Bild: Videc

01 Kontrolle über den Prozess auf Basis eines Risikomanagements

Monitoring und Erkennung von Anomalien in Anlagen

Normungen und Vorgaben erfüllen das Herz eines Betreibers nicht immer mit Freude. Bei der BSI CS 134 wurde allerdings ein wichtiger Schritt in die richtige Richtung der IT/OT-Security gemacht. Die Kernthemen sind in der BSI CS 134 beschrieben. Dazu gehören das Monitoring – die systemische Überwachung und Beobachtung der Kommunikation, die Anomalieerkennung in der Kommunikation mit entsprechender Archivierung, Protokollierung und Analyse sowie die Angriffserkennung (Intrusion Detection) mit Alarmierung im Bedarfsfall.

Text: Dieter Barelmann

Man stelle sich einmal vor, wir würden heute Produkte in prozesstechnischen Anlagen ohne Leit- oder Scada-System herstellen wollen: keine Sichtbarkeit, keine Kontrolle über den Prozess. Die Automatisierung läuft zwar, jedoch kann man nichts über den Zustand der Anlage aussagen. Solch eine Situation wäre heute kaum noch denkbar, im Bereich OT-Security ist sie allerdings Stand der Dinge.

Die Folgen der zunehmenden Vernetzung

Im Zuge der Digitalisierung streben Unternehmen einen immer höheren Grad der Vernetzung mit der Automatisierung im Zusammenhang stehenden Geräte und Systeme an. Die Folge ist eine zunehmende Abhängigkeit von deren Verfügbarkeit. Die Anzahl der Teilnehmer am Ethernet erhöht sich signifikant, ebenso die Kommunikation selbst.

Bild: Videc/iStock_Erik Khalitov

02 Ganzheitlicher Schutz vor Cyber-Angriffen in Produktionsanlagen mit Irma – übersichtliche Darstellung auf dem Dashboard

Wer jedoch mit wem kommuniziert – berechtigt oder auch nicht, ist kaum jemandem bekannt. Erschwerend kommt noch hinzu, dass mehrere Anlagenteile oft von unterschiedlichen Lieferanten installiert werden. Die steigende Komplexität im Netzwerk und die Implementierung von nicht immer vollständig IP-standardkonformen Geräten führt immer wieder zu Seiteneffekten im Netzwerk, die zunächst nicht bemerkt werden und irgendwann zu einem Störfall werden können. Dies wäre mit einer kontinuierlichen Überwachung des Netzwerkverkehrs aufgefallen und vermeidbar gewesen.

Im Bereich der OT-Security fließen die meisten Investitionen allerdings in Netzwerksegmentierungen und in Firewalls; der Blick auf die Anlage und die Kontrolle über die Kommunikation bleiben so verwehrt. Sicherlich sind die Investitionen im klassischen Sinn der Security notwendig, jedoch in keinem Fall ausreichend. Denn wenn erst einmal ein Netzwerk zum Beispiel über einen infizierten Programmierrechner unbemerkt befallen ist, kann sich der Angreifer weiter austoben. Sogar das Nachladen von Schadcode würde von einer Firewall nicht verhindert werden, da der Verbindungsaufbau ins Internet aus der internen Zone erfolgt. Hier hat das BSI aus Sicht der IT Sicherheit mit dem BSI CS 134 dem Hase-und-Igel-Spiel zwischen dem Angreifer und dem Schützenden einen wichtigen Impuls zugunsten des Betreibers gegeben.

Passives Monitoring und Angriffserkennung

Die Vorteile des passiven Monitorings neben der Möglichkeit der Angriffserkennung sind vielschichtig. Hier nur ein kurzer Ausschnitt: Jeder Anlagenbetreiber hat sofort alle Teilnehmer im Blick und externe Dienstleister lassen sich über die Zugänge genau kontrollieren. Zusätzlich erhält die IT wichtige Informationen für die Feinjustierung der Firewall – ein wichtiger Punkt bei der Angriffsabwehr. Bei der Alarmierung in der Angriffserkennung lässt sich der Servicebereich in der Regel optimieren und spart Kosten.

Die verschiedenen Ansichten über eine aktive bzw. passive Abfrage der Assets ist aus Sicht der Automatisierung sehr einfach. Die sensible Struktur der Automatisierungsgeräte mit ihren unterschiedlichen Generationen ist bei einem 24/7-Betrieb keine Spielwiese für aktive Abfragen. Das höchste Gut der OT ist die Verfügbarkeit – diese verträgt lediglich die passive Variante.

Die Kontrolle über den Prozess auf Basis eines Risikomanagements zu behalten, Sichtbarkeit der aktuellen Assets und eine Alarmierung bei Unregelmäßigkeiten in der Kommunikation sind die wichtigen Bausteine für eine sichere Produktion. Das ist heute schon nicht nur eine Empfehlung des BSI, sondern Stand der Technik (**Bild 1**).

Security muss übersichtlich, bedienbar und einfach sein. Dieser Anspruch gilt bei dem Anbieter Videc [1] in der Entwicklung ebenfalls für den Bereich OT-Security – seit über fünf Jahren in der Produktentwicklung (**Bild 2**). Das Resultat ist die komplette Erfüllung der Vorgaben des BSI CS 134. (hz)

Literatur

[1] Videc GmbH, Bremen: www.videc.de

Autor

Dipl.-Ing. Dieter Barelmann ist Geschäftsführer der Videc GmbH in Bremen.
DBarelmann@videc.de