GESELLSCHAFT
FÜR INFORMATIK

PRESSEMITTEILUNG

GI fordert sicherere IT-Hardware und -Software in Europa

Der Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit" der Gesellschaft für Informatik e.V. (GI) fordert die jahrzehntelange Unsicherheit marktgängiger PC- und Server-Prozessoren endlich zu beenden

Berlin, 28. August 2018 – Der Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit" der Gesellschaft für Informatik e.V. (GI) sieht grundlegende Defizite bei der Informationssicherheit in Europa: Vertraulichkeit, Integrität und auch Verfügbarkeit der Daten von Behörden, Unternehmen und Privatpersonen sind nach wie vor nicht gewährleistet. Zahllose Sicherheitslücken sind Einfallstore für erfolgreiche Angriffe auf Daten und digitale Infrastrukturen.

Prof. Dr. Hartmut Pohl, Sprecher des GI-Präsidiumsarbeitskreises „Datenschutz und IT-Sicherheit", warnt davor, die Erfahrungen der Vergangenheit zu ignorieren: „Die Erkenntnisse der letzten 18 Jahre zeigen, mit welchem Aufwand und Erfolg Spionage und Sabotage in Industrie und Politik international betrieben werden. Dazu zählen etwa der Echelon-Bericht des Europäischen Parlaments (2001), die Enthüllungen Edward Snowdens (2013) und viele weitere. Sie zeigen: Zum Eindringen in IT-Systeme werden nicht nur versehentlich entstandene, sondern auch gezielt eingebaute Sicherheitslücken genutzt: Hintertüren in Software, Firmware und Microcode."

So sind mindestens seit 2009 in den meisten marktgängigen Prozessoren integrierte Mikrocontroller ('engines') verbaut, deren Firmware unzulänglich dokumentiert oder unveröffentlicht ist. Diese Firmware ist komprimiert und signiert und kann unter Umgehung des Hauptprozessors von Dritten – auch bei ausgeschaltetem Computer - aktiviert werden, ohne dass der Anwender etwas davon bemerkt. Die Firmware kann uneingeschränkt auf alle verbundenen Geräte und Komponenten zugreifen und (undokumentiert) Daten verschlüsselt mit dem Internet austauschen. Darüber hinaus tauschen gängige Betriebssysteme permanent Daten mit ihrem Hersteller aus, ohne dass sich dies vollständig unterdrücken lässt. Auch der Inhalt dieser Daten lässt sich nur zum Teil überprüfen.

Somit haben wir es fast immer mit Systemen zu tun,

- die zahlreiche - bekannte und unbekannte - Sicherheitslücken enthalten und
- deren Funktionsumfang also unklar und vom Anwender prinzipiell nicht vollständig kontrollierbar ist.

Prof. Dr. Hartmut Pohl warnt vor den möglichen Folgen dieser Sicherheitsversäumnisse: „Das aktuelle Schadenspotential reicht von der Manipulation demokratischer Wahlen zur politischen Destabilisierung über das Ausspähen von Unternehmensgeheimnissen bis zur Manipulation industrieller Prozesse."

Die Verbesserung der IT-Sicherheitslage erfordert weit mehr als die Veröffentlichung von Sicherheitslücken, die Behörden, Unternehmen oder Privatpersonen bekannt geworden sind. Es reicht auch nicht aus, die Verheimlichung von Sicherheitslücken unter Strafe zu stellen. Solche

reaktiven Maßnahmen sind zwar unverzichtbar; sichere IT-Infrastrukturen können aber letztlich nur durch eine proaktive Vorgehensweise erreicht werden: Hardware, Firmware, System-Software, Anwendungen und Netzkomponenten, Sicherheitssoftware u.a. müssen frei von Sicherheitslücken, insbesondere frei von Hintertüren entwickelt werden.

„Die Bedeutung der IT-Sicherheit ist dem Gesetzgeber zwar grundsätzlich bewusst; mit dem IT-Sicherheitsgesetz ist auch ein erster richtiger Schritt der Absicherung vollzogen. Allerdings werden Geräte und Programme international u.a. von den Herstellern grundlegend (inhärent) mit Sicherheitslücken für Spionage- und Sabotagezwecke ausgerüstet, die Sicherheitsmaßnahmen wirkungslos werden lassen. Dies wird von den Nachrichtendiensten der meisten Staaten und der weltweiten Organisierten Kriminalität seit Jahren zu erfolgreichen Angriffen ausgenutzt.", so Prof. Dr. Hartmut Pohl.

Die Aussichten auf wirksame internationale Vereinbarungen für eine politisch-rechtliche Lösung erscheinen derzeit gering angesichts der auf internationaler Ebene massiv verfolgten geostrategischen Interessen mächtiger Akteure. Nur ein durch angemessene Industriepolitik und volkswirtschaftlich-strategische Maßnahmen vorangetriebener massiver Aufbau und Ausbau eigener Hard- und Softwareherstellung in Deutschland und der EU ermöglicht sicherere Systeme.

Vor dem Hintergrund der aktuellen Lage stellt der Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit" klare Forderungen an die Politik: „Als GI fordern wir massive Anstrengungen zur Erreichung digitaler Souveränität der Bundesrepublik und der in der EU verbundenen Staaten. Das gilt für Behörden, Unternehmen und Privatanwender gleichermaßen. Dazu ist proaktiv eine eigenständige europäische Entwicklung und Produktion sicherer Systeme (Computer: Hardware und Software) unverzichtbar, die vollständig dokumentiert von allen Anwendern nachvollziehbar keine Überwachungsmöglichkeiten enthalten. Damit würde sich Europa darüber hinaus in eine sehr starke Wettbewerbssituation bringen. Insgesamt eine Aufgabe, die gerade vor dem Hintergrund der aktuellen Herausforderungen der EU ein neues Gemeinschaftsgefühl schaffen könnte."