OT-Risikoanalyse von Controlware: Sicherung der Betriebstechnologie gegen Cyber-Bedrohungen

Die Situation

Die zunehmende Digitalisierung in der Industrie bietet Unternehmen große Chancen, bringt jedoch auch neue Risiken für die Betriebstechnologien (OT) mit sich, die für die Steuerung und Überwachung von Produktionsprozessen verantwortlich sind. SCADA-Anlagen und IIoT-vernetzte Geräte, die traditionell getrennt und isoliert von den klassischen IT-Netzwerken betrieben wurden, sind heute oft eng in die IT-Infrastruktur eingebunden. Diese enge Vernetzung macht OT-Infrastrukturen jedoch verwundbar. Angriffe auf IIoT-Geräte, z.B. durch Ransomware, gezielte Manipulationen von Steuerungssystemen und Cyberangriffe bedrohen daher heute zwangsläufig nicht nur die IT, sondern auch OT-Systeme.

Die Folgen eines Angriffs auf OT-Infrastrukturen können gravierend sein: Betriebsausfälle, Produktionsstörungen, Verlust sensibler Daten, Umwelt- und Personenschäden und Reputationsverlust. Ein einziger Sicherheitsvorfall kann die gesamte Produktion außer Kraft setzen und enorme finanzielle Verluste verursachen. Um diese Herausforderungen zu bewältigen und die Sicherheit der Produktionsprozesse zu gewährleisten, ist mittlerweile eine umfassende OT-Risikoanalyse unverzichtbar. Mit dieser Analyse lassen sich potenzielle Schwachstellen frühzeitig identifizieren.

Herausforderungen der OT-Sicherheit

Die Herausforderungen der OT-Sicherheit liegen vor allem in den speziellen Anforderungen und der hohen Komplexität der Betriebstechnologie. OT-Systeme müssen kontinuierlich und ohne Unterbrechung verfügbar sein, da schon kleinste Ausfallzeiten die Produktionsprozesse beeinträchtigen können. Traditionelle Sicherheitsmaßnahmen wie regelmäßige Updates und Systemneustarts lassen sich in der OT schwer umsetzen, da sie zu Betriebsunterbrechungen führen könnten.

Zusätzlich bestehen OT-Infrastrukturen oftmals aus einer Mischung von neuen und älteren Systemen verschiedener Hersteller, die ursprünglich ohne moderne Sicherheitsstandards konzipiert wurden. In der Regel bieten diese veralteten Komponenten potenzielle Angriffspunkte, da sie nicht mit aktuellen Sicherheitsprotokollen kompatibel sind und sich nur schwer in eine einheitliche Sicherheitsstrategie integrieren lassen.

Ein weiteres Risiko stellt die mangelnde Segmentierung vieler OT-Netzwerke dar. Im Gegensatz zur IT, in der Netzwerke klar getrennt und gesichert sind, fehlt es in OT-Umgebungen häufig an einer sicheren Trennung der Netzwerkbereiche. Dadurch können Angreifer, wenn sie einmal Zugang zu einem Bereich erhalten, leicht auf andere Teile des Netzwerks übergreifen.

Zusätzlich sind OT-Systeme in vielen Branchen spezifischen regulatorischen Vorgaben unterworfen, wie den IEC 62443-Standards für die industrielle Cybersicherheit, IT-SG2, KRITIS oder den NIS-2-Richtlinien. Diese Standards erfordern spezielle Sicherheitsmaßnahmen, beispielsweise durch Risikomanagement, Schwachstellenmanagement, Netzwerksicherheit und Zugangssteuerung. Die Einhaltung dieser Vorgaben ist komplex und zeitaufwendig, aber unverzichtbar, um den Schutz der OT-Systeme zu gewährleisten und regulatorische Anforderungen zu erfüllen.

Die NIS2-Richtlinie stärkt den Schutz von OT-Systemen: Zunächst Risiken erkennen, dann gezielte Sicherheitsmaßnahmen implementieren, kontinuierlich überwachen und im Ernstfall schnell reagieren. Diese Schritte sind entscheidend, um die Resilienz und Betriebssicherheit zu gewährleisten.

Sprechen Sie uns gerne dazu an!

Der Lösungsansatz: OT-Risikoanalyse für sichere Produktionsprozesse

Die OT-Risikoanalyse verfolgt einen systematischen Ansatz, um die Sicherheit und Widerstandsfähigkeit von OT-Systemen zu stärken. Sie orientiert sich am NIS-2-Cybersecurity-Framework und umfasst die wesentlichen Schritte: Identifizierung, Schutz, Erkennung, Reaktion und Wiederherstellung.

Der Prozess beginnt zunächst mit der Definition des Scopes. Daran schließt sich die detaillierte Bestandsaufnahme der gesamten OT-Infrastruktur an. Alle Komponenten und Kommunikationswege werden erfasst, um ein vollständiges Inventar zu erstellen, das die Grundlage für die Identifikation und gezielte Adressierung potenzieller Schwachstellen bildet.

Anschließend erfolgt die Risikobewertung, bei der die identifizierten Risiken noch Schweregrad und Wahrscheinlichkeit klassifiziert werden. Hierbei helfen Risikobewertungsmodelle um die größten Schwachstellen zu priorisieren und entsprechende Maßnahmen gezielt auf die kritischsten Risiken zu fokussieren und ggf. Risiken zu akzeptieren.

Basierend auf den Analyse-Ergebnissen können dann spezifische Schutzmaßnahmen implementiert werden. Ein Notfallplan stellt sicher, dass im Ernstfall eine schnelle Reaktion möglich ist, um Betriebsunterbrechungen zu minimieren.

Ein weiterer zentraler Bestandteil der OT-Risikoanalyse ist die Schulung der Mitarbeitenden. Regelmäßige Sensibilisierungsmaßnahmen fördern das Bewusstsein für OT-spezifische Sicherheitsrisiken und tragen dazu bei, menschliche Fehler zu reduzieren, die nicht selten Ursache für Sicherheitsvorfälle sind.

Vorteile der OT-Risikoanalyse

Die Risikoanalyse ermöglicht es, ein Risikomanagement zu etablieren und proaktiv die bestehenden Risiken zu minimieren. Die durchgehende Überwachung und Einführung einer klaren Sicherheitsarchitektur sorgen dafür, dass sich Sicherheitsvorfälle frühzeitig erkennen und abwehren lassen, bevor es zu Schäden kommt.

Darüber hinaus erleichtert die Risikoanalyse die Einhaltung regulatorischer Anforderungen und branchenspezifischer Standards. Da viele Branchen strengen Vorschriften unterliegen, vereinfacht eine systematische OT-Risikoanalyse die Nachweisführung und minimiert das Risiko von Compliance-Verstößen. Die Unternehmen sind in der Lage, nachweislich sicherheitskonforme Prozesse und Systeme zu betreiben, was nicht nur das Vertrauen der Stakeholder stärkt, sondern auch potenzielle Strafen und Reputationsschäden vermeidet.

Ein weiterer Vorteil liegt in der Ressourcen-Effizienz. Die Priorisierung der Risiken ermöglicht eine gezielte Zuteilung der Sicherheits-Ressourcen, wodurch Unternehmen ihre IT- und OT-Abteilungen entlasten und die Produktivität steigern können.

Warum Controlware

Die Controlware GmbH ist ein führender IT-Dienstleister und Managed Service Provider mit über 40 Jahren Erfahrung. Wir entwickeln, implementieren und betreiben umfassende IT- und OT-Lösungen für Cloud-, Data Center-, Enterprise- und industrielle Umgebungen. Mit unserem ISO 27001-zertifizierten Customer Service Center gewährleisten wir höchste Servicequalität.

Die Controlware Experten verfügen über fundiertes Know-how in der Gestaltung moderner Netzwerke, einschließlich IT- und OT-Sicherheitslösungen. Wir unterstützen Kunden aus unterschiedlichsten Branchen bei der Absicherung und Optimierung ihrer IT- und OT-Infrastrukturen. Dabei legen wir besonderen Fokus auf die Integration von IT- und OT-Systemen, um Stabilität und Sicherheit zu gewährleisten.

Zentrale

Controlware GmbH
Waldstraße 92
63128 Dietzenbach
Tel. +49 6074 858-00
Fax +49 6074 858-108

info@controlware.de
www.controlware.de
blog.controlware.de

Besuchen Sie uns auf: