06.02.2017

Eckpunkte der Bundesregierung zu „Trusted Computing“

Präambel

Die Bundesregierung hält Rahmenbedingungen für eine vertrauenswürdige, selbstbestimmte und sichere Nutzung von Informationstechnik (IKT) für unerlässlich, um die Umsetzung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[1] zu erreichen. Grundlegende Voraussetzung hierfür ist die Kontrollierbarkeit von IKT-Systemen durch den Eigentümer und die umfassende Aufklärung des Nutzers über die Eigenschaften der eingesetzten Hardware, Software und Dienste. Diese Forderungen der Bundesregierung richten sich insbesondere an die Hersteller und Anbieter von Produkten und ermöglichen bei deren Auswahl und Erwerb eine bewusste Entscheidung. Klare Kriterien sollen dabei die Durchsetzung geeigneter Produkte am Markt sichern.

Begriffsbestimmung

Unter „Trusted Computing“ versteht die Bundesregierung in Zusammenhang mit diesem Dokument die Bereitstellung von vertrauenswürdigen Informationen über die Konfiguration und den Software-Zustand eines IKT-Systems, z.B. auf Basis von Messwerten und Checksummen. Auf Basis dieser Informationen können dann z. B. (Software-)Entscheidungen getroffen oder Sicherheitsrichtlinien durchgesetzt werden.

Forderungen

1. Sicherheit ohne Zwangsbündelung

   Anwender von IKT-Systemen dürfen nicht implizit gezwungen werden mit der Nutzung von „Trusted Computing“ -Architekturen oder -Systemen weitere von ihnen nicht gewünschte Funktionen akzeptieren zu müssen.

2. Wahlfreiheit sichern

   „Trusted Computing“-Architekturen oder -Systeme dürfen die Möglichkeit der wahlfreien Nutzung von Software und digitalen Inhalten nicht einschränken (z.B. die Installation alternativer Betriebssysteme auf PC, Routern etc.), sofern der Anwender keine eingeschränkte Nutzung (z.B. aus Sicherheitsgründen) wünscht (wahlweise Opt-out / Opt-in). Der Anwender muss die die uneingeschränkte Verfügungsgewalt behalten.

3. Datenhoheit für digitale Inhalte

   „Trusted Computing“-Architekturen oder –Systeme dürfen nicht verwendet werden, um digitale Inhalte, die an eine Person gebunden sind, zusätzlich an eine spezielle Hardware zu binden. Nutzer müssen ihr Recht auf Datenübertragbarkeit ausüben und jederzeit die mit ihrer Person verknüpften Daten auf andere Plattform übertragen können, so dass die Verfügungsgewalt erhalten bleibt.

Eigenschaften

4. Offene und transparente Strukturen, Standards und Protokolle

   „Trusted Computing“-Architekturen oder -Systeme müssen auf offenen Standards und Protokollen basieren. Dokumentation und Lizenzbedingungen, Systemarchitektur und

[1] BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 333), http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

Algorithmen sind offenzulegen. Open Source und interoperable Implementierungen sind zu fördern.

5. Zertifizierung
„Trusted Computing“-Architekturen oder -Systeme müssen für den Einsatz in besonders schützenswerten Einsatzumgebungen nach Common Criteria (EAL 4+ oder höher) zertifizierbar sein.

6. Ausfallsichere Architektur
Grundsätzlich darf “Trusted Computing“ für die Sicherung eines Systems keine Netzanbindung voraussetzen. Sofern darüber hinaus externe Infrastrukturen für die Funktionen “Trusted Computing“ benötigt werden, sollten diese redundant ausgelegt sein. Ein gestörtes „Trusted Computing“ darf nicht zu einem Systemausfall führen.

7.

Anwendungsspezifische Empfehlungen:

Bürgerinnen und Bürger:

„Trusted Computing“ kann in Zeiten steigender Bedrohung der IKT-Systeme bei Bürgerinnen und Bürgern einen wertvollen Beitrag dazu leisten die Systeme sicherer zu machen. Dadurch, dass IKT-Systeme zunehmend in alle Bereiche des täglichen Lebens vordringen, erhöht sich auch die Abhängigkeit von diesen Systemen. Dabei kommen IKT-Systeme zunehmend im häuslichen Umfeld zum Einsatz. Beispiele hierfür sind, neben bereits etablierten IT-Komponenten wie PC, Smartphone und Tablet, die elektronische gesteuerte Heizung, elektronische Zutrittsanlagen und IT-gesteuerte Raumlufttechnik. Durch die zunehmende Vernetzung dieser IT-Systeme (mit dem Internet), sei es für Service- und Wartungszwecke (z.B. Softwareupdate) oder für Komfortfunktionen (Smart-Home, Ambient Assisted Living), können auch ferngesteuerte Manipulationen an der Software dieser Geräte nicht ausgeschlossen werden. Sofern in diesen Bereichen „Trusted Computing“ verwendet wird, sollte eine Opt-out Lösung (Security by Default) zur Anwendung kommen. Dies ist sinnvoll, da der Durchschnittsnutzer der IKT-Systeme kein Sicherheitsexperte ist und ein System erwartet, dessen Auslieferungszustand vertraut werden kann. Dennoch sollte der Eigentümer dieser IKT-Systeme die Entscheidungshoheit darüber besitzen, ob er die herstellerseitig vorgesehene Softwarekonfiguration nutzt, oder ggf. alternative Software in seinem System installiert, sofern dem keine übergeordneten Hinderungsgründe (Gesetze, Sicherheit) entgegenstehen. Dies muss ihm durch die Deaktivierung von „Trusted Computing“ im Rahmen einer Opt-out Lösung möglich sein.

Automotive, Gesundheitswesen:

IKT-Systeme werden im Automotive-Bereich und Gesundheitswesen zunehmend in Funktionsbereichen eingesetzt, die sicherheitskritisch auch im Sinne von „safety“ (d.h. es handelt sich um Systeme die Leben schützen oder retten sollen) sind. Zertifizierte „Trusted Computing“-Architekturen oder -Systeme können eine geeignete Infrastruktur darstellen (z.B. im KfZ-Zulassungsverfahren, in der Luft-, Bahn- oder Schifffahrt, Medizintechnik), um die erforderlichen Sicherheitseigenschaften abzubilden und damit die Systemhersteller ihrer Gesamtproduktverantwortung gerecht werden können.

Industrie, Kritische Infrastrukturen, Verwaltung:

IKT-Systeme in Kritischen Infrastrukturen, Industrie, und Verwaltung erfordern ein besonders hohes Maß an Verfügbarkeit und Sicherheit. „Trusted Computing“-Architekturen oder -Systeme können in diesem Bereich genutzt werden, um überwachen zu können, dass die eingesetzten IKT-Systeme bestimmungsgemäß funktionieren. „Trusted Computing“ kann dabei unterstützen, dass nur autorisierte Software auf den Hardwaresystemen abläuft und damit die Systemverantwortlichen ihre Gesamtverantwortung für Sicherheit wahrnehmen können. Im Zuge dieser Gesamtverantwortung darf der Eigentümer in keinem Falle gezwungen werden in Gänze oder auch nur in Teilen die Kontrolle an Dritte außerhalb des eigenen Einflussbereichs abzutreten.