IT-Sicherheit aus dem Werkzeugkasten

Die Fabrik der Zukunft muss effizient und intelligent sein – und vor allem sicher

Für das Smartphone lädt man sich neue Zusatzfunktionen einfach und bequem aus dem App-Store. Schon bald kann der Unternehmer der Zukunft seine Maschinen auf die gleiche Weise mit neuen Datensätzen versorgen. Die Daten werden aus dem Technologiedatenmarktplatz heruntergeladen – eine Art App-Store für die Industrie 4.0.

Genau wie bei Smartphones eröffnet der „App-Store der Industrie 4.0“ ein ganz neues Geschäftsmodell: Früher mussten Datensätze für Maschinen analog bezogen werden. In der Industrie 4.0 gibt es dafür den Technologiedatenmarktplatz, in dem Zusatzfunktionen für die vernetzten und intelligenten Maschinen digital heruntergeladen werden können. Daher werden Industrieunternehmen von morgen neben den klassischen Produkten auch verstärkt Service-Dienstleistungen anbieten, die der Kunde je nach Bedarf zu seinen Maschinen dazu kaufen kann.

Wie in allen Bereichen, in denen Vernetzung und Digitalisierung eine große Rolle spielen, stellt sich die Frage nach der IT-Sicherheit. Die Antworten für die vernetzten Fabriken der Zukunft will IUNO finden, das Nationale Referenzprojekt zur IT-Sicherheit in Industrie 4.0.

Welche tragende Rolle IT-Sicherheit in der virtuellen Fabrik spielt, fasst Reiner Anderl, Professor am Fachbereich Maschinenbau der TU Darmstadt und Sprecher von IUNO, zusammen: „Durch die Digitalisierung in der Produktentwicklung entstehen hochsensible Daten über neue, innovative Produkte in vernetzten Industrieanlagen – es wäre eine Katastrophe, wenn diese Daten durch Cyberangriffe oder Spionage entwendet würden.“ Deswegen beschäftigen sich die Forscherinnen und Forscher im Nationalen Referenzprojekt damit, wie man Daten, die in der Industrie 4.0 anfallen, sicher aufbewahren kann. Wenn mehrere Personen mit den Daten arbeiten, müssen beispielsweise die Zugriffsrechte sicher definiert sein. Auch die Datenströme – innerhalb und außerhalb der Unternehmen – müssen abgesichert und verschlüsselt werden.

Schon früh war Professor Anderl klar, dass IT-Sicherheit im Maschinenbau eine große Rolle spielen wird: „Cybersicherheit mitzudenken lag in der Natur der Sache, als man die Zeichenbretter abgeschafft und die rechnergestützte Konstruktion eingeführt hat.“ Über ein Viertel seiner wissenschaftlichen Mitarbeiter arbeiten daher am drängenden Thema IT-Sicherheit in der Industrie 4.0.

Doch was bedeutet Industrie 4.0 eigentlich konkret? Der Begriff bezeichnet die vierte industrielle Revolution, welche die Produktion mit modernster Kommunikationstechnik verzahnt. Anhand intelligenter, digital vernetzter Systeme wird eine verbesserte Wertschöpfung in der Produktion möglich. Die Unternehmen profitieren von effizienten und hochflexiblen Produktionsprozessen, die individuelle Kundenanforderungen zu Kosten der Massenfertigung erfüllen können.

Aufgabe des IUNO-Projekts sei es nun, die IT-Sicherheit und auch eine neue Sicherheitskultur in der Industrie 4.0 zu etablieren, erklärt Professor Anderl. Die Themenfelder sind dabei sichere Prozesse, sichere Daten und sichere Dienste und gleichzeitig eine sichere Vernetzung aller dieser Komponenten.
Die Wissenschaftlerinnen und Wissenschaftler forschen an wichtigen Grundlagen der IT-Sicherheit, die speziell in der Industrie 4.0 benötigt werden, zum Beispiel dem Identitätsmanagement oder der Anomalieerkennung. In anderen Fällen sorgen sie aber auch dafür, dass bereits bestehende Sicherheitstechnologien den Weg in die Industrie finden. Anhand von sogenannten Anwendungsszenarios werden die Forschungsergebnisse dann auf reale Situationen in der Praxis angewendet. Am Ende des Projekts, also 2018, steht den Unternehmen der Industrie 4.0 so ein „Werkzeugkasten" zur Verfügung, mit allgemein anwendbaren Lösungen für Herausforderungen der IT-Sicherheit in intelligenten Fabriken. Damit der Transfer der Forschungsergebnisse in die mittelständische Wirtschaft gelingt, arbeiten neben der TU Darmstadt sechs weitere Forschungseinrichtungen und Universitäten zusammen mit auch 14 Unternehmen der deutschen Industrie im IUNO-Projekt zusammen.

„In der Fertigungsindustrie herrscht ein gigantischer Bedarf an Konzepten für Sicherheitskulturen", stellt Anderl klar, denn bisher seien IT-Sicherheitskonzepte nur in sehr geringem Maße eingeführt worden. Er kritisiert das in der Vergangenheit fehlende Bewusstsein: „Die Fertigungsindustrie hat jetzt erst verstanden, dass man sich um die Sicherheit der Systeme grundlegend kümmern muss – etablierte Sicherheitskonzepte, wie eine Firewall und Passwort-Richtlinien, reichen nicht aus. IT-Sicherheit muss deutlich darüber hinausgehen". Ein weiteres Ziel von IUNO ist es daher, das Bewusstsein für die Notwendigkeit von IT-Sicherheit und ganzheitlichen Sicherheitskonzepten zu schaffen.

Die Idealvorstellung sei natürlich „Security by Design", die Umsetzung und Berücksichtigung von IT-Sicherheit schon im Entwicklungsprozess, so Anderl: „Meine große Hoffnung ist es, dass die Systeme der Zukunft nicht mehr ohne eingebaute IT-Sicherheit hergestellt werden." Natürlich sei es nicht möglich, alle Maschinen auf einmal auszutauschen, daher betont er auch: „Das Nachrüsten von IT-Sicherheit für bestehende Systeme ist auf jeden Fall möglich." Dabei spiele in vielen Unternehmen im Moment die Kostenfrage noch eine große Rolle – doch die Kosten-Nutzen-Rechnung für IT-Sicherheit falle in jedem Fall positiv aus, ist sich Professor Anderl sicher: „In fünf Jahren wird die Fertigungsindustrie völlig anders aussehen."

Zur Person

Professor Reiner Anderl leitet das Fachgebiet „Datenverarbeitung in der Konstruktion“ am Fachbereich Maschinenbau der Technischen Universität Darmstadt und ist Sprecher von IUNO, dem Nationalen Referenzprojekt IT-Sicherheit in der Industrie 4.0, und Mitglied von CYSEC, dem Profilbereich Cybersicherheit der TU Darmstadt.

IUNO - Das Nationale Referenzprojekt IT-Sicherheit in der Industrie 4.0

IUNO betrachtet reale und in der Industrie 4.0 relevante Szenarien aus der produzierenden Industrie. Anhand von vier Anwendungsfällen werden Bedrohungen und Risiken für die intelligente Fabrik identifiziert, Schutzmaßnahmen entwickelt und exemplarisch an Demonstratoren umgesetzt. Ziel des Projekts ist es, möglichst allgemein verwendbare Lösungen für Herausforderungen der IT-Sicherheit im industriellen Anwendungsfeld zu entwickeln. Die getesteten und übertragbaren IT-Sicherheitslösungen können besonders von den kleinen und mittelständischen Unternehmen als „Blaupause“ für die sichere Industrie 4.0 herangezogen werden.

IUNO wird vom Bundesministerium für Bildung und Forschung mit einem Projektvolumen von 33 Millionen Euro gefördert.

CYSEC – Der Profilbereich Cybersicherheit der TU Darmstadt

Am Profilbereich CYSEC (Cybersecurity [at] TU Darmstadt) sind mehr als 30 Fachgebiete aus acht Fachbereichen beteiligt und forschen an zentralen Themen der Cybersicherheit und des Privatheitsschutzes. International anerkannte Spitzenforschung in zahlreichen Bereichen der Cybersicherheit und die Ausbildung von Experten für IT-Sicherheit sind Kernkompetenzen von CYSEC. Technologietransfer über nationale und internationale Kooperationen mit außeruniversitären Forschungseinrichtungen und industriellen Partnern runden das Profil von CYSEC ab.

Kontakt

CYSEC - Profilbereich Cybersicherheit der TU Darmstadt
Ann-Kathrin Braun, Wissenschaftskommunikation, akbraun@cysec.tu-darmstadt.de, 06151 / 16-22662