Hochschule RheinMain
University of Applied Sciences
Wiesbaden Rüsselsheim

Hochschule RheinMain · Postfach 3251 · 65022 Wiesbaden

Der Präsident
Pressemitteilung

Transparente IT-Produktion für digitale Souveränität

23. März 2018
6/2018

Unsichere Informationstechnik ist eine Gefahr für Bürger, Unternehmen und Staaten. Prof. Dr. Steffen Reith von der Hochschule RheinMain und weitere IT-Experten renommierter Hochschulen und Institute plädieren daher für transparente IT-Produkte.

Ob Automobil-, Energie- oder Finanzsektor: Während Informationstechnik fast alle Bereiche des Lebens zunehmend durchdringt, werden Sicherheitslücken, die sich durch globalisierte Produktionsketten von geschlossenen Hard- und Softwarekomponenten ergeben, immer schlechter kalkulierbar. Zu diesem Ergebnis kommen die 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 zum Thema digitale 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.

Fragile Sicherheit digitaler Infrastrukturen

„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“, so die Diagnose von 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 aktuell Cyberangriffe wie WannaCry, „Trojanische Pferde“ und der unlängst bekannt gewordene Angriff auf die IT-Infrastruktur der 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.

Katrin Bracko
+49 611 94 95-1585

Matthias Munz
+49 611 94 95-1175

presse@hs-rm.de

Unter den Eichen 5
65195 Wiesbaden

www.hs-rm.de

Öffnung der gesamten Wertschöpfungskette

Theoretisch gäbe es die Möglichkeit, Sicherheitseigenschaften von Komponenten und Systemen 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 vorbeigehen, 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.

Mit dem Aufbau von Open-Hardware Communities, die alle Komponenten überprüfen und testen, lassen sich Designfehler oder der Einbau von Hintertüren vermeiden. Allerdings sollten solche Communities hierzu besser organisiert sein 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. 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 RheinMain. Die Konzentration allen Wissens in nur zwei Regionen der Welt und die entsprechende Zentralisierung der Wertschöpfung würden dadurch tendenziell aufgelöst.

Maßnahmen für mehr IT-Souveränität

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

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

Die Hochschule RheinMain

Über 70 Studienangebote an zwei Studienorten mit einem internationalen Netzwerk – das ist die Hochschule RheinMain. Mehr als 13.000 Studierende lernen an den Fachbereichen Architektur und Bauingenieurwesen, Design Informatik Medien, Sozialwesen und Wiesbaden Business School in Wiesbaden sowie am Fachbereich Ingenieurwissenschaften in Rüsselsheim.

www.hs-rm.de | www.facebook.com/HSRheinMain