OPERATIONAL TECHNOLOGY: Wandel, Herausforderungen und neue Sicherheitsbedürfnisse in der Smart Factory

Die digitale Transformation schreitet in der Industrie – und insbesondere der Produktion – immer weiter voran. Dabei rückt nun die Operative Technologie (engl. Operational Technology [OT]) stärker in den Mittelpunkt. Es ist nicht länger nur ein IT-Thema – beispielsweise sind die Daten- und Vernetzungsaspekte Teil der Informationstechnik (engl. Information Technology [IT]).

Mit dem Wandel der OT gehen allerdings spezifische Herausforderungen einher, die in diesem Report skizziert werden. Setzen sich die Unternehmen damit nicht auseinander, können sie die mit der digitalen Transformation verbundenen betriebswirtschaftlichen Vorteile wie Kosteneinsparungen oder Ertragspotenziale nicht vollständig ausschöpfen.

Grundsätzlich handelt es sich bei der OT laut Gartner um „Hardware und Software, die eine Änderung durch die direkte Überwachung und/oder Kontrolle von physikalischen Geräten, Prozessen und Ereignissen im Unternehmen erkennen oder verursachen." Demnach ist die OT bei den Unternehmen in erster Linie im Produktionsbereich – auf dem Shopfloor – zu finden. Die IT wiederum umfasst die Technologien und Prozesse für Vernetzung, Informations- und Datenverarbeitung sowie die Cloudumgebung. Während die Geräte der OT die physische Welt steuern, ist die IT auf Daten und Anwendungen fokussiert.

Bis heute sind die beiden Bereiche – IT und OT – voneinander getrennt. Auch wenn IT und OT teilweise die gleichen Werkzeuge aus Soft- und Hardware nutzen, machten unterschiedliche Charakteristika, Zielsetzungen, Schutzanforderungen und Prioritäten eine differenzierte Verwaltung erforderlich. Die IT ist auf die Erbringung von datenorientierten Diensten und Anwendungen fokussiert, die durch standardisierte Technologien kostengünstig erbracht werden – unter Anwendung der Prinzipien von Vertraulichkeit, Integrität und Verfügbarkeit. Die OT ist auf die Ausfallsicherheit und Produktivität der Herstellungsprozesse fokussiert und nutzt die Prinzipien Verfügbarkeit sowie Verlässlichkeit. Außerdem bildete die OT meist ein eigenes Ökosystem, da keine Kommunikation mit anderen Unternehmensnetzwerken oder dem Internet bestand, was bei der IT hingegen immer der Fall war. Diese Trennung wandelt sich allerdings im Zuge der digitalen Transformation, die insbesondere zu Veränderungen bei der OT führt. Es entwickelt sich eine IT/OT-Konvergenz. Beide Bereiche kommen sich näher – gerade die OT übernimmt dabei Prozesse und Best-Practice-Ansätze der IT.

Im Folgenden wird diese Konvergenz näher beleuchtet. Eine große Rolle spielt dabei das Thema Cybersecurity, um das sich Unternehmen nun auch im OT-Bereich kümmern müssen.

Wandel der OT

Im Zuge der digitalen Transformation wandelt sich die OT. Dies betrifft verschiedene Bereiche. Ein wesentlicher Punkt ist hier das Thema Vernetzung. Die OT ist nicht mehr von der Außenwelt isoliert – die Abschottung nimmt sukzessive ab. Im Internet der Dinge (engl. Internet of Things [IoT] oder Industrial Internet of Things [IIoT]) sind auch Maschinen und Geräte der OT mit dem Internet verbunden. Außerdem nimmt im Produktionsbereich die Bedeutung von Cloudlösungen zu, wodurch IT-Infrastrukturen und Arbeitslasten in fremde Rechenzentren verlagert werden. Darüber hinaus werden die Maschinen und Geräte der OT zunehmend „intelligenter". Mithilfe von künstlicher Intelligenz (KI) kann in der Produktion die Automatisierung gesteigert werden. Sowohl in der maschinellen Produktion als auch im Produktionsumfeld ist KI in den verschiedensten Bereichen einsetzbar: Von der Produkt- und Prozessentwicklung über die Ressourcenplanung und den Einkauf bis hin zu Instandhaltung und Logistik. KI-gesteuerte Maschinen eröffnen neue Optionen zur Gestaltung des Produktionsprozesses, indem sie selbstständig Erkenntnisse gewinnen und Prozesse intuitiv steuern, welche dadurch weniger menschliche Intervention erfordern. Mit KI werden Maschinen befähigt, selbstständig zu lernen, sich zu optimieren und auf Änderungen zu reagieren.

Insgesamt wird die OT heterogener und vernetzter. Außerdem spielen immer mehr Aspekte bei der OT eine Rolle, die bisher verstärkt in der IT verortet sind. Damit kommen sich OT und IT immer näher.

IT/OT-Konvergenz

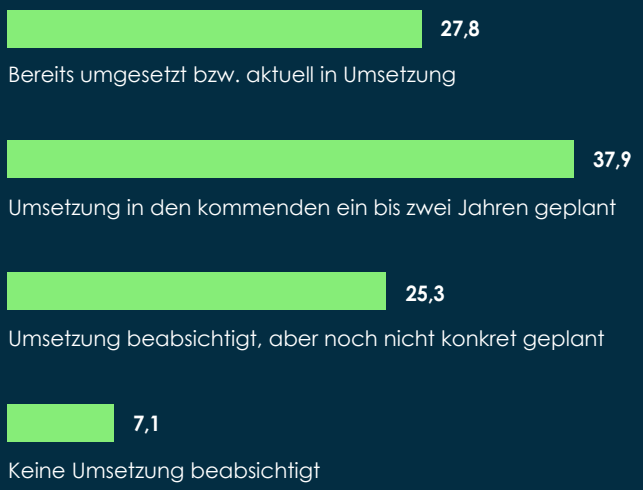
Die IT/OT-Konvergenz im Zuge der digitalen Transformation zeigt sich darin, dass die aus der IT bekannten und seit Jahrzehnten etablierten Prozesse und Prinzipien wie beispielsweise Asset Management, Service Level Agreements, Service Management und Steuerung der IT-Umgebung nun auch in der OT relevant werden. Ohne diese IT/OT-Konvergenz können die mit der Digitalisierung verbundenen Potenziale im Produktionsbereich nicht vollständig realisiert werden.

Mit der Konvergenz sind damit diverse Vorteile hinsichtlich Effizienz, Kosten und Produktivität verbunden. Werden die IT-Prozesse und -Prinzipien auch in der OT angewendet, können die Ressourcen effektiver und effizienter eingesetzt werden. Damit reduzieren die Unternehmen ihre Kosten.

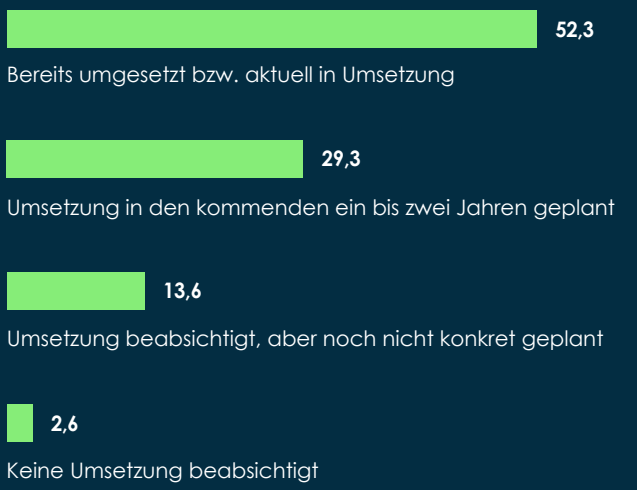
Außerdem kann mit der zunehmenden Nutzung der anfallenden Daten die Effizienz der OT gesteigert werden – und damit die Produktivität des gesamten Unternehmens. Des Weiteren ist im Zuge der Konvergenz eine Flexibilitätsverbesserung möglich. Mit der Einbindung von Echtzeit-Daten, durch die Vernetzung und KI-basierte Automatisierung kann die OT schneller an die Veränderungen der Rahmenbedingungen angepasst werden.

Weitere Best Practices rund um das Thema Daten, die von der IT auf die OT übertragen werden können, sind die richtige Umsetzung von Datentransparenz sowie eine sinnvolle Dokumentation von Ereignissen. Daraus können wiederum Ansätze zur Verbesserung der Prozesse abgeleitet werden.

IoT gewinnt in der Produktion zunehmend an Bedeutung
Anteil der befragten Unternehmensentscheider:innen, für die IoT in Zukunft wichtig für die Produktion ist, in Prozent; Differenz zu 100 Prozent: weiss nicht/keine Angabe



Cloud Services bereits bei mehr als der Hälfte der Unternehmen im Einsatz
Anteil der befragten Unternehmensentscheider:innen, für die Cloud Services in Zukunft wichtig für die Produktion sind, in Prozent; Differenz zu 100 Prozent: weiss nicht/keine Angabe



Quellen jeweils: Handelsblatt Research Institute / TeamViewer

Bei dieser Entwicklung darf allerdings nicht übersehen werden, dass OT und IT nicht nur ein Technologiethema sind. Prozesse und Personen müssen bei der IT/OT-Konvergenz ebenfalls mitberücksichtigt werden. Durch die bisherige Trennung beider Bereiche waren auch die Prozesse und die verantwortlichen Beschäftigten getrennt. Zwischen den IT- und OT-Teams gab es keine Zusammenarbeit. Diese Trennung zog sich durch bis in die Geschäftsführung. Denn typischerweise berichtete das OT-Team an den COO (Chief Operating Officer) und das IT-Team an den CIO (Chief Information Officer).

Mit zunehmender Konvergenz müssen beide Seiten stärker zusammenarbeiten. Hierbei gilt es auch, die unterschiedlichen Prioritäten in Einklang zu bringen. Das IT-Team strebt beim Einsatz von IT-Lösungen im Produktionsbereich an, die dortigen Prozesse zu verbessern. Für das OT-Team – Werksleiter:in und Fertigungsbeschäftigte – stehen hingegen hohe Effizienz und Qualität sowie geringe Ausfall- und Ausschussquoten im Vordergrund.

Der Wandel der OT im Zuge der digitalen Transformation führt zu anderen Prozessen bei den Beschäftigten. Gerade mit der zunehmenden autonomen Steuerung der Maschinen werden diese sich in erster Linie selbst überwachen. Erst auf der nächsten Ebene kontrollieren die Beschäftigten die OT und können damit für mehr Geräte verantwortlich sein als bisher – ohne größeren Aufwand. Außerdem wird nun auch Remote Work für den OT-Bereich möglich, zumindest ein Teil der Belegschaft kann die Tätigkeiten beispielsweise von zu Hause aus erledigen. Dies ist zugleich auch ein Treiber für die Veränderung.

Herausforderungen beim Wandel der OT

Aus dem Wandel der OT im Zuge der IT/OT-Konvergenz ergeben sich für die Unternehmen Herausforderungen, auf die sie reagieren müssen.

OT-Cybersecurity

Cybersecurity war in der Vergangenheit nur ein Randthema für den OT-Bereich. Aufgrund der Abtrennung vom IT-Bereich und dem Internet („Air Gap“) war die OT für Angreifer auf digitalem Weg nicht erreichbar. Die Unternehmen mussten nur den physischen Zugang überwachen und schützen, um die OT zu sichern.

Mit einer zunehmenden Vernetzung der OT und neue Technologien wie intelligenten Geräten sowie IoT ändert sich dies allerdings. Der Produktionsbereich wird zu einem möglichen Ziel von Cyberangriffen. Zuletzt haben diese Angriffe auf die OT zugenommen. Beispiele wie der Computerwurm Stuxnet zeigen, dass solche Schadprogramme am Ende auch physische Schäden erzeugen können.

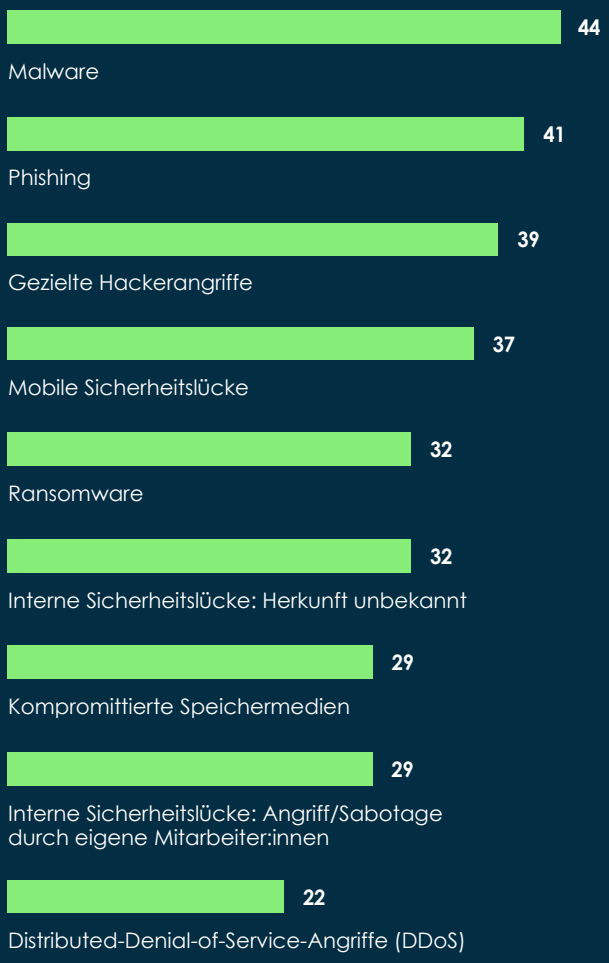
Unternehmen müssen deshalb das Thema Cybersecurity nun ebenfalls im OT-Bereich etablieren – mit allen relevanten Aspekten. Zu Beginn gilt es, die besonders schützenswerten Bereiche zu identifizieren – die „Kronjuwelen“, ohne die ein weiterer Betrieb nicht möglich ist. Anschließend müssen Bedrohungslage und Risikostatus untersucht werden. Davon leiten sich dann die Sicherheitsanforderungen ab. Hier kann der OT-Bereich auch von den langjährigen Erfahrungen mit der Cybersecurity im IT-Bereich lernen. So ist das dort erprobte

93%
der Unternehmen mit OT verzeichneten in den vergangenen zwölf Monaten mindestens einen Cyberangriff

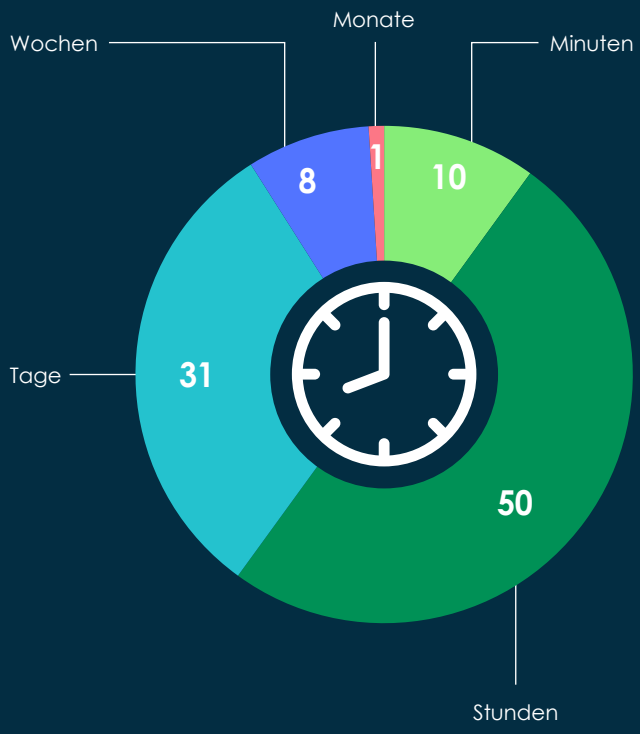
61%
der Angriffe führten zu Störungen bei der OT

90%
der Störungen dauerten Stunden oder länger bis zur Wiederherstellung der Systeme

Malware ist die Hauptangriffsart
Jew. Anteil der mehr als 500 befragten Unternehmen, die Cyberangriffe auf ihre OT-Infratsruktur erfasst haben, in Prozent; Mehrfachnennungen möglich



Die Störungen sind grösstenteils erst in Stunden oder Tagen behoben
Längste Dauer zur Behebung der Störung; Anteil der mehr als 500 befragten Unternehmen, die Cyberangriffe auf ihre OT-Infratsruktur erfasst haben, in Prozent



Quelle für alle Grafiken: FORTINET

Zero-Trust-Konzept auch für den OT-Bereich eine potenzielle Lösung. Bei Zero Trust wird grundsätzlich allen Diensten, Anwender:innen und Geräten misstraut. Deshalb haben sich sämtliche Anwender:innen und Geräte zu authentifizieren und der Datenverkehr ist grundsätzlich verschlüsselt. Alles und jeder wird regelmäßig überprüft und kontrolliert, bevor der Zugriff auf Unternehmensdaten und -netzwerke gewährt wird. Und auch wenn die Identität der Anwender:innen verifiziert ist, wird immer nur die niedrigste Zugriffsstufe gewährt, die zur Erledigung der Aufgaben ausreicht. Zusätzlich wird das OT-Netzwerk in kleinere Einheiten segmentiert, sodass Angreifer im Erfolgsfall nur Zugriff auf einen kleinen Teilbereich erlangen und nicht auf das gesamte Netzwerk.

Die Übertragung der Expertise vom IT-Bereich auf den OT-Bereich ist allerdings nur zu einem bestimmten Grad möglich. Denn es gibt auch unterschiedliche Bedingungen bei der Cybersecurity im OT-Bereich. So ist die OT – anders als mittlerweile die IT – nicht „per Design" auf Cybersicherheit ausgelegt. Die Systeme sind vielmehr so entwickelt, dass die Ausfallsicherheit und damit die Verfügbarkeit optimal sind. Dies betrifft geradeältere Systeme, die im OT-Bereich noch vielfach im Einsatz sind. Dazu kommt, dass regelmäßige Sicherheitsupdates bei OT-Systemen äußerst herausfordernd sind, da die Systeme nicht einfach für einen gewissen Zeitraum heruntergefahren werden können.

Was allerdings im OT-Bereich ähnlich wie im IT-Bereich bei der Cybersecurity wichtig ist: die Sensibilisierung und Schulung der Beschäftigten. Gerade für die OT-Belegschaft war Cybersecurity bisher kein Thema. Es ist erforderlich, den Beschäftigten die Gefahren aufzuzeigen und sie im richtigen sowie sicheren Umgang damit zu trainieren.

Legacy – Umgang mit den Alt-Systemen

Ein Risikofaktor mit Blick auf die Cybersecurity ist der Fakt, dass in der OT noch vielfach Alt-Systeme – Legacy – im Einsatz sind. Aus wirtschaftlichen Gründen können Unternehmen nicht ihre gesamte OT in einem Durchlauf erneuern. Vielmehr erstreckt sich die digitale Transformation der OT über einen langen Zeitraum, weshalb die OT-Landschaft sehr heterogen ist. Mit der Legacy steigt allerdings das Angriffsrisiko, da diese älteren Systeme noch aus einer Zeit stammen, wo Cyberangriffe kein Thema waren. Insofern gibt es keine eingebauten Schutzmaßnahmen dagegen. Zusätzlich sind auch oftmals noch ältere Betriebssysteme im Einsatz, die nur ein geringes Cybersecurity-Level aufweisen. Updates sind unter Umständen nicht mehr verfügbar oder Maßnahmen zur Verbesserung der Sicherheit nicht kompatibel.

Die Legacy bringt allerdings auch über den Cybersecurity-Aspekt hinaus Nachteile für die Unternehmen mit sich. Da in den Unternehmen weiterhin Alt-Systeme zum Einsatz kommen, kann das volle Potenzial der Digitalisierung nicht realisiert werden. Nicht alle Bereiche sind auf dem aktuellen technischen Stand und Prozesse werden unter Umständen durch eingeschränkte Kompatibilität verlangsamt.

Change Management

Die IT/OT-Konvergenz ist, wie erwähnt, kein reines Technologiethema, sondern erfordert auch eine Anpassung bei der Aufbau- und Ablauforganisation. Der Wandel der OT und das Übertragen von IT-Prozessen sowie -Prinzipien macht ein Change Management erforderlich. Aufgrund der unterschiedlichen Kultur und Prioritäten bei den OT-Beschäftigten kann die zunehmende Bedeutung von Best Practices aus der IT allerdings zu Konflikten führen. Zudem behindern organisatorische Barrieren die „neue" Art der OT-Arbeit. Genau daran muss gearbeitet werden. Es gilt, von vornherein Konflikte zu vermeiden und Einblicke in die Arbeit des IT-Teams zu ermöglichen. Etwaige Datensilos sollten aufgebrochen werden.

Darüber hinaus ist die Übernahme von IT-Prozessen und -Prinzipien auch mit neuen Qualifikationsanforderungen verbunden. Durch den verstärkten Einsatz von IT-Lösungen im OT-Bereich sowie die zunehmende Bedeutung von Cybersecurity benötigen die Beschäftigten die dafür erforderlichen Fähigkeiten. Das Training zum Aufbau des Know-hows kann „cross-sectional" – über OT und IT hinweg – gestaltet werden, um das Zusammenwachsen der Teams zu fördern.

Einschätzung von ServiceNow

Infolge des Booms von Industrie 4.0 sind die Technologien, die in Fertigungsumgebungen zum Einsatz kommen, zunehmend komplexer und integrierter geworden. Viele Fertigungsunternehmen sind jedoch weiterhin auf manuelle Prozesse und veraltete Verfahren angewiesen, um ihre OT am Laufen zu halten. Daher fällt es ihnen schwer, sich einen vollständigen Überblick über ihre OT zu verschaffen und die Mitarbeitenden, Prozesse und Technologien zu vernetzen.

Eine erfolgreiche IT/OT-Konvergenz kann nur stattfinden, wenn ein sicheres und einheitliches Konzept geschaffen wird, welches die digitale und die physische Welt miteinander vernetzt. Durch die Einführung von Smart-Factory-Technologien (zum Beispiel IoT-Devices) werden immer mehr Maschinen miteinander vernetzt und es steht eine große Menge an Daten zur Verfügung. Der Weg von der Erkenntnisgewinnung hin zu einer sinnvollen Maßnahmenumsetzung ist jedoch nach wie vor ein Kernproblem. Zunächst geht es darum, sich einen Überblick über die betriebliche Technologie zu verschaffen. Mit dieser Übersicht können Fertigungsanlagen und -prozesse effizient gesichert, überwacht und verwaltet werden.

Darüber hinaus stehen manuelle und fehleranfällige Prozesse im Fokus, da viele arbeitsintensive Fertigungsschritte nach wie vor nicht digitalisiert sind und Potenziale zur Produktivitätssteigerung nicht realisiert werden. Die Betriebstechnologie mit digitalen Arbeitsprozessen zu verbinden und mit künstlicher Intelligenz zu integrieren, kann Probleme in der Fertigung analysieren, diese reduzieren und die Produktivität steigern.

Wie kann ServiceNow dabei helfen?

ServiceNow hilft Unternehmen bei der digitalen Transformation zur Fertigungsindustrie 4.0, um die Produktivität zu steigern, Risiken zu verringern und die Kundenerfahrungen zu verbessern. Als Grundlage für alle digitalen Workflows verbindet die Now Platform® unternehmensweit Menschen, Funktionen und Systeme.

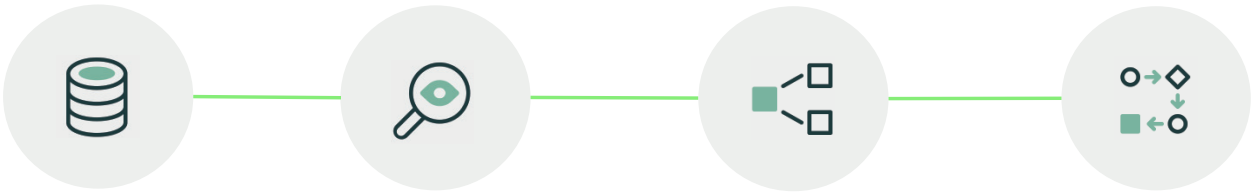
Unser Portfolio für die Produktionsumgebung umfasst die Lösung ServiceNow Operational Technology Management.

ServiceNow Operational Technology Management ermöglicht es Ihnen, eine vollständige Ansicht aller OT-Systeme mit Kontextinformationen zu erhalten. Mit Hilfe von digitalen Workflows können Sie Ihre Betriebstechnologie mit den Fertigungsprozessen verknüpfen, um bei Problemen oder Änderungen schnellstmöglich zu reagieren und den Betrieb wieder herzustellen.

Mit ServiceNow Operational Technology Management erhalten Unternehmen ein „Single System of Action" für die Fertigungsumgebung zur Unterstützung der Produktionseffektivität.

OPERATIONAL TECHNOLOGY MANAGEMENT

Eine zentrale Plattform, die Sie bei der Sicherung und Verwaltung all Ihrer OT-Systeme in Ihrem gesamten Fertigungsbetrieb unterstützt



OT-Foundation

Aufbau einer soliden Datengrundlage

OT-Visibility

Visualisierung aller IT&OT Assets

OT-Vulnerability Response

Kontrolle von kritischen Komponenten

OT-Service Management

Standardisierung des Servicegrads

Quelle: ServiceNow

Impressum

servicenow

Kontakt

Jürgen Schön,
Director, Manufacturing Industry GTM – EMEA,
juergen.schoen@servicenow.com

Sebastian Kapitza,
Advisory Solution Consultant,
sebastian.kapitza@servicenow.com

Über ServiceNow

Für eine Welt, in der Arbeit weniger Arbeit macht – das ist die Vision von **ServiceNow**. Wir transformieren manuelle Prozesse in moderne, digitale Workflows. Mitarbeiter und Kunden bekommen schnellen, unkomplizierten Zugriff auf Informationen und Dienstleistungen, so, wie sie es aus ihrem Privatleben gewohnt sind. Routine-Aufgaben werden strukturiert und automatisiert, Machine Learning und KI steigern die Effizienz und helfen, Fehler zu vermeiden und Probleme proaktiv zu adressieren. Die Now Platform®: Die intelligente und intuitive Cloud Plattform.

ServiceNow transformiert manuelle Prozesse in moderne, digitale Workflows – für eine Welt, in der Arbeit weniger Arbeit macht.

Handelsblatt
RESEARCH INSTITUTE

Das **Handelsblatt Research Institute (HRI)** ist ein unabhängiges Forschungsinstitut unter dem Dach der Handelsblatt Media Group. Es erstellt wissenschaftliche Studien im Auftrag von Kunden wie Unternehmen, Finanzinvestoren, Verbänden, Stiftungen und staatlichen Stellen. Dabei verbindet es die wissenschaftliche Kompetenz des 20-köpfigen Teams aus Ökonom:innen, Sozial- und Naturwissenschaftler:innen, Informationswissenschaftler:innen sowie Historiker:innen mit journalistischer Kompetenz in der Aufbereitung der Ergebnisse. Es arbeitet mit einem Netzwerk von Partner:innen und Spezialist:innen zusammen. Daneben bietet das Handelsblatt Research Institute Desk-Research, Wettbewerbsanalysen und Marktforschung an.

Konzept, Analyse und Gestaltung
Handelsblatt GmbH
Handelsblatt Research Institute
Toulouser Allee 27
40211 Düsseldorf
www.handelsblatt-research.com

Autor: Dr. Sven Jung
Layout: Kristine Reimann, Christina Wiesen
Bilder: unsplash, freepik

Stand: März 2023