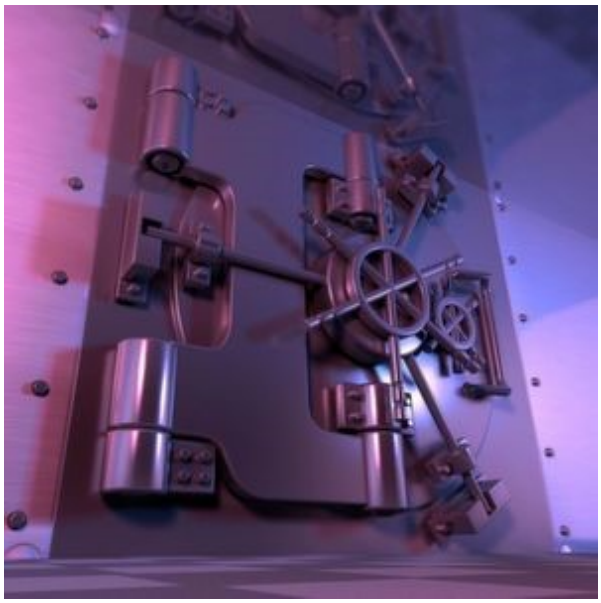
INDUSTRY OF THINGS

Sichere APIs

API? Bitte effizient und sicher!

10.12.18 | Autor / Redakteur: Sebastian Rohr / Sebastian Human



Die Relevanz sicherer APIs sollte nicht unterschätzt werden. (Bild: Pixabay / CC0)

Viele Unternehmen setzen sowohl intern als auch extern immer mehr Schnittstellen ein. Um hierbei operative Effizienz sowie die notwendige und rechtlich geforderte Datensicherheit gewährleisten zu können, ist ein ordentliches API Management und eine ausreichende API Sicherheit wichtig.

Ist die für die Schnittstelle relevante IT-Sicherheit ungenügend oder falsch konzipiert, führt dies unmittelbar zu kritischen Schwachstellen oder gar zu einem regulatorischen Albtraum. Merkwürdig bleibt die Erkenntnis, dass viele Unternehmen unabhängig von ihrer Branche bereits praktische Erfahrungen mit solchen negativen Auswirkungen gemacht haben – dennoch wird die IT-Sicherheit in der Entwicklung meist viel zu spät oder gar nicht betrachtet. Das ist nicht nur verwunderlich, sondern hat im Ernstfall fatale Folgen. Darum sollte das Thema IT-Sicherheit in einem professionell geplanten Secure Software Development Life Cycle (SSDLC) in jedem Schritt integriert sein. Insbesondere im boomenden Bereich der Internet of Things (IoT) -Applikationen ist verstärkt darauf zu achten, dass eine ausreichende Sicherheitsbetrachtung bereits in der Design-Phase erfolgt. Kostspielige Anpassungen nachträglich sichtbar werdender Schwachstellen können so bereits im Vorfeld vermieden werden. Eine Korrektur ist in diesem frühen Zustand deutlich einfacher umzusetzen.

Auch in Industrieanlagen ist mit Blick auf Industrie 4.0 Anwendungen ein starker Anstieg von APIs feststellbar. Der Vorteil, einen einfachen REST-API-Aufruf aufzubauen, abzuschicken und gegebenenfalls das Ergebnis zu

verarbeiten, benötigt in den meisten Fällen nur wenig Rechenkapazität. Auch hier kann der fehlende Fokus auf die IT-Sicherheit die angedachten Vorteile einer digitalen Transformation des innerbetrieblichen Logistikwesens schnell neutralisieren.

Fünf Faktoren für sichere APIs

Um Schnittstellen (APIs) sicher entwickeln zu können, sollten stets diese fünf Faktoren beachtet werden:

1. Identifizierung & Authentifizierung. Zuerst muss klar sein, wer oder was auf die eigenen Ressourcen zugreifen möchte. Nur, wenn diese Daten vorliegen, sollte ein Zugriff erlaubt werden.
2. Autorisierung. Nach einer erfolgreichen Authentifizierung sollte eine separate Autorisierung erfolgen, um einen Zugriff / Nutzbarkeit entsprechend der Benutzerberechtigung bereitzustellen.
3. Hiernach ist eine Überprüfung erforderlich, ob ein API-Aufruf Informationen über die dahinter liegende Architektur preisgibt. Denn das darf niemals der Fall sein.
4. API Keys sind keine Secrets. Daher muss sichergestellt sein, dass diese auch nicht als solche behandelt werden.
5. Nun können Input-, Data- und Plausibilitätskontrollen folgen.

Natürlich gibt es neben den fünf genannten Faktoren noch weitere, welche in der Entwicklung und im Lifecycle beachtet werden sollten.

Beispielarchitektur

Im Kontext der industriellen Nutzung von APIs und IoT-Geräten würde eine Architektur wie folgt aussehen (siehe Abbildung 1).

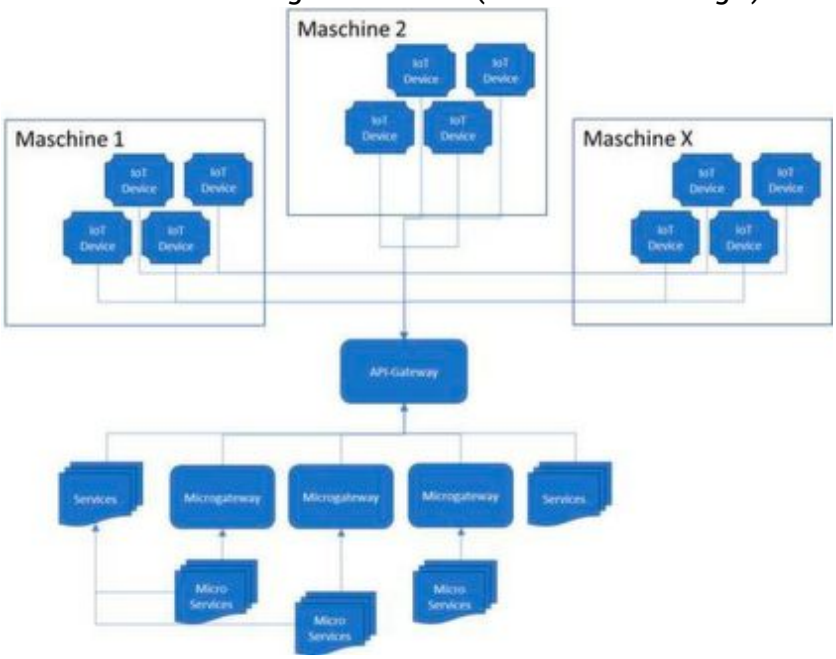


Abb.1: Vernetzung über eine (Micro-) API-Architektur (Bild: Accessec GmbH)

Die Grafik veranschaulicht beispielhaft, wie Sensoren oder andere IoT- Geräte an Maschinen einer Produktion über eine (Micro-) API-Architektur angebunden werden könnten. Hierbei hat jede Maschine eigene IoT Geräte, welche jeweils

eine andere Funktion erfüllen. Jene sind durch diverse Anwendungsfälle definiert, wie beispielsweise das Messen der Temperatur, Luftfeuchtigkeit, die Position der Produkte oder deren Abmessung. Dabei koordiniert ein API-Gateway die Schnittstellen, damit die IoT-Geräte die Anfragen an eine zentrale Stelle schicken. An dieser Stelle können dann entsprechende Sicherheitsmechanismen platziert werden. Das API- Gateway leitet die Anfragen an die einzelnen Endpunkte zur Verarbeitung weiter. Zusätzlich helfen Micro Gateways dabei, die Micro Services zu koordinieren und zu managen.