Digital Manufacturing, 6/19
Experten-Umfrage: IT-Security in der Produktion
Frühzeitig anfangen und konsequent umsetzen
S. 25

Benjamin Isak

Account Manager IIoT/Industrie 4.0 (DACH) bei NCP engineering

1. Neben Verschlüsselung, sicherer Fernwartung und der Identifizierung aller kritischen Assets im Produktionsnetz, ist eine kontinuierliche Überwachung der Kommunikation sinnvoll. Dadurch lassen sich Anomalien erkennen und unterbinden. Weiterhin sollten Shopfloor-Akteure nicht direkt mit überlagerten IT-Systemen (Topfloor), Clouds oder gar externen Stakeholdern kommunizieren. Vielmehr ist hier eine zentrale Komponente essenziell, die die OT sicher und dediziert mit der IT und externen Stellen verbindet. Dabei ist es wichtig, dass nur die notwendige Menge an Daten an genau das System gehen, für das sie gedacht sind.

2. Die Mitarbeiter spielen eine Schlüsselrolle. Unternehmen sind hier in der Pflicht, Awareness für Cyber-Sicherheit zu schaffen und für das Thema zu sensibilisieren. Dabei sollten sie früh mit Angriffen und potenziellen Schäden konfrontiert werden, um das entsprechende Mindset aufzubauen. Auch ein grundlegendes Verständnis zwischen den verschiedenen Gruppen von IT- und OT-Mitarbeitern muss vorhanden sein.

3. Dies lässt sich durch ein ganzheitliches und durchgängiges Security-Konzept erreichen. Beginnend bei zentralen Komponenten, Gateways, Firewalls über VPN und IDS/IPS, sollten Industrie-4.0-Systeme nach dem Security-by-Design-Ansatz entwickelt werden. Darüber hinaus sollten Produktionsnetze in sogenannte IIoT-Inseln segmentiert werden. Mögliche Angriffe lassen sich so schnell isolieren. Außerdem ist eine lose Kopplung zwischen IT und OT unerlässlich, wie ich es bereits in der Antwort 1 erläutert habe. Zu guter Letzt darf der Faktor Mensch nicht außer Acht gelassen werden. Unternehmen müssen ihre Mitarbeiter schulen und auf potenzielle Gefahren hinweisen. Dazu gehört auch die Unternehmensorganisation. Silodenken war gestern.