Der Standard

Ein Vorhängeschloss für die Cloud

Wann können Systeme, die miteinander kommunizieren, als vertrauenswürdig bezeichnet werden? Forscher der FH Burgenland beschäftigen sich mit dem Securityaspekt der digitalen Industrie.

5 Dez. 2018 Alois Pumhösel

Damit alles gut läuft für die IT-Anwendungen der modernen Industrie, wird Sicherheit in der Cloud messbar gemacht.

Wenn man Gemüse in der Stadt produzieren möchte, braucht man dafür Platz. Ein Konzept dafür ist sogenanntes Vertical Farming: Pflanzen werden dabei in Bahnen neben- und übereinander gezogen. Roboterarme rasen hin und her und versorgen die Wurzeln auf Basis von Sensordaten mit Nährstoffen und Wasser. Das Licht wird ebenso datengetrieben gesteuert. Im Projekt AgriTec 4.0, bei dem die FH Burgenland, Forschung Burgenland, das Austrian Institute of Technology (AIT) und das Unternehmen Phytonik kooperieren, möchte man die Mittel der Digitalisierung auf die Produktion von Gemüse oder Pharmazieplanzen anwenden.

Bei der Etablierung von digitalisierten Produktionssystemen – egal ob sie nun der Herstellung von Autos oder Gemüse dienen – muss Sicherheit von Anfang an mitgedacht werden. „Die Angreifer haben es vielleicht nicht auf einen konkreten Industrieroboter abgesehen – obwohl das auch passieren kann", erklärt Markus Tauber vom Research Center for Cloud & Cyber Physical Systems Security der FH Burgenland. „Wahrscheinlicher ist aber ein Angriff auf die Infrastruktur mit dem Ziel, Rechenkapazitäten abzuziehen, also sogenannte Botnets zu schaffen." Berühmt wurde etwa die Schadsoftware Mirai, die 2016 die Sicherheitslücken in hunderttausenden mit dem Internet verbundenen Geräten vom Router bis zur Kamera ausnutzte, um gezielt Angriffe gegen Webseiten auszuführen.

Vertrauenswürdige Sensoren

Ein Fokus in der Arbeit von Tauber – er ist auch bei dem kürzlich gestarteten AgriTec-4.0-Projekt mit an Bord – liegt darin, für mehr Sicherheit in den Internetof-Things- und cloudbasierten Systemen der Industrie 4.0 zu sorgen. Unter anderem ist er, wiederum gemeinsam mit dem AIT und mit mehr als 100 weiteren Partnern an dem Projekt Productive 4.0 beteiligt, das aktuell zu den größten in diesem Bereich zählt. In dessen Rahmen konzentrieren sich die Forscher aus dem Burgenland auf eine sichere Kommunikation innerhalb der digitalisierten Produktionssysteme.

„Wenn ein Temperatursensor mit einem System, das die Temperatur regelt, kommuniziert, soll sichergestellt werden, dass sich die beiden vertrauen können", gibt Tauber ein Beispiel. „Wir arbeiten an einer Art Werkzeugkasten für cyberphysikalische Systeme, durch den die Komponenten auf Basis von Zertifikaten eindeutig identifiziert werden können. Das ist etwa relevant, wenn Bauteile ausgetauscht werden. Es wird geprüft, ob der neuen Hardware vertraut werden kann." Der Werkzeugkasten wird als OpenSourceProjekt Arrowhead veröffentlicht.

Daneben tragen Tauber und Kollegen auch zum Projekt Semi 4.0 bei, das wie Productive 4.0 vom Halbleiterhersteller Infineon koordiniert wird. Die Projekte, in denen auch Studierende des Studiengangs Cloud Computing Engi- neering an der FH Burgenland beteiligt sind, werden von den Förderschienen EU Ecsel Joint Undertaking und IWB-EFRE unterstützt.

In Semi 4.0 arbeiten die Forscher daran, die – zumindest formale – Sicherheit eines Gesamtsystems besser messbar zu machen. Die Frage, ob in den IT-Systemen allgemeine Sicherheitsstandards eingehalten werden, soll auf automatisierten Wegen beantwortet werden.

Standards erfüllen

Ist die Firmware – also die Basissoftware – der Geräte auf aktuellem Stand? Wie werden mobile Datenträger wie USB-Sticks gemanagt? Verlangt das System starke Passwörter? – In entsprechenden Compliance-Standards wird eine Vielzahl solcher Regeln vorgegeben. Tauber und seine Kollegen erstellen „Agents", das sind kleine Programmskripts, die diese Fragen für die jeweiligen Systeme beantworten und in ein einfaches Ergebnis zusammenfassen. „Man kann dann etwa ablesen, dass ein System 75 Prozent aller relevanten Indikatoren erfüllt", erklärt Tauber. In der Praxis könnte ein derartiges Continous-Security Compliance-System etwa für verlässliche Einhaltung von Sicherheitsstandards entlang einer ganzen Lieferkette sorgen. Die Wahrscheinlichkeit, dass die gelieferten Waren kompromittiert sind, sinkt damit – auch in rechtlicher Hinsicht ein wichtiger Faktor.

Sicherheit kostet – auch in der Industrie 4.0. Je niedriger das Sicherheitsrisiko sein soll, desto höher der Aufwand an Geld und Zeit. Welcher Aufwand ist also vertretbar? Welches Risiko nimmt man in Kauf? Jedes Unternehmen muss hier seine Balance finden. Im Projekt MIT 4.0 – auch hier ist Tauber mit an Bord – versuchen die Forscher den Aufwand für das Erfüllen von Compliance-Standards zu beschreiben und zu beziffern. Tauber: „Auf der einen Seite versuchen wir, die Sicherheit eines Systems messbar zu machen, auf der anderen Seite beantworten wir auch die Frage: Was kostet das?"