Bundesministerium
für Wirtschaft
und Energie

Trusted Cloud

Trusted Clouds für die digitale Transformation in der Wirtschaft

Teil 4: Von Trusted Clouds zu Trusted-Cloud-Infrastrukturen

4

Impressum

Herausgeber
Bundesministerium für Wirtschaft und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Text und Redaktion
Kompetenzzentrum Trusted Cloud

Gestaltung
A&B One Kommunikationsagentur, Berlin

Stand
Februar 2015

Herausforderungen für die Zukunft

Mit der Digitalen Agenda hat die Bundesregierung deutlich gemacht, dass sie der digitalen Transformation in der Wirtschaft eine überragende Rolle zuordnet und mit ihren Mitteln die deutsche Wirtschaft dabei unterstützen wird. Mit dem Programm Industrie 4.0 ist ein konkretes Vorhaben vorgeschlagen worden, mit dem die deutsche Industrie nicht nur ihre technologische Spitzenstellung verteidigen kann, sondern mit einem Quantensprung in der Technologieentwicklung auch neue Maßstäbe im globalen Wettbewerb setzen will. Die exponentiell zunehmende Vernetzung unterschiedlichster Objekte und die grenzüberschreitende Kollaboration in Ökosystemen stellen ganz neue Herausforderungen dar. Vor dem Hintergrund zunehmender Bedrohungen für existierende Informations- und Kommunikationsinfrastrukturen kommt dabei der Sicherheit dieser Infrastrukturen und der über sie verfügbar werdenden Daten eine entscheidende Rolle zu.

Die gegenwärtige Diskussion über die Sicherheit von Anwendungen der Informations- und Kommunikationstechnologien ist durch eine große Betroffenheit gekennzeichnet. Dies ist eine Seite der Medaille. Die andere Seite der Medaille lässt erkennen, dass das Thema zwar für relevant, ja sogar für kritisch gehalten wird, aber nicht immer Anlass für entsprechendes Handeln ist. Dies gilt nicht nur für den Bürger als Konsumenten, sondern häufig auch für Unternehmen. Es wird sogar vermutet, dass Sicherheitsprobleme an vielen Stellen sichtbar werden und entsprechende Verletzungen der Sicherheit stattfinden, diese aber nicht notwendigerweise öffentlich werden, weil die Betroffenen einen Imageschaden befürchten müssen. Es wird von einer signifikanten Dunkelziffer gesprochen.

Mit seinem Förderprogramm Trusted Cloud hat das Bundesministerium für Wirtschaft und Energie einen wichtigen Aspekt der digitalen Transformation, das Thema „Vertrauen“, in das Bewusstsein der Fachöffentlichkeit und der Öffentlichkeit insgesamt gebracht. Während im Rahmen des Programms die zukünftige Bereitstellung von vertrauenswürdigen Leistungen der Informations- und Kommunikationstechnologien durch Dienste aus einer Cloud im Mittelpunkt der Betrachtung stand, sind andere Aspekte, wie z. B. die vertrauenswürdige Kommunikation zwischen dem Endnutzer und der Cloud, nicht betrachtet worden. Dass auch deren Vertrauenswürdigkeit sichergestellt sein muss, ist offensichtlich, denn jede Kette ist nur so stark wie ihr schwächstes Glied.

Das Internet mit seinem durchschlagenden Erfolg für die mögliche globale Kommunikation ist nun auch der technologische Kandidat für die Kommunikation in sicherheitskritischen Anwendungen. Die mit der Einbettung sicherheitskritischer industrieller Systeme in das weltweite, durch das Internetprotokoll (IP) gesteuerte Internet entstehenden Sicherheitsrisiken sind in den letzten Jahren mehr als deutlich geworden. Sie sind nunmehr auch der Anlass dafür, über vertrauenswürdige Kommunikation in kritischen Anwendungen wie z. B. Industrie 4.0 neu nachzudenken.

Ergebnis dieser Überlegungen sind Vorschläge zur Entwicklung alternativer – und hoffentlich vertrauenswürdigerer – Kommunikation. Dabei ist davon ausgegangen worden, dass die grundlegend neue Entwicklung der Kommunikationstechnologien keine ernst zu nehmende Perspektive sein kann, sondern dass mit den heute und in absehbarer Zeit verfügbaren Technologien vertrauenswürdige Lösungen geschaffen werden müssen. Die verfolgten Ansätze sind demzufolge eher technisch-organisatorische Konzepte neben den technischen Konzepten, mit denen der jeweils erforderliche Grad an Vertrauenswürdigkeit hergestellt werden kann. Dazu wird der Gedanke des globalen, aus Nutzersicht uniformen Internets wieder stärker an dem orientiert, was auch schon heute – aus technischer Sicht – die Realität des Internets darstellt: die Betrachtung des Internets als ein „Netz der Netze". Schon heute werden – und dies dank des Internetprotokolls – zwischen den verschiedenen auch technologisch heterogenen physikalischen Netzen „Brücken" geschaffen, über die letztlich die globale Kommunikation ermöglicht wird. Auch für die Kommunikation in cyberphysikalischen Ökosystemen werden sehr unterschiedliche Systeme und Anlagen mit ihren jeweils eigenen Kommunikationskonzepten zu grenzüberschreitenden Kommunikationsinfrastrukturen verbunden werden müssen.

Diese Frage stellt sich – vor dem Hintergrund der nunmehr stattfindenden flächendeckenden und hochgradig vernetzten Nutzung von Informations- und Kommunikationstechnologien in kritischen Infrastrukturen z. B. für die Energieversorgung, das Gesundheitswesen, für Transport, Waren- und Personenverkehr und vor dem Hintergrund der exponentiell zunehmenden Bedrohungen – verändert, um nicht zu sagen ganz neu. Dazu ist es nötig, alle Komponenten und Systeme der Informations- und Kommunikationstechnologien in ihren jeweiligen Nutzungen ganzheitlich zu betrachten. Weil in der Zwischenzeit aber deren Vernetzung global ist, entziehen sich viele Bereiche dieser globalen Infrastruktur entsprechenden Sicherheitsanalysen. Dies kann dennoch nicht der Anlass für die Vernachlässigung der Analysen und für einen Verzicht auf Präventionsmaßnahmen sein.

Neben den oben erwähnten „versteckten" Sicherheitsrisiken sind in den Informations- und Kommunikationstechnologien auch „offene" Sicherheitsrisiken „fest eingebaut". Dies wird bei näherer Betrachtung schon bei der Hardware – also bei den Basistechnologien – offensichtlich, denn viele der heute verfügbaren Hardwaresysteme (zusammen mit den die Hardwarenutzung steuernden Mikro-Codes) sind nicht sicherheitstechnisch, sondern leistungstechnisch optimiert entwickelt worden. Zusammen mit der auf den jeweiligen Hardwaresystemen installierten Betriebssoftware (Betriebssysteme, Treiber etc.) und der jeweiligen Anwendungssoftware sind weitere nicht sicherheitsoptimierte Systeme in Betrieb, die der fortlaufenden Pflege und Wartung und Aktualisierung bedürfen. Für all dies werden in vernetzten Umgebungen die in den Systemen eingebauten „Backdoors" genutzt, über die normalerweise kontrolliert Updates an die jeweiligen Systeme „eingespielt" werden können, die häufig aber auch missbräuchlich genutzt werden können.

Andererseits ist die kontinuierliche Betriebsbereitschaft der Hardware-/Softwaresysteme davon abhängig, dass die permanente kommunikative Verbindung zwischen der Technologie des Nutzers und der Technologie des Herstellers sichergestellt ist. Diese Verbindung wird über das Internet ermöglicht, und damit beginnt das Sicherheitsproblem, ein ganzheitliches Problem für Informations- und Kommunikationstechnologien zu werden. Da Kommunikationsinfrastrukturen und damit auch das Internet nicht der jeweiligen nationalen Jurisdiktion unterworfen sind, verliert der Nutzer von Hardware-/Softwaresystemen in seinen Anwendungen einen Teil seiner Souveränität. Für den Fall, dass auch die Sicherheit des Internets selbst illegal bedroht wird, wird die kommunikative Kopplung zwischen Nutzer und Hersteller, aber auch die kommunikative Kopplung zwischen verschiedenen Nutzern zum Risiko für alle Beteiligten.

Die geschilderten Probleme sind der Anlass dafür, eine über das Trusted-Cloud-Programm hinausgehende Initiative vorzuschlagen: die Entwicklung von ganzheitlichen „Trusted-Cloud-Infrastrukturen“.

www.bmwi.de