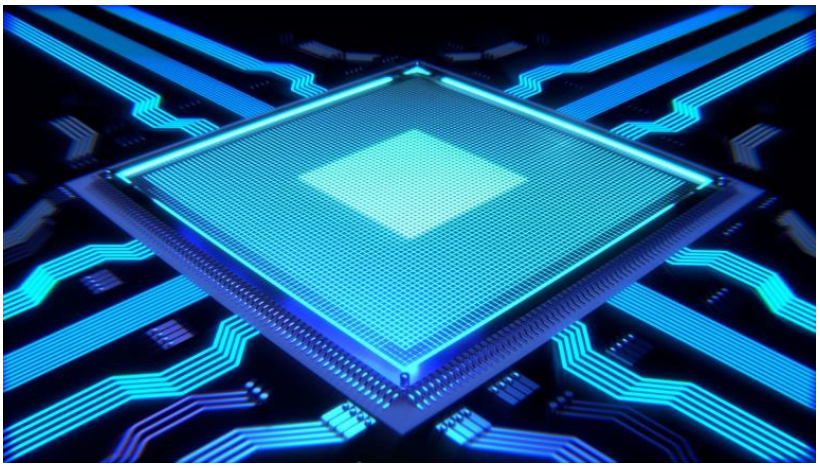
Transparente IT-Produktion für digitale Souveränität

IT-Sicherheitslücken betreffen Bürgerinnen und Bürger genauso wie Unternehmen und Staaten – IT-Experten plädieren für den Einsatz verifizierter Open-Source-Produkte



Raus aus der Black Box: Open Source-Hardware kann IT-Systeme sicherer machen (Abbildung: Pixabay, CC0 Creative Commons).

Monika Landgraf
Pressesprecherin,
Leiterin Gesamtkommunikation

Hermann-von-Helmholtz-Platz 1
76344 Eggenstein-Leopoldshafen
Tel.: +49 721 608-21105
E-Mail: presse@kit.edu

Weiterer Pressekontakt:

Jonas Moosmüller
ITAS - Öffentlichkeitsarbeit
Tel.: +49 721 608 26796
jonas.moosmueller@kit.edu

Margarete Lehné
Stv. Pressesprecherin
Tel.: +49 721 608-21157
margarete.lehne@kit.edu

Ob Automobil-, Energie- oder Finanzsektor: Informationstechnik durchdringt zunehmend alle Bereiche des Lebens. Gleichzeitig werden Sicherheitslücken, die sich durch globalisierte Produktionsketten von geschlossenen Hard- und Softwarekomponenten ergeben, immer schlechter kalkulierbar. Zu diesem Ergebnis kommen IT-Sicherheitsexperten des Karlsruher Instituts für Technologie (KIT), des Fraunhofer Instituts für Sichere Informationstechnologie, von Fraunhofer Singapur, der Hochschule RheinMain und der Technischen Universität Berlin. In einem jetzt vorgelegten Arbeitspapier zur digitalen Souveränität schlagen die Autoren vor, alle Produktionsschritte in der Lieferkette von IT-Produkten transparent zu machen – von der Software bis hin zu den Werkzeugen in Chip-Fabriken.

„Informationstechnik ist allgegenwärtig. Aber es besteht die Gefahr, dass diese Systeme von außen abgeschaltet oder manipuliert werden können und dass Daten unbemerkt ausgelesen oder gegen die Nutzer verwendet werden“, sagt Arnd Weber, Experte für IT-Sicherheit vom Institut für Technikfolgenabschätzung und Systemanalyse

(ITAS) des KIT und Koautor des Papiers. Wie fragil die Sicherheit digitaler Infrastrukturen ist, führen uns Cyberangriffe wie WannaCry, Sicherheitslücken wie Meltdown und Spectre in Prozessoren, spähende „Trojanische Pferde“ oder Blockaden von Servern wie Mirai und der unlängst bekannt gewordene Angriff auf die IT-Infrastruktur der deutschen Bundesregierung eindrucksvoll vor Augen.

Ein zentraler Grund für die zunehmende Anfälligkeit von IT ist: „Viele Software- und Hardwareprodukte haben den Charakter einer Blackbox“, so Jean-Pierre Seifert, Mitautor und Leiter des Instituts für Softwaretechnik und Theoretische Informatik an der TU Berlin. Dies sei eine Bedrohung für die Sicherheit jedes Einzelnen wie auch für ganze Wirtschaftszweige, die auf zugelieferte IT-Technik angewiesen sind. Selbst Nationalstaaten müssten um die Sicherheit ihrer zunehmend digitalisierten Infrastruktur fürchten. Diese Probleme können direkte Auswirkungen auf Leib und Leben haben, etwa bei IT in der Energieversorgung oder in Automobilen. Nicht zuletzt begrenzt die Konzentration der Herstellung von Informationstechnik in den USA und in China die Wertschöpfung in Europa.

Öffnung der gesamten Wertschöpfungskette

Theoretisch gäbe es die Möglichkeit, Sicherheitseigenschaften von Komponenten und Systeme zu zertifizieren. „Angesichts ihrer Komplexität, der schweren Analysierbarkeit von Hardware und der Patentrechte ist dies aber ein schwieriger Weg“, sagt Koautor Michael Kasper von der Fraunhofer-Gesellschaft (SIT und Singapur). Jeglicher Versuch, alle Stufen der Wertschöpfung im IT-Bereich unter nationale Kontrolle bekommen zu wollen, wie dies etwa von China oder Indien angestrebt wird, würde am Kern des weltweiten Problems vorbei gehen, das sich Handelsnationen stellt. „Weit vielversprechender im Sinne digitaler Souveränität ist der Ansatz, nach Open Source-Software, wie Linux und Android, auch Open Source-Hardware zu bauen“, so Michael Kasper. Dabei müssten auch alle verwendeten Werkzeuge zur Platzierung von Schaltkreisen auf Chips einen öffentlichen Quellcode haben.

Open-Hardware Communities

Mit dem Aufbau von Open-Hardware Communities, die, ähnlich wie bei Open-Source Software Communities für Linux oder BSD, alle Komponenten überprüfen und testen, ließen sich Designfehler oder der Einbau von Hintertüren vermeiden, so die Autoren des Arbeitspapiers. Allerdings sollten solche Communities hierzu besser organisiert und privatwirtschaftlich oder staatlich gefördert sein, um Komponenten besser zu verifizieren, damit Fehler nicht unbehoben blieben, wie

dies manchmal in der Vergangenheit der Fall gewesen sei. Idealerweise sollten solche Communities sogar mathematisch beweisen, dass die Komponenten ausschließlich die spezifizierten, d.h. gewünschten Eigenschaften haben. Derartige Beweise existierten bereits für einige offene Betriebssystemkerne. Erste Ansätze für eine Hardware Community fänden sich in den USA, wo Firmen wie Nvidia und Western Digital planen, offene Prozessorarchitekturen in ihren Produkten zu verwenden und dazu mit Universitäten zusammenarbeiten.

Von dem Beschreiten dieses offenen Pfads würden nicht nur Industrie und Endkunden in Deutschland und Europa profitieren: „Letztlich bekäme die ganze Welt eine offene und sichere Basis für alle Geräte, die IT enthalten“, so Koautor Steffen Reith von der Hochschule Rhein-Main. Die Konzentration allen Wissens in nur zwei Regionen der Welt und die entsprechende Zentralisierung der Wertschöpfung würden dadurch tendenziell aufgelöst.

Aufbauend auf einer detaillierten Darstellung zum Stand der Forschung und zu möglichen Handlungsoptionen empfehlen die Autoren als ersten Schritt eine Entwicklung und Produktion derartiger offener Komponenten und Lösungen für das „Internet of Things“, gefördert durch Investoren und Politik. Als zweiten Schritt schlagen die Autoren die Entwicklung hochleistungsfähiger offener Hardware vor.

Arnd Weber, Steffen Reith, Michael Kasper, Dirk Kuhlmann, Jean-Pierre Seifert und Christoph Krauß: Sovereignty in Information Technology. Security, Safety and Fair Market Access by Openness and Control of the Supply Chain.

Das Arbeitspapier wurde in englischer Sprache verfasst, um zur Internationalisierung der Diskussion offener Wertschöpfungsketten beizutragen. Es ist auf der Website des entsprechenden Projektes „Quattro S: Security, Safety, Sovereignty, Social Product“ verfügbar:

http://www.QuattroS-Initiative.org/

Als „Die Forschungsuniversität in der Helmholtz-Gemeinschaft“ schafft und vermittelt das KIT Wissen für Gesellschaft und Umwelt. Ziel ist es, zu den globalen Herausforderungen maßgebliche Beiträge in den Feldern Energie, Mobilität und Information zu leisten. Dazu arbeiten rund 9 300 Mitarbeiterinnen und Mitarbeiter auf einer breiten disziplinären Basis in Natur-,

Ingenieur-, Wirtschafts- sowie Geistes- und Sozialwissenschaften zusammen. Seine 26 000 Studierenden bereitet das KIT durch ein forschungsorientiertes universitäres Studium auf verantwortungsvolle Aufgaben in Gesellschaft, Wirtschaft und Wissenschaft vor. Die Innovationstätigkeit am KIT schlägt die Brücke zwischen Erkenntnis und Anwendung zum gesellschaftlichen Nutzen, wirtschaftlichen Wohlstand und Erhalt unserer natürlichen Lebensgrundlagen.

Das KIT ist seit 2010 als familiengerechte Hochschule zertifiziert.

Diese Presseinformation ist im Internet abrufbar unter: www.sek.kit.edu/presse.php

Das Foto steht auf https://pixabay.com/de/prozessor-cpu-computer-chip-2217771/ zum Download bereit (CC0 Creative Commons).