IDS-Software mehrfach nutzen

Prozessoptimierung per Intrusion Detection System

Bild: ©Grispb/stock.adobe.com

Mit Intrusion-Detection-Systemen wollen Firmen Anomalien in ihren Netzwerken und somit potenzielle Eindringlinge erkennen. Aus einem anderen Blickwinkel betrachtet, können diese Systeme aber auch zur Optimierung von Produktionsprozessen beitragen.

Cybersecurity-Lösungen erheben Daten, um etwa das Geschehen in den eigenen Netzwerken besser zu verstehen. So lassen sich Lücken schließen und generell die IT-Sicherheit verbessern. Cybersecurity heißt also auch, Daten zu erfassen und richtig zu verwenden. Dabei können ähnliche Probleme entstehen, wie sich bei der Erfassung von Produktionsdaten auftreten: Es werden viele Daten ohne greifbare Vorstellung erfasst, wie sie aggregiert, verarbeitet und genutzt werden können, um neue Erkenntnisse zu gewinnen.

Daten und Metadaten

Innerhalb von industriellen Prozessen wie der Auslastung einer Maschinenlinie fallen nicht nur die Nutzdaten und Kennzahlen an, wie der Auftrags-ID, das Produkt, die produzierte Stückzahl pro Zeit und so weiter. Es werden auch Metadaten in Form von Bandbreitennutzung und Kommunikationsbeziehungen zwischen Komponenten erzeugt. Diese bleiben meist ungenutzt. Metadaten können jedoch in zweierlei Hinsicht Verwendung finden. Zum einen können sie die Cybersecurity direkt unterstützen. So lässt sich beispielsweise

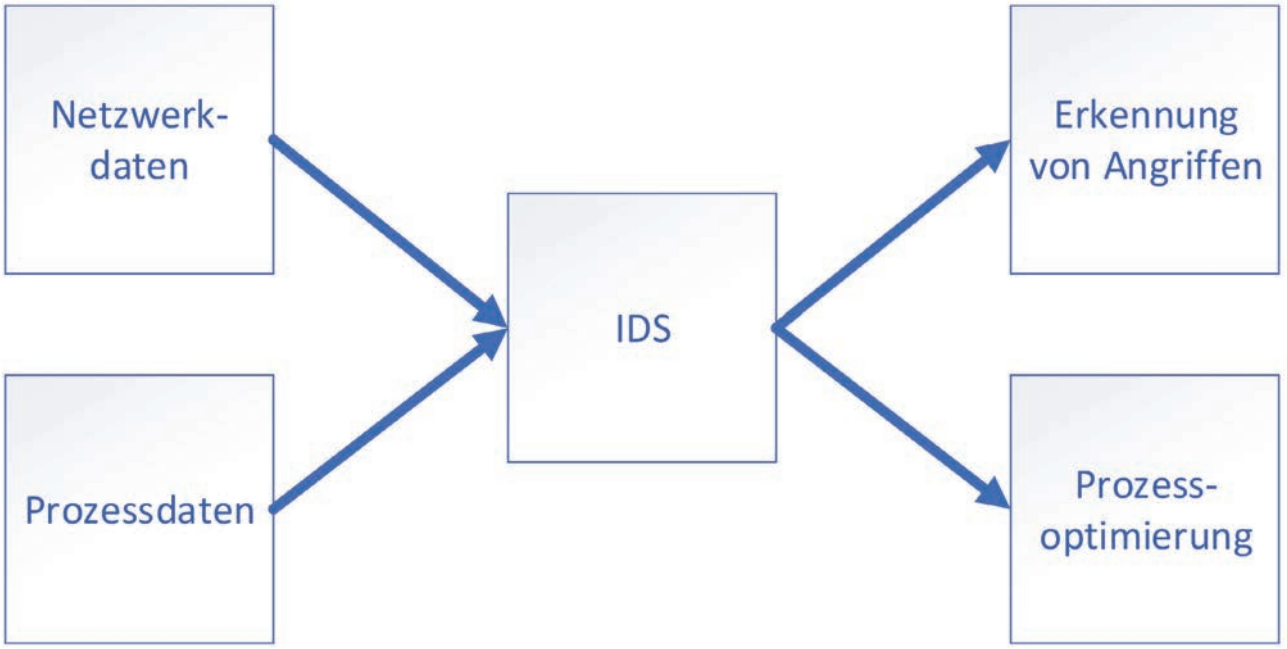

Bild: T&G Automation GmbH

beantworten, ob eine Komponente mit den richtigen Kommunikationspartnern spricht oder ob plötzlich unerwünschte Teilnehmer auftauchen, die bestehende Komponenten manipulieren könnten. Zum anderen lässt sich mit Hilfe der Metadaten herausfinden, ob eine Komponente sich anders verhält, beispielsweise ob sie plötzlich viel mehr oder viel weniger als erwartet kommuniziert. Zusätzlich können Metadaten dabei helfen, Fragen bezüglich der Maschinenprozesse zu beantworten: Wird eine höhere oder niedrigere Taktung gefahren? Ist die Sensorseite für den Ausschuss überproportional aktiv? Ist die Maschine, die für diesen Auftrag runtergefahren wurde, tatsächlich weniger aktiv? Solche Fragen lassen sich teils auch über Prozessleitsysteme beantworten, sofern diese korrekt angepasst sind. Dennoch kann es dienlich sein, über eine zusätzliche Partei eine weitere Perspektive einzubringen, um ein vollständiges Bild zu erhalten. Solange alle Perspektiven zusammenpassen, können Betreiber davon ausgehen, das der Prozess erwartungsgemäß funktioniert. Wenn eine Diskrepanz zwischen den Perspektiven auftritt, kann ein genauerer Blick lohnen.

Intrusion Detection Systems

Eine solche zusätzliche Perspektive können sich Verantwortliche mit einem Intrusion Detection System (IDS) verschaffen. Ein IDS im klassischen Sinn wird für die Erkennung von ungewöhnlichem Netzwerkverkehr eingesetzt und kann somit Angriffe auf ein Netzwerk melden. Das System arbeitet mit Regelsätzen und Signaturen für typisches Kommunikationsaufkommen bekannter Angriffe. Diese Regelsätze können komplexe mehrdimensionale Zusammenhänge enthalten, wie das Kommunikationsverhalten einer Komponente im Netzwerk zu bestimmten Tageszeiten in Relation zu anderen Komponenten. Einerseits kann ein so designtes IDS als zusätzliches Schutzsystem für industrielle Netzwerke eingesetzt werden. Sie können aber auch komplexe Metadaten erfassen. Mit einem definierten Satz an Regeln und Signaturen können so auch Prozessinformationen erhoben werden, die bisher nicht berücksichtigt wurden. Diese können anschließend mit der Kommunikationsaktivitäten der einzelnen Maschinen einer Produktionslinie abgebildet werden. Hierdurch lassen sich komplexe Zusammenhänge wie der Alterungsprozess einer Maschine oder die Effizienz eines neuen Prozesses besser erfassen und verstehen.

Mehr Information zum Prozess

Etwa für einen verbesserten Predictive-Maintenance-Ansatz als auch zur Prozessoptimierung kann zusätzliches Potenzial abgerufen werden. Andersherum können aus den Prozessinformationen auch sicherheitsrelevante Vorgänge beobachtet werden, was der Cybersicherheit hilft. Die Kombination aus Prozessdaten sowie Metadaten erlaubt es, eine Verbindung zwischen einer langsameren oder schnelleren Taktung sowie einem niedrigeren oder höheren Netzwerkkommunikationsaufkommen herzustellen und somit Fehlalarme zu reduzieren. Dieser Dual-Use, also die Mehrfachverwendung des IDS, verschafft noch einmal mehr Informationen über die Prozesse im Werk, womit sich weitere Optimierungsmöglichkeiten eröffnen. Dieser Gewinn an Prozessdaten ist ökonomisch greifbarer als der Sicherheitsgewinn, der sich immer gegen das Risiko und Schadenspotential von Cyber-Attacken aufrechnen muss. Somit ist ein Dual-Use-IDS wirtschaftlich attraktiv, da es nicht nur der Verteidigung dient, sondern über die Prozessoptimierung zur Wertschöpfung beiträgt. ■

Die Autoren: Martin Aman ist Leiter Technik und Laurin Dörr ist Leiter Business Development bei TG Alpha GmbH.

www.tgalpha.de