Strategische Ausrichtung für den Schutz von IoT-Systemen

Wie das US-Verteidigungsministerium kritische Infrastrukturen schützen will – und welche Schlüsse IT-Fachleute daraus ziehen können.

Michael Kallus

Sie gilt als eine der technologisch führenden Organisationen – dabei beschäftigt sie selbst nur 140 Fachleute. Aber diese Experten engagieren universitäre, militärische und industrielle Forschungseinrichtungen und verbinden deren exzellente Mitarbeiter miteinander. Diese Vernetzung wurde oft beschrieben als „100 Genies, die von einem Reisebüro verbunden sind".

Das Reisebüro ist die DARPA, die Defense Advanced Research Projects Agency. Sie investiert im Auftrag des US-Verteidigungsministeriums in Forschungsprojekte, die im Interesse der Nationalsicherheit liegen, und fördert dabei Innovationen in beinahe jedem Feld – von Biologie über Mikroelektronik bis hin zu unbemannten Fluggeräten. Auf diese Weise schuf die DARPA die Grundlagen für das Internet. Sie hatte Ende der 60-er Jahre Forscher zusammengezogen, die das Arpanet entwickelten, aus dem später das Internet hervorging.

Zu ihren Aufgaben gehört auch, kritische Infrastrukturen wie Krankenhäuser oder Industrieanlagen zu sichern. Daher hat die DARPA Ende 2016 Underwriters Laboratories (UL) beauftragt, ein Forschungs- und Prüfunternehmen, die Cyber Security von IoT-Gateways für industrielle Steuerungssysteme zu erforschen.

„Unser Auftrag ging über neun Monate", berichtet Alexander Köhler, Business Development Manager bei UL Cyber Security. Um alle Anforderungen zu überblicken, hatte das Cyber Security Team von UL die gesamte IoT-Architektur im Fokus, also sämtliche Software von Micro-Chips, den Komponenten und Systemen. „Wir haben strukturierte Penetration-Tests durchgeführt und untersucht, wie Systeme auf Remote-Geräte zugreifen und Software-Updates durchführen", erzählt Köhler.

Warum der Lifecycle in IoT essentiell ist

Durch diese Forschung erkennt UL früh, in welche Richtung sich IoT-Systeme aktuell entwickeln. Ein wesentlicher Punkt dabei ist die Betrachtung des Lebenszyklus. Wurde etwa ein Algorithmus in einem Produkt gehackt, muss es getauscht werden. „Ein Komponentenlieferant muss also frühzeitig die Entwicklung eines neuen Produkts betrachten und in seinen Prozessen definiert haben, was bei Produkteinstellung mit den Anlagen passiert, wo es eingesetzt wird", erläutert Köhler.

UL ist dazu auch der Partner, der die Werkzeuge anbieten wird. „Eine UL 2900-Norm prüft, ob der Komponentenhersteller Prozesse zum Lifecycle-Management implementiert hat", berichtet Köhler. So lassen sich Hersteller identifizieren, die diese Verantwortung übernehmen. Ein weiteres Beispiel: Die Normenreihe IEC 62443 bietet Kriterien, um sichere Prozesse und Produktentwicklung herzustellen. Die UL 2900-2-2 ist darauf ausgelegt, diese Sicherheitskriterien aus IEC 62443 auf Produkte und Systeme anzuwenden.

Die UL 2900-2-2 präzisiert die Anforderungen u.a. derart, dass zertifizierbare Prüfungen von Komponenten jetzt durchgeführt werden können.

Solche Services unterstützen IT-Verantwortliche, die neue Prozesse benötigen, um auf Veränderungen am Produkt reagieren zu können. „Wir erwarten hier ein entsprechendes Maß an Automatisierung, um IoT-Geräte zu managen", so Köhler. „IT-Verantwortliche benötigen heute ein stetes Monitoring ihrer IoT-Landschaft."

Strategische Empfehlungen aus dem DARPA-Projekt

In seinen Tests verfolgt UL über längere Zeit, wie sich Patches für Komponenten und Steuerungs-Software auf die Sicherheit von IoT-Systemen auswirken. „Das ist Teil unserer Risikoanalyse, auch Updates müssen cyber-sicher sein", erläutert Köhler. Das Patch-Management ist ebenfalls ein Bestandteil der UL-Norm 2900 und regelt, wie ein Komponentenhersteller damit umgehen muss.

Mit der Sicherung von cyberphysischen Systemen beschäftigt sich UL schon seit zehn Jahren. Um diese Anstrengungen zu bündeln, hat das Unternehmen sein Cyber Assurance Program (CAP) initiiert. Es untersucht Risiken von Industrie-4.0-Systemen u.a. in den Bereichen Automobil, Fabrikautomation, Medizin und Beleuchtung und setzt auf die UL 2900-Normenreihe auf.

Vor dem Hintergrund dieser Forschungstätigkeit wird deutlich, warum sich UL als ein globales Unternehmen im Bereich der Sicherheitswissenschaft versteht. „Für uns ist das Projekt mit DARPA eine Anerkennung für das Know-how von UL im Bereich Cyber Security", resümiert Ingo Rübenach, Vice President, UL DACH & Eastern Europe. „Und es zeigt, dass wir mit unserer Forschung dazu beitragen, Industrie 4.0 mit Leben zu füllen."

germany.ul.com/industrie-4.0

INDUSTRIE 4.0 REALISIERBAR MACHEN

„Betrachtet man alle die Felder, auf denen durch IoT neue Technologien hervorgehen, dann stehen uns revolutionäre Umwälzungen bevor. In der Fabrik von morgen sind die Lieferketten durchgängig und transparent und neue Services mit künstlicher Intelligenz gestalten die Produktion hocheffizient, Stichwort Advanced Manufacturing. Aber viele Perspektiven müssen noch beleuchtet werden. Das fängt bei Cyber Security an, geht weiter mit Interoperabilität und reicht bis zur Mensch-Maschine-Kommunikation, welche die Sicherheit am Arbeitsplatz in ein neues Licht rückt. In all diesen Fällen ist Sicherheit ein Kern des Umsetzungsprozesses. Unsere Mission dabei: UL will Industrie 4.0 realisierbar machen."
Ingo Rübenach, Vice President, DACH & Eastern Europe, UL International Germany GmbH

Ingo Rübenach
Vice President,
DACH & Eastern Europe,
UL International Germany GmbH
T: +49 69 489810 291
E: Ingo.Ruebenach@ul.com