montag von der Münchner Sicherheitskonferenz und der Deutschen Telekom durchgeführte zweite Cyber Security Summit zu einem guten Zeitpunkt.

Die Kernforderungen des Summits - mehr Investitionen in IT-Sicherheit, mehr Transparenz, vielleicht eine Meldepflicht für IT-Angriffe – waren zwar nicht neu, bekamen durch die aktuelle Situation aber neue Dringlichkeit.

Die noch amtierende Bundesjustizministerin Sabine Leutheusser-Schnarrenberger machte bei der Veranstaltung klar: "Der Widerstand gegen die anlasslose Speicherung war aus rechtsstaatlichen Erwägungen notwendig." Dabei erteilte sie erneut dem von Bundesinnenminister Hans-Peter Friedrich (CSU) propagierte Supergrundrecht Sicherheit eine Absage. Sie warb erneut dafür, die grundlegenden Regelungen der geplanten EU-Datenschutzgrundverordnung möglichst noch vor den Europawahlen im Mai 2014 zu verabschieden. "Jetzt sind die Regierungen am Zug", erklärte Leutheusser-Schnarrenberger.

10 Grundthesen zur Zukunft der Cybersicherheit

Jetzt legte die Liberale nach. Sie formulierte 10 Grundthesen zur Zukunft der Cybersicherheit, die wir hier dokumentieren:

1. Das Vertrauen in den Schutz privater und geschäftlicher Daten muss wieder hergestellt werden. Datenschutz und Datensicherheit muss gewährleistet werden, damit dieses Vertrauen begründet ist.

2. Aufklärung darüber, an welchen Geheimdienst oder auch andere Stellen unter welchen Voraussetzungen Daten der Kunden gelangen, ist die erste Voraussetzung für neu zu begründendes Vertrauen.

3. Erforderlich ist endlich ein Paradigmenwechsel hin zur Sicherung von Daten bei konkreten Anlässen anstelle einer anlasslosen Datenhäufung.

4. Die Nutzung von Cloud-Diensten nimmt immer weiter zu.

5. Zugleich nimmt auch die Gefährdung von Geschäftsgeheimnissen, Kunden- und Nutzerdaten immer weiter zu. Die Themen Datenschutz und Datensicherheit müssen deshalb auch im Rahmen von Compliance-Bemühungen eine starke Rolle einnehmen.

6. Dass es in Deutschland keine Schnittstellenpflicht und keine Geheimgerichte gibt, ist ein Vertrauens- und damit Standortvorteil.

7. Investitions- und Infrastrukturmaßnahmen sind erforderlich, um den Motor des dynamischen Wachstumsmarktes in Deutschland, die mittelständischen Unternehmen, zu unterstützen.

8. Europa kann sich durch den Rechtsrahmen einer europäischen Datenschutzgrundverordnung und ein regionales Netz einen Standortvorteil erarbeiten. Dazu bedarf es einer engen interdisziplinären Kooperation zwischen Juristen, Wissenschaftlern und Informationstechnikern.

9. Das Marktortprinzip ist notwendig, um die Wettbewerbsfähigkeit europäischer Unternehmen zu gewährleisten.

10. Im Verhältnis zu den USA müssen klare Forderungen im Hinblick auf No Spy-Abkommen, das Swift-Abkommen, Safe Harbour und ein Datenschutzabkommen gestellt werden.

Mehr zum Thema

- Cyber Security Summit [1]
- IT-Nutzerfreundlichkeit ist Wirtschaftsfaktor [2]
- Pilotprojekt "Datenschutz-Zertifizierung von Cloud-Diensten" [3]

Links
[1] http://www.cybersecuritysummit.de/ [2] http://www.liberale.de/content/it-nutzerfreundlichkeit-ist-wirtschaftsfaktor [3] http://bmwi.de/DE/Presse/pressemitteilungen,did=600746.html