Sichern Sie Ihr IoT-Geschäftsmodell

Wie das US-Verteidigungsministerium kritische Infrastrukturen schützen will – und was deutsche Unternehmen daraus für ihre IoT-Plattformen lernen.

Michael Kallus

Es war eine US-Behörde, welche die Grundlagen für das Internet schuf. Sie hatte Ende der 60-er Jahre Forscher zusammengezogen, die das ARPANET entwickelten, aus dem später das Internet hervorging. Diese Behörde 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 technische Innovationen - von Biologie über Mikroelektronik bis hin zu unbemannten Fluggeräten.

Zu ihren Aufgaben gehört auch, kritische Infrastrukturen wie Krankenhäuser oder Industrieanlagen vor Cyber-Risiken zu sichern. Daher hat die DARPA Ende 2016 UL (Underwriters Laboratories) beauftragt, ein globales Forschungs- und Prüfunternehmen, die Cyber Security von IoT-Gateways für industrielle Steuerungssysteme zu erforschen. Diese Gateways verbinden IoT-Komponenten mit dem Internet und sind ein kritisches Element in IoT-Umgebungen.

Den ganzen IoT-Stack im Blick

„Unser Auftrag ging über neun Monate“, berichtet Heike Thomas, Business Development Manager, Automation, bei UL in Deutschland. 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 ferngesteuerte Geräte zugreifen und Software-Updates durchführen“, erzählt Heike Thomas. Aus diesen Untersuchungen leiten die Ingenieure wissenschaftlich-basierte, reproduzierbare Testkriterien ab und entwickeln Prüfmethoden für IoT-Gateways. UL’s Ziel ist es, daraus einen Cyber Security Standard spezifisch für die Software von industriellen IoT-Gateways zu entwickeln.

Durch diese Forschung erkennt UL früh, in welche Richtung sich IoT-Systeme aktuell entwickeln. „Dieses Wissen hat sich auch im deutschen Markt bewährt, in dem wir seit fast 20 Jahren tätig sind“, berichtet Thomas. Zu den Kunden, die UL in Sachen Cyber Security unterstützt, gehören große Unternehmen.

Viele deutsche Unternehmen planen gerade, ihre Produktion mit einer IoT-Plattform zu vernetzten, oder bauen sie schon. „Und viele haben Bedenken, ihre IoT-Projekte würden durch steigende Sicherheitsanforderungen zu komplex“, berichtet Heike Thomas. „Wer sich jedoch durch Standards darauf verlassen kann, dass seine Komponenten eine hohe Cybersicherheit besitzen, kann sich auf umfassendere Sicherheitskonzepte konzentrieren wie beispielsweise Network Behavior Analysis, Honeypots oder zentrale Protokollierung - und so eine Defense-in-Depth-Sicherheitsstrategie entwickeln.“

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

Derzeit wird Cyber Security auf der Komponenten-Ebene stark diskutiert. „Es ist eine große Herausforderung, die unterschiedlichen Anwendungsbereiche und geographische Diversität der Komponenten zu überblicken“, erläutert Heike Thomas. „Sind die Komponenten auf Cybersicherheit zertifiziert, reduziert das deutlich die Komplexität.“

Strategische Empfehlungen aus dem DARPA-Projekt

„Wir empfehlen Unternehmen, ihre vorhandene Sicherheitsrichtlinien und Best Practices in den Produktlebenszyklus einzubinden, um auch Wartung und Support in die Security-Bemühungen zu integrieren“, erläutert Thomas. In der Praxis bewährt hat sich, auszuarbeiten, wie Angriffe auf IoT-Systeme aussehen können, indem man Bedrohungsszenarien modelliert und simuliert. „So lassen sich Risiken besser verstehen und daraus Schutzmechanismen entwickeln“, erklärt Thomas.

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 hohe 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 all 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 – angefangen von Cyber Security, bis hin zu Interoperabilität und 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