Holger Reibold

OT-Sicherheit in der Praxis

Wenn das schächste Glied entscheidet

BRAIN-MEDIA.DE

Holger Reibold

OT-Sicherheit in der Praxis

Wenn das schwächste Glied entscheidet

BRAIN-MEDIA.DE

ISBN: 978-3-95444-345-1

Cover: pixabay / cortixxx

Brain-Media.de

Dr. Holger Reibold – Huber-Müller-Str. 52 – 66113 Saarbrücken

info@brain-media.de – www.brain-media.de

Inhaltsverzeichnis

Vorwort

OT-Sicherheit: Vom Nischenthema zur Chefsache.

Die industrielle Welt befindet sich in einem tiefgreifenden Wandel. Produktionsanlagen, Energieversorgungssysteme und kritische Infrastrukturen sind heute stärker vernetzt als je zuvor. Was lange Zeit isoliert und durch physische Trennung geschützt war, ist inzwischen Teil digitaler Wertschöpfungsketten geworden. Mit dieser Entwicklung entstehen neue Chancen – aber auch neue Risiken.

Die Sicherheit von Operational Technology (OT) ist dabei zu einer zentralen Herausforderung geworden. Während in der klassischen IT Vertraulichkeit und Datenschutz im Vordergrund stehen, gelten in der OT andere Prioritäten: Verfügbarkeit und funktionale Sicherheit haben oberste Bedeutung. Ein ungeplanter Stillstand kann nicht nur wirtschaftliche Schäden verursachen, sondern auch Menschen gefährden und kritische Prozesse unterbrechen.

Gleichzeitig zeigt die Realität in vielen Unternehmen ein anderes Bild als die idealisierten Architekturen aus Lehrbüchern und Standards. Gewachsene Strukturen, jahrzehntealte Systeme und fehlende Transparenz prägen den Alltag. In diesen sogenannten Brownfield-Umgebungen treffen moderne Bedrohungen auf Technologien, die

ursprünglich nie für eine vernetzte Welt konzipiert wurden. Sicherheitsmaßnahmen lassen sich hier nicht einfach nach IT-Vorbild umsetzen.

Hinzu kommt ein grundlegender Zielkonflikt: Jede Änderung an einem System – sei es ein Patch, ein Update oder eine neue Sicherheitsfunktion – kann Auswirkungen auf die Stabilität und Sicherheit der Anlage haben. In der OT gilt daher ein anderes Prinzip als in der IT: Nicht jede Schwachstelle kann sofort behoben werden. Oft geht es darum, Risiken zu verstehen, abzuwägen und pragmatische Schutzmaßnahmen zu implementieren.

Dieses Buch verfolgt einen bewusst praxisorientierten Ansatz. Es richtet sich an Verantwortliche, die nicht im Idealzustand starten, sondern in bestehenden, oft komplexen Umgebungen arbeiten. Ziel ist es, ein realistisches Verständnis von OT-Sicherheit zu vermitteln und konkrete Wege aufzuzeigen, wie Sicherheitsmaßnahmen schrittweise und wirksam umgesetzt werden können.

Dabei werden sowohl technische als auch organisatorische Aspekte betrachtet. Denn erfolgreiche OT-Sicherheit ist keine reine Technologiefrage. Sie erfordert Zusammenarbeit zwischen IT und OT, klare Verantwortlichkeiten und ein gemeinsames Verständnis von Risiken und Prioritäten. Insbesondere die zunehmenden regulatorischen Anforderungen, wie sie etwa durch die NIS2-Richtlinie entstehen, machen deutlich, dass OT-Sicherheit längst ein Thema auf Managementebene ist.

Ein zentrales Leitmotiv dieses Buches ist die Erkenntnis, dass Sicherheit immer im Kontext der Realität erfolgen muss. Perfekte Architekturen existieren selten. Entscheidend ist, Risiken zu reduzieren, Transparenz zu schaffen und schrittweise Verbesserungen umzusetzen. Oder anders formuliert: Es geht nicht darum, sofort alles richtig zu machen, sondern darum, die richtigen Dinge konsequent zu verbessern.

Wenn dieses Buch dazu beiträgt, die Komplexität von OT-Sicherheit verständlicher zu machen und konkrete Handlungsschritte aufzuzeigen, hat es seinen Zweck erfüllt.

Herzlichst

Holger Reibold

1 Einführung in OT-Sicherheit

IT reicht nicht: Warum OT eigene Regeln braucht.

Die Sicherheit industrieller Systeme hat sich in den letzten Jahren von einem Nischenthema zu einer zentralen Herausforderung entwickelt. Operational Technology steuert physische Prozesse – von Produktionsanlagen über Energieversorgung bis hin zu kritischen Infrastrukturen. Anders als klassische IT-Systeme wirken sich Störungen hier unmittelbar auf reale Abläufe aus.

Mit der zunehmenden Vernetzung von Anlagen, der Integration von IT-Systemen und dem Einsatz von Industrial IoT entstehen neue Angriffsflächen. Systeme, die ursprünglich für isolierte Umgebungen konzipiert wurden, sind heute oft Teil komplexer, vernetzter Architekturen. Gleichzeitig bleiben viele dieser Systeme über Jahrzehnte im Einsatz und lassen sich nur eingeschränkt aktualisieren.

Dieses Kapitel legt die Grundlage für das Verständnis von OT-Sicherheit. Es erläutert die Unterschiede zwischen IT und OT, zeichnet die Entwicklung industrieller Systeme nach und beschreibt die spezifischen Sicherheitsziele. Darüber hinaus werden typische Bedrohungen sowie die Auswirkungen der IT/OT-Konvergenz betrachtet. Ziel ist es, ein gemeinsames Begriffsverständnis zu schaffen und die Besonderheiten von OT-Umgebungen klar einzuordnen.

1.1 Definition und Abgrenzung von IT und OT

Operational Technology (OT) und Information Technology (IT) verfolgen unterschiedliche Ziele und sind historisch aus verschiedenen Anforderungen heraus entstanden. Während IT-Systeme primär der Verarbeitung, Speicherung und Übertragung von Daten dienen, steuert OT physische Prozesse in der realen Welt. Dazu gehören beispielsweise Produktionsanlagen, Energieverteilung, Wasseraufbereitung oder Verkehrssysteme.

Ein zentrales Unterscheidungsmerkmal liegt in den Prioritäten der Sicherheit. In der IT steht traditionell die Vertraulichkeit von Informationen im Vordergrund, gefolgt von Integrität und Verfügbarkeit. In der OT hingegen gilt eine andere Reihenfolge: Verfügbarkeit und funktionale Sicherheit haben oberste Priorität, da ein Ausfall unmittelbare Auswirkungen auf Anlagen, Umwelt oder sogar Menschen haben kann. Integrität ist ebenfalls kritisch, während Vertraulichkeit häufig eine untergeordnete Rolle spielt.

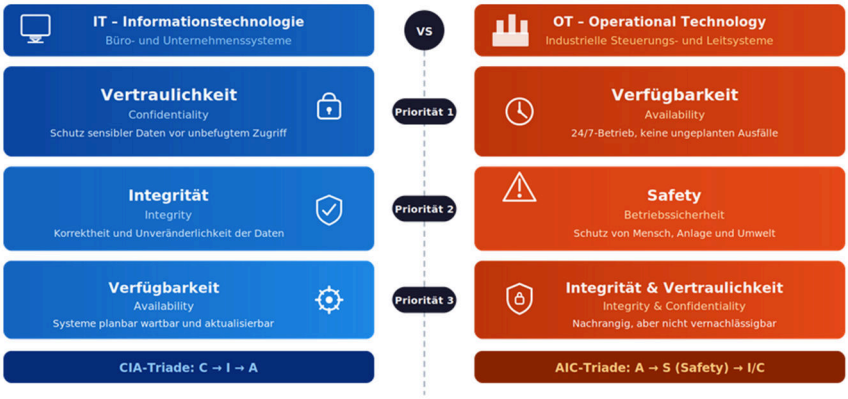
Auch die technischen Eigenschaften unterscheiden sich deutlich. IT-Systeme sind in der Regel standardisiert, nutzen weit verbreitete Betriebssysteme und werden regelmäßig aktualisiert. OT-Systeme hingegen bestehen häufig aus spezialisierten Komponenten wie speicherprogrammierbaren Steuerungen (SPS/PLC), Leitsystemen (SCADA, DCS) und proprietären Protokollen. Diese Systeme sind oft auf lange Lebenszyklen ausgelegt und können über Jahrzehnte

betrieben werden. Updates oder Patches sind daher nur eingeschränkt möglich oder mit erheblichen Risiken verbunden.

Ein weiterer wesentlicher Unterschied ist die Veränderungsdynamik. IT-Umgebungen sind auf Flexibilität und schnelle Anpassung ausgelegt. Neue Softwareversionen, Sicherheitsupdates und Konfigurationsänderungen gehören zum Tagesgeschäft. In der OT hingegen ist Stabilität entscheidend. Änderungen werden sorgfältig geplant, getestet und häufig nur in festgelegten Wartungsfenstern durchgeführt, um Produktionsunterbrechungen zu vermeiden.

Die zunehmende Konvergenz von IT und OT führt dazu, dass diese ursprünglich getrennten Welten immer stärker zusammenwachsen. Produktionsdaten werden in IT-Systeme integriert, Fernwartung erfolgt über IP-basierte Netzwerke und Cloud-Anbindungen ermöglichen neue Geschäftsmodelle. Gleichzeitig entstehen dadurch neue Schnittstellen und potenzielle Angriffsvektoren.

Für ein wirksames Sicherheitskonzept ist es daher entscheidend, die Unterschiede zwischen IT und OT zu verstehen und zu berücksichtigen. Maßnahmen, die in der IT etabliert sind, lassen sich nicht ohne Weiteres auf OT-Umgebungen übertragen. Stattdessen erfordert OT-Sicherheit einen angepassten Ansatz, der technische, organisatorische und betriebliche Besonderheiten gleichermaßen berücksichtigt.



Vergleich der Sicherheitsprioritäten in IT und OT. Während in der IT Vertraulichkeit dominiert, stehen in der OT Verfügbarkeit und Sicherhiet im Fokus. Diese unterschiedliche Gewichtung beeinflusst alle Sicherheitsmaßnahmen.

1.2 Entwicklung industrieller Systeme

Die Entwicklung industrieller Systeme ist eng mit dem technologischen Fortschritt der letzten Jahrzehnte verbunden. Ursprünglich waren Produktionsanlagen weitgehend mechanisch geprägt und wurden lokal, oft manuell gesteuert. Mit dem Einzug der Elektronik in den 1960er- und 1970er-Jahren begann die Automatisierung durch erste speicherprogrammierbare Steuerungen (SPS/PLC). Diese Systeme ersetzten starre Relaislogiken und ermöglichten flexiblere und effizientere Produktionsprozesse.

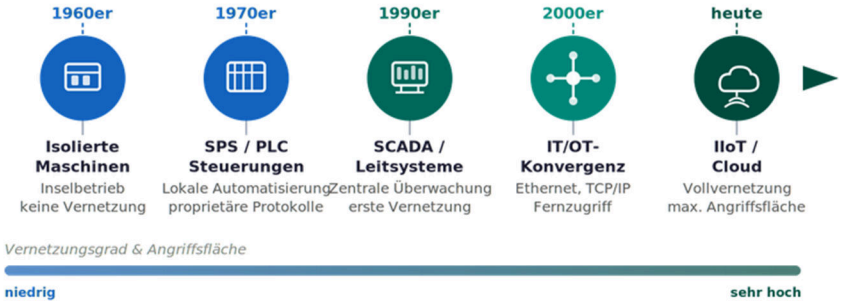
In den folgenden Jahrzehnten wurden diese Steuerungen zunehmend miteinander vernetzt. Leitsysteme wie SCADA (Supervisory Control and Data Acquisition) und DCS (Distributed Control Systems)

entstanden, um komplexe Anlagen zentral zu überwachen und zu steuern. Die Kommunikation erfolgte dabei über proprietäre Protokolle und dedizierte Netzwerke. Sicherheit spielte in dieser Phase eine untergeordnete Rolle, da die Systeme physisch isoliert waren („Air Gap“) und somit als inhärent geschützt galten.

Mit der Verbreitung von Standardtechnologien ab den 1990er-Jahren änderte sich dieses Paradigma grundlegend. Ethernet-basierte Netzwerke und TCP/IP hielten Einzug in die industrielle Kommunikation. Dies brachte erhebliche Vorteile hinsichtlich Interoperabilität und Skalierbarkeit, führte jedoch auch dazu, dass industrielle Systeme zunehmend mit klassischen IT-Strukturen vergleichbar wurden – inklusive ihrer Schwachstellen.

Im Zuge der Digitalisierung und Industrie 4.0 wurden OT-Systeme schließlich eng mit IT-Systemen verzahnt. Produktionsdaten werden heute in Echtzeit analysiert, Cloud-Plattformen ermöglichen standortübergreifende Steuerung, und Fernwartung ist ein etablierter Standard. Gleichzeitig sind viele Altanlagen weiterhin im Betrieb, die nie für diese Vernetzung ausgelegt waren.

Diese historische Entwicklung erklärt die heutige Ausgangssituation: eine heterogene Landschaft aus modernen, vernetzten Systemen und langlebigen Legacy-Komponenten. Sicherheitskonzepte müssen daher sowohl aktuelle Technologien als auch gewachsene Strukturen berücksichtigen. Ein tiefes Verständnis dieser Evolution ist entscheidend, um Risiken realistisch einzuschätzen und geeignete Schutzmaßnahmen abzuleiten.



Die Evolution industrieller Systeme von isolierten Steuerungen hin zu vernetzten Architekturen. Mit zunehmender Vernetzung steigen Komplexität und Angriffsfläche erheblich.

1.3 Sicherheitsziele in OT

Die Sicherheitsziele in der Operational Technology unterscheiden sich grundlegend von denen der klassischen Information Technology. Während in der IT häufig die sogenannte CIA-Triade – Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability) – im Vordergrund steht, verschiebt sich die Priorisierung in der OT deutlich. Hier dominieren Verfügbarkeit und funktionale Sicherheit, da sie unmittelbar mit dem sicheren Betrieb physischer Anlagen verknüpft sind.

Verfügbarkeit bedeutet in der OT, dass Systeme und Prozesse kontinuierlich und zuverlässig funktionieren. Ein ungeplanter Stillstand kann Produktionsausfälle, Lieferkettenprobleme oder erhebliche wirtschaftliche Schäden verursachen. In kritischen Infrastrukturen

Stichwortverzeichnis

I

K

L

M

N

O

P

R

S

T

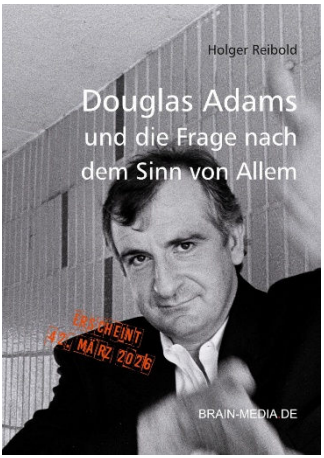
U

V

W

Z

Mehr von Brain-Media.de



42 – Douglas Adams und die Frage nach dem Sinn von Allem

Am 11. Mai 2026 ist Douglas Adams 25 Jahre tot. Der Kultautor hat der Welt wunderbar, skurrile Werke geschenkt. Jetzt ist es an der Zeit, den Autor kennenzulernen.

Umfang: 140 Seiten

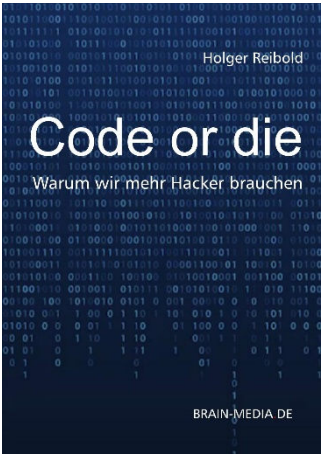
Preis: 14,99 EUR

Erscheint: 42. März 2026

Towelday, das ultimative Handtuch für alle Fans

An seinem Todestag, dem Towelday, erinnern sich Fans an Douglas Adams und huldigen dem Kultautor.

100 % intergalaktisch geprüfte Baumwolle, nachhaltig Produktion zum Preis von 42 EUR.



Code or die – Warum wir mehr Hacker brauchen

Ein Manifest für mehr digitale Selbstbestimmung, Neugierde und Eigenverantwortung. Medienkompetenzen alleine genügen nicht; die Gesellschaft von morgen braucht Digitalkompetenzen.

Umfang: 120 Seiten

Preis: 14,99 EUR

Lokale KI – Sichere Architektur, Betrieb und Governance von GenAI- und RAG-Systemen

RAG- und LLM-Plattformen mit Architektur und Governance kontrolliert und resilient betreiben.

Umfang: 270 Seiten

Preis: 29,99 EUR

Knowledge as a Service

Personal

Business

Enterprise

IT-Security, Compliance und KI entwickeln sich schneller als jedes gedruckte Buch. Um dieser Dynamik Rechnung zu tragen, hat Brain-Media.de **KaaS – Knowledge as a Service** entwickelt. Mit KaaS erhalten Sie ein lebendes **Wissenssystem**: Alle Titel als PDF/E-Book, **regelmäßig aktualisierte Living Documents** sowie **exklusive Downloads** – Checklisten, Vorlagen und sofort einsetzbare Templates.

Speziell für **Regulierung und Audits**: Inhalte zu NIS-2, DORA, CRA & AI Act werden laufend gepflegt und helfen Ihnen, Anforderungen strukturiert umzusetzen und auditfähig zu bleiben. Für fortgeschrittene Nutzung stehen Inhalte zusätzlich als **Markdown- und JSON-Rohdaten** bereit – ideal für die Automatisierung und Integration in Ihre Umgebungen. Außerdem: strategische Audio-Briefings für Entscheider.

KaaS ist die wachsende **Bibliothek für**
Praxis, Compliance und Resilienz.