Die Chancen von Industrial IoT richtig nutzen

Industrial IoT (Industrial Internet of Things) erlebt zurzeit eine Sternstunde: Das Konzept des Austauschens und Auswertens von Daten stellt zwar eine Herausforderung dar, dennoch profitieren Unternehmen jeder Grösse nachhaltig von einem System dieser Art. Ein Einblick.

TEXT **LARS MEIER**

Grosse Maschinen und Anlagen erleichtern zweifelsohne den Arbeitsablauf und -fluss. Nichtsdestotrotz fordern sie uns dennoch immer wieder aufs Neue heraus und machen ein Umdenken unumgänglich. Beispielsweise kann die Anwesenheit der Anlagenverantwortlichen sowie des Wartungspersonals aus verschiedensten Gründen nicht immer gewährleistet werden, was nicht zuletzt auch eine Kostenfrage aufwirft.

Ein ausgeklügeltes Konzept

Industrial IoT schafft hier Abhilfe: Denn durch die Vernetzung lassen sich Maschinen, Werkzeuge und Anlagen miteinander verknüpfen, was im Zuge dessen eine vollumfängliche Automatisierung der einzelnen Prozesse oder sogar ganzen Prozessketten mit sich zieht. Mit der Bildung von virtuellen Schnittstellen von Mensch zu Maschine und Maschine zu Maschine lassen sich Geräte sowie deren Umfeld via Internet weltweit überwachen und steuern. Ein rollenbasiertes Fernwartungskonzept reduziert dabei die Risiken für die Vernetzung von Anlagen, indem es die Zugänge für Hersteller und Wartungstechniker sicherstellt. Wichtig ist zudem, dass man diese mit einer starken Authentifizierung sichert und die Zugänge durch ein Security Operation Center zugleich proaktiv überwacht.

Gut zu wissen

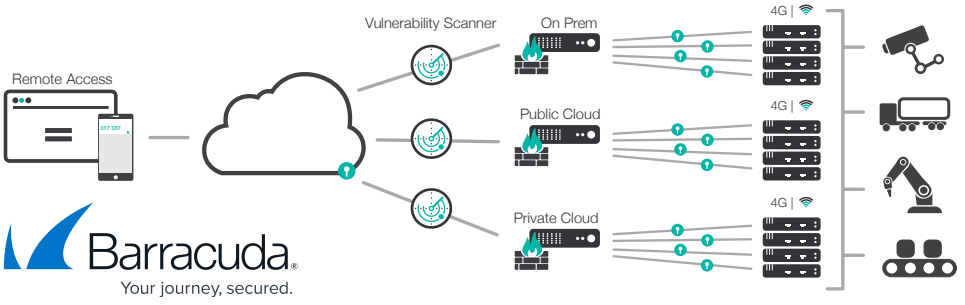
Achtung: Die separate Ausführung der Trennung und Verschlüsselung pro Gerät ist das A und O. Andernfalls könnten sich Anlagen gegenseitig beeinflussen und Schaden zufügen. Auf dem Remote Access für Wartungszugänge muss schlussendlich sichergestellt werden, dass ein Anbieter nur auf die für ihn freigeschaltete Anlage zugreifen kann. Die Sichtbarkeit der Anlagen und der damit verbundenen Systeme wird beim Einsatz einer qualifizierten Industrial-Security-Lösung neu definiert. Zu wissen, welche Schwachstellen auf diesen Systemen vorherrschen und von welchen Anlagen besonders hohe Risiken ausgehen, ist folglich von enormer Wichtigkeit. Denn Systeme, welche in einer Industrial-Security-Umgebung betrieben werden, können durch proaktive Cyber-Defense-Organisationen mit einer Kombination aus Managed-Security-Service-Provider und Security-Operation-Center granular auf Regelverstösse und Angriffe auf die Systeme reagieren und diese schützen.

Gefahren sukzessive vermeiden

Ein unkontrolliertes Verbinden von Anlagen und Systemen mit Netzwerken birgt nämlich mehr Gefahren, als man meinen könnte. So muss man etwa mit erheblichen Beeinträchtigungen oder Störungen der Produktion rechnen sowie schlimmstenfalls Reputationsschäden bei Kunden und Lieferanten hinnehmen, die sich kaum oder nur schwer wiedergutmachen lassen. Etwaige Lieferverzögerungen können ebenfalls für erhebliche Schwierigkeiten sorgen. Gleiches gilt aus rechtlicher Perspektive: Denn eine kritische Infrastruktur kann einen Verstoss gegen gesetzliche Auflagen darstellen.

ANZEIGE

CYBER DEFENCE FÜR INDUSTRIEUMGEBUNGEN



Barracuda
Your journey, secured.

SECURITY SERVICES AG
CLUE

Clue Security Services AG unterstützt Sie bei Konzeption, Aufbau und Betrieb von Industrial Security Umgebungen mit spezialisierten Cyber Defence und Managed Security Services.

CLUE SECURITY SERVICES AG | GRABENSTRASSE 17 | CH-6340 BAAR | +41 44 667 77 66 | INFO@CLUE.CH | **CLUE.CH/IOT**