Von wegen „smart“: Wo hapert’s noch im IoT?

München, 02.12.2019: Einen Smart TV hat heute schon fast jeder im Haus: Das Fernsehgerät verbindet sich mit dem heimischen WLAN und bietet so neben dem TV-Programm auch noch praktische Apps zum Streamen und Einkaufen. Genau wie im Wohnzimmer fasst auch im industriellen Sektor das Internet der Dinge (IoT) Fuß: Zum Beispiel kommunizieren in Fabriken Geräte miteinander, um Produktionsnachschub zu gewährleisten.[1]

Doch Unternehmen sehen sich bei der Umsetzung von IoT-Projekten mit komplexen Herausforderungen konfrontiert. Eines der größten Hemmnisse stellen in Deutschland Bedenken hinsichtlich der IT-Sicherheit dar – zu diesem Ergebnis kommt eine Studie der International Data Corporation (IDC).[2] Zwar hält fast ein Drittel der befragten Unternehmensvertreter IoT-Integration für eine geschäftskritische Entwicklung, ein nahezu ebenso großer Teil hat allerdings ernsthafte Vorbehalte und sorgt sich um Datenschutz und Datensicherheit im Internet der Dinge.

IT-Security-Experte Dr. Hubert Jäger von der Münchner TÜV SÜD-Tochter uniscon GmbH kann die Bedenken der Anwender nachvollziehen. Er sieht in puncto IoT-Sicherheit derzeit vor allem drei große Baustellen: „Unsichere Geräte, fehlende Transparenz und privilegierten Zugriff.“

IoT: Das Internet der unsicheren Geräte?

„Das IoT ist in seinem derzeitigen Zustand geradezu eine Einladung zu Sicherheitsverletzungen“, sagt Jäger: Jedes Gerät, das die Anwender ins Netzwerk bringen, könnte ein potenzieller Einstiegspunkt für Cyberkriminelle sein. Schon der Smart TV kann zum Problem werden, etwa wenn sich Hacker über im Gerät gespeicherte Daten Zugang zum heimischen WLAN verschaffen. In der Industrie, wo in der Regel eine Vielzahl von IoT-Geräten miteinander verknüpft sind, multipliziert sich dieses Risiko dementsprechend.

Wie Unternehmen Datenflüsse kontrollieren

Für die Verunsicherung der Anwender macht Jäger indes vor allem mangelnde Transparenz verantwortlich: „Es muss klar ersichtlich sein, welche Daten ein Gerät erhebt und speichert und was mit diesen Daten geschieht.“ Wenn also der Smart TV ein Nutzerprofil erstellt und auswertet, muss der Nutzer das erfahren und gegebenenfalls widersprechen können. Analog dazu müssen Industrieunternehmen die Datenflüsse von IoT-Geräten kontrollieren können und verhindern, das wertvolle oder sensible Daten in unbefugte Hände kommen. Jäger: „Unternehmen setzen bei der Übertragung und Verarbeitung von Daten aus IoT-Anwendungen häufig auf eigene Rechenzentren, seltener auf Cloud-Angebote aus dem Netz.“ Dabei würden die Unternehmen bewusst auf Geschäftsvorteile verzichten, die Cloud-Anwendungen mit sich brächten.

Einfallstor „privilegierter Zugriff“

Der Gedanke dahinter sei, so Jäger, dass Unternehmen die Daten im eigenen Rechenzentrum besser im Griff behalten und die Datensicherheit eher gewährleisten könnten. „Das stimmt allerdings nur bedingt.“ Denn genau wie in der Cloud würden Daten im eigenen Rechenzentrum zwar verschlüsselt übertragen und gespeichert, „liegen aber zur Verarbeitung unverschlüsselt und damit quasi ungeschützt auf den Servern vor“.

---

[1] https://industrie-wegweiser.de/internet-der-dinge-iot/

[2] https://www.idc.com/getdoc.jsp?containerId=prEUR145546419

Cyberkriminelle könnten sich Zugang zu diesen Daten verschaffen, indem sie beispielsweise privilegierte Nutzerkonten, wie sie etwa für Administratoren vorgesehen sind, ausnutzen. Erschwerend kommt hinzu, dass bei vielen Unternehmen Unklarheit herrscht, welche privilegierten Benutzerkonten es überhaupt gibt und wo sich diese im Unternehmen befinden.

Eine sichere Cloud als Basis für IoT-Plattformen?

„Der Mensch ist nach wie vor einer der größten Risikofaktoren in der IT-Sicherheit“, betont Jäger. Doch mittlerweile gibt es IT-Infrastrukturen, die Verarbeitungsserver mit rein technischen Maßnahmen schützen und den privilegierten Zugriff durch Administratoren oder Mitarbeiter vollständig ausschließen: „Diese „Versiegelung“ genannte Technologie ist beliebig skalierbar und lässt sich auch auf ganze Rechenzentren ausweiten“, sagt Jäger. „So lassen sich damit auch Cloud-Angebote realisieren, mit denen nicht nur IoT-Anwendungen rechtskonform umsetzbar sind, sondern auch andere sicherheitskritische Applikationen, etwa aus den Bereichen RegTech und eHealth.“

Als Beispiel nennt Jäger uniscons sealed platform, die Anfang des Jahres mit dem Deutschen Rechenzentrumspreis in der Kategorie „Innovationen im Whitespace“ ausgezeichnet wurde[3]. „Mit dieser hochsicheren Cloud-Plattform als Basis für ihre IoT-Plattformen haben Industrieunternehmen sensible Daten jederzeit zuverlässig im Griff – egal, ob diese in der Cloud oder im eigenen Rechenzentrum liegen“, sagt Jäger. Und sind die Sicherheitsbedenken erst einmal aus der Welt geschafft, können sich die Unternehmen auf ihre Kernkompetenzen konzentrieren – und auf die Entwicklung neuer, innovativer IoT-Angebote.

uniscon – ein Unternehmen der TÜV SÜD Gruppe

Die uniscon GmbH ist ein Unternehmen der TÜV SÜD Gruppe. Als Teil der Digitalisierungsstrategie von TÜV SÜD bietet uniscon hochsichere Cloud-Anwendungen und Lösungen für sicheren und gesetzeskonformen Datenverkehr. TÜV SÜD ist ein weltweit führendes technisches Dienstleistungsunternehmen mit über 150 Jahren branchenspezifischer Erfahrung und heute mehr als 24.000 Mitarbeitern an etwa 1000 Standorten in 54 Ländern. In diesem starken Verbund ist uniscon in der Lage, mit der Sealed Cloud und ihren Produkten internationale Großprojekte in den Bereichen IoT und Industrie 4.0 zuverlässig zu realisieren.

Weitere Informationen zu Partnern und Produkt: www.uniscon.com

Pressekontakt

uniscon GmbH, Claudia Seidl
Ridlerstr. 57
80339 München
E-Mail: presse@uniscon.de
Internet: www.uniscon.com
Telefon: 089 / 41 615 988 104

Kafka Kommunikation GmbH & Co KG, Julia Fehrle
Auf der Eierwiese 1
82031 Grünwald
Tel. +49 (0) 89 74747058-0
Fax + 49 (0) 89 74747058-20

[3] https://www.future-thinking.de/deutscher-rechenzentrumspreis/