Medieninformation

asvin – mehr Sicherheit für das Internet der Dinge

Erpressung, Datenklau, Sabotage – wenn Cyberkriminelle Geräte im Internet der Dinge kapern, können die Folgen verheerend sein. Das Risiko für Unternehmen ist hoch, denn industrielle IoT-Geräte sind bevorzugte Ziele für Cyberangriffe. Dabei spielen Sicherheitslücken durch fehlende Updates eine zentrale Rolle. Um das Internet der Dinge sicherer zu machen, hat das Stuttgarter Start-up asvin.io eine Lösung entwickelt, die den Software-Lifecycle von der Entwicklung, Verteilung bis zum Betrieb auf Geräten absichert und überwacht.

Jedes Jahr entsteht der deutschen Wirtschaft durch Angriffe von Hackern ein Gesamtschaden von über 100 Milliarden Euro. Um Systeme übernehmen zu können, nutzen Angreifer Sicherheitslücken von internet-konnektierten Maschinen oder Anlagen. Hinzu kommt, dass die Lösungen in der Industrie 4.0 über zunehmend komplexe Softwarelieferketten aufgebaut sind: Schon eine unsichere Komponente kann dann eine gesamte Produktionsanlage in Unsicherheiten stürzen. Lange Lebenszyklen von industriellen Anlagen und mangelhafte Pflege der Software verstärken die Risiken für die Industrie.

Sicherheit scheitert oft am Know-how

Zu den gefährlichsten Schwachstellen bei IoT-Geräten gehören fehlende Updates. Für mittelständische Hersteller ist es in der Praxis oft nicht machbar, mehrere hunderttausende verkaufte IoT-Produkte mit aktualisierten Versionen der Software zu versorgen. Denn im Unterschied zu Konzernen fehlt es kleinen Firmen an Manpower und Know-how, um ohne großen Aufwand und Kosten eine sichere OTA-Infrastruktur für Updates zu konzipieren und zu implementieren.

Updates und Patches als wichtiger Baustein

Das Stuttgarter Start-up asvin nimmt sich dieses Themas an und hat eine sichere, robuste Lösung entwickelt, um Sicherheitslücken von IoT-Geräten über Updates zu schließen und langfristig funktionsfähig zu halten. Die von asvin bereitgestellte Software-Plattform und die dezentrale Infrastruktur verteilen Updates und Patches für IoT-Endgeräte, der Vorgang wird dokumentiert und sichert die Auslieferung der Updates so vor Manipulationen.

Diese Lösung ist als „Software as a Service“ einfach zu bedienen, zuverlässig und kostengünstig. Mit dem Angebot von asvin sind individuelle Update-Rollout-Pläne ebenso möglich wie das automatische Ausführen von schnellen Sicherheitsupdates im Krisenfall.

asvin GmbH
Schulze-Delitzsch-Str. 16
70565 Stuttgart
T 0711 2204093 0
F 0711 2240493 44

contact@asvin.io
www.asvin.io

@asvin_io

IBAN: DE64 6117 0024 0043 2245 00
BIC: DEUTDEDB611

Sitz Stuttgart
HRB 76700, Amtsgericht Stuttgart

Gleichzeitig wird sichergestellt, dass Manipulationsversuche durch Angreifer schnell erkannt und abgewehrt werden können. Darüber hinaus schafft die asvin Chain-of-Trust die Vertrauensbasis für Softwarelieferketten von der Zertifizierung einer Software bis zum Update eines Gerätes und dem Betrieb der Software.

Die elegante Lösung von asvin

Nach dem Motto make or buy können sich Hersteller von IoT-Geräten mit asvin „Software as a Service“ einfach einkaufen. Der Aufwand für die Versorgung mit Updates und das Monitoring durch asvin lassen sich im Voraus zuverlässig kalkulieren. So ist der von asvin angebotene Service und Support effizienter als eine inhouse entwickelte und betriebene Lösung. Der Vorteil für industrielle Nutzer von IoT-Geräten liegt auf der Hand: Geräte und Anlagen sind besser gegen Cyberattacken geschützt, ihre Funktion kann aufrechterhalten oder schnell wiederhergestellt werden.

Abdruck honorarfrei, Beleg (Print, Scan) oder Link erbeten.

asvin GmbH
Schulze-Delitzsch-Str. 16
70565 Stuttgart
T 0711 2204093 0
F 0711 2240493 44

contact@asvin.io
www.asvin.io

@asvin_io

IBAN: DE64 6117 0024 0043 2245 00
BIC: DEUTDEDB611

Sitz Stuttgart
HRB 76700, Amtsgericht Stuttgart