Redaktion: Helmut Reimer

Report

BfDI: Leitfaden für die wissenschaftliche Evaluation von Sicherheitsgesetzen

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar hat am 21.11.2012 einen Leitfaden zur Gesetzesevaluation vorgestellt. Der Leitfaden wurde im Auftrag des Bundesbeauftragten vom Deutschen Forschungsinstitut für öffentliche Verwaltung, unter der Leitung von Professor Dr. Jan Ziekow, erarbeitet.

Peter Schaar: „Die Eignung gesetzlicher Maßnahmen und ihre Folgen für die Grundrechte der Bürgerinnen und Bürger müssen nach wissenschaftlichen Kriterien beurteilt werden. Die Deutungshoheit hierfür darf nicht weiter bei den Stellen liegen, die mit zusätzlichen Befugnissen ausgestattet wurden. Vielmehr muss der Deutsche Bundestag auf Basis unabhängiger und nach wissenschaftlichen Kriterien durchgeführter Evaluation darüber entscheiden, ob einmal beschlossene Befugnisse weiterhin gerechtfertigt sind."

Die Erfahrung zeige, dass insbesondere die aufgrund konkreter Bedrohungen eingeführten Befugnisse der Sicherheitsbehörden selbst nach einer Entspannung der Sicherheitslage nicht zurückgenommen wurden. Noch im vergangenen Jahr wurden die nach dem 11. September 2001 unter Zeitdruck erlassenen Anti-Terror-Gesetze erneut ohne gründliche, unabhängige Überprüfung verlängert. Der gesetzlich geforderte Evaluierungsbericht wurde vor der Verabschiedung des Gesetzentwurfs nicht vorgelegt.

Der „Leitfaden zur Durchführung von ex-post-Gesetzesevaluationen unter besonderer Berücksichtigung der datenschutzrechtlichen Folgen" richtet sich an Abgeordnete und Beamte, die mit einer Gesetzesevaluation betraut sind. Der Leitfaden setzt sich umfassend mit den Standards, Evaluationsinstrumenten und Methoden auseinander, die für die Evaluation gelten und stellt die verfassungsrechtlichen Rahmenbedingungen dar. Er gibt zudem einen praktischen Überblick über die notwendigen Abläufe bei den evaluierenden Stellen. Schon bevor eine Evaluierung in Auftrag gegeben wird, hilft der Leitfaden den Entscheidungsträgern, dafür die richtigen Bedingungen festzulegen.

Der Leitfaden ist über die Website des BfDI verfügbar: *http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/Evaluation_Leitfaden.html?nn=408908*

Eckpunktepapier der Bundesregierung zu „Trusted Computing" und „Secure Boot"

Im August 2012 hat die Bundesregierung, vertreten durch das Bundesministerium für Wirtschaft und Technologie ein neues Eckpunktepapier zu ‚Trusted Computing' veröffentlicht. Es löst das Eckpunktepapier „Trusted Computing" der Bundesregierung vom 04 September 2007 ab.

1. Begriffsbestimmung

Die Bundesregierung versteht unter „Trusted Computing" die Architekturen, Implementierungen, Systeme und Infrastrukturen, die auf den Standards der Trusted Computing Group (TCG) basieren oder diese nutzen. Dazu gehört insbesondere „Secure Boot" und weitere Funktionen im Unified Extensible Firmware Interface (UEFI)-Standard des Unified EFI Forums, der auf den TCG-Standards oder nahe verwandten Techniken aufbaut. Zur Vermeidung von Missverständnissen wird eine darüber hinausgehende, allgemeinere Verwendung des Begriffs „Trusted Computing" stets besonders gekennzeichnet.

2. Erhöhung der IT-Sicherheit

Die Bundesregierung unterstützt eine Erhöhung des Niveaus der IT-Sicherheit auf IT-Plattformen von Unternehmen, öffentlicher Verwaltung und Privatanwendern durch die Einführung von „Trusted Computing"-Lösungen auf Grundlage der Standards der TCG, soweit diese die hier aufgeführten Eckpunkte erfüllen.

3. Vollständige Kontrolle durch Geräte-Eigentümers

Ein Geräte-Eigentümer muss über die vollständige Kontrolle (Steuerbarkeit und Beobachtbarkeit) der gesamten „Trusted Computing"-Sicherheitssysteme seiner Geräte verfügen. Der Geräte-Eigentümer muss im Rahmen seiner Ausübung der Kontrolle über das Gerät entscheiden können, inwieweit er eben diese Kontrolle an seine Nutzer oder Administratoren delegiert. Eine Delegation dieser Kontrolle an Dritte (Hardware oder Software-Komponenten des Geräts oder den Geräte-Hersteller) setzt eine bewusste und informierte Einwilligung des Geräteeigentümers voraus (also u. a. in voller Kenntnis der möglichen Einschränkungen der Verfügbarkeit durch Maßnahmen des oder der Dritte, an den oder die Kontrollmöglichkeiten delegiert wurden).

4. Entscheidungsfreiheit

Bei der Auslieferung von Geräten müssen „Trusted Computing"-Sicherheitssysteme deaktiviert sein („Opt-in"-Prinzip). Geräte-Eigentümer müssen in der Lage sein, aufgrund der vorausgesetzten technischen und inhaltlichen Transparenz von „Trusted Computing"-Lösungen eigenverantwortliche Entscheidungen zur Produktauswahl, Inbetriebnahme, Konfiguration, Anwendung und Stilllegung zu treffen. Eine spätere Deaktivierung muss ebenfalls möglich sein („Opt-out"-Funktionalität) und darf keine negativen Einflüsse auf die Funktionalität der Hard- und Software haben, die nicht die Funktion der „Trusted Computing"-Technik nutzen.

5. Öffentliche Verwaltung, nationale und öffentliche Sicherheitsinteressen

Aufgrund der hohen Verbreitung von „Trusted Computing"-Sicherheitssystemen im privatrechtlichen Massenmarkt kann und soll die öffentliche Verwaltung von der Verfügbarkeit wirtschaftlicher Lösungen auch für ihren Bereich profitieren. Der Betrieb und die Verfügbarkeit von Geräten in der öffentlichen Verwaltung und im Bereich der nationalen und öffentlichen Sicherheit bedingen aller-