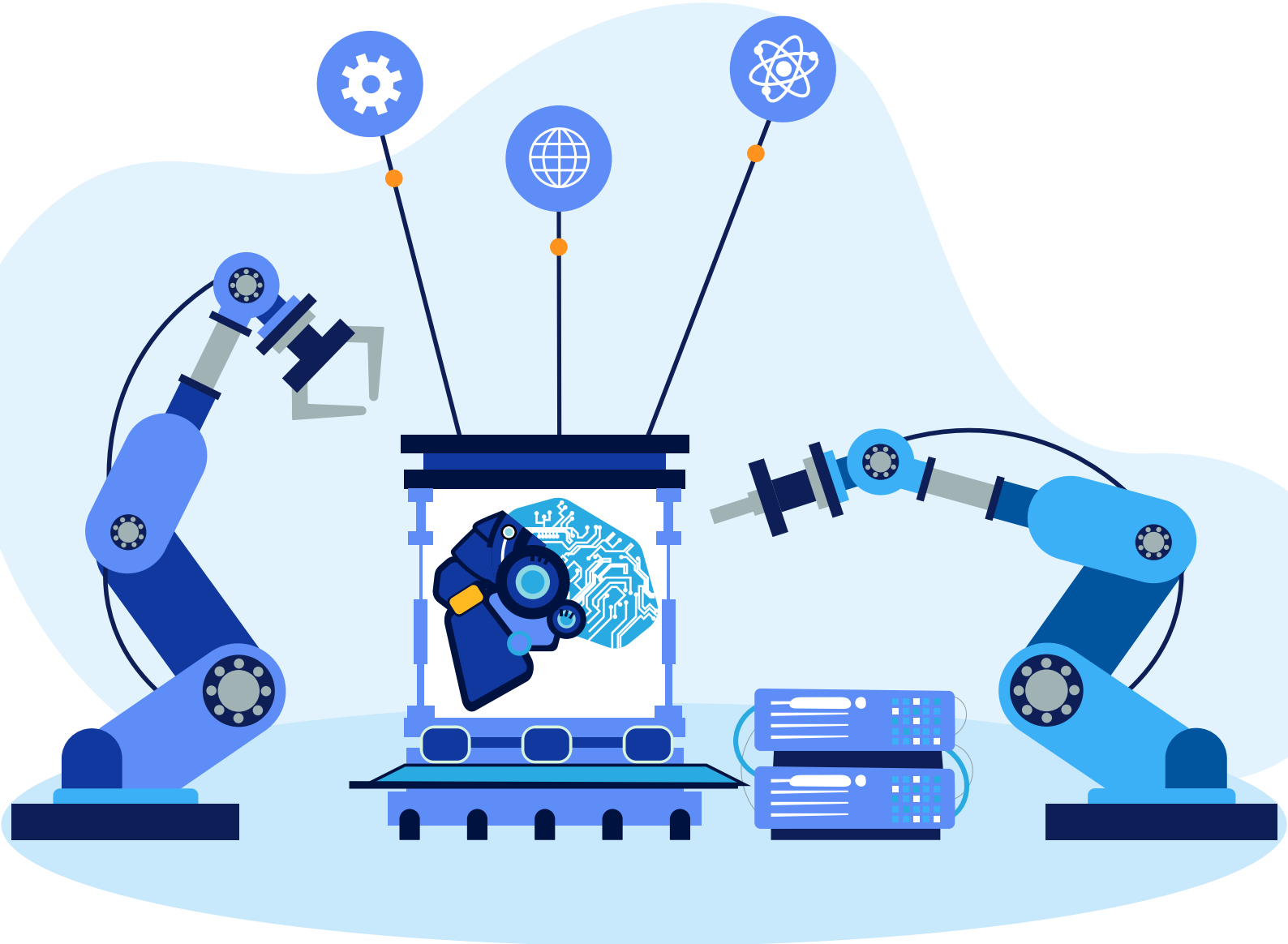


STUDIE

INDUSTRIAL IOT

2025



**DIE WICHTIGSTEN ERGEBNISSE
PRÄSENTIERT VON**



Matthias Teichmann
Director Research

Liebe Leserinnen, liebe Leser,

vielen Dank für Ihr Interesse an den Ergebnissen unserer Studie „Industrial IoT 2025“, die in Zusammenarbeit mit unserem Studienpartner Avanade entstanden ist. An der Umfrage von CIO und COMPUTERWOCHE, die im November 2024 online durchgeführt wurde, haben sich insgesamt 315 (IT-) Entscheiderinnen und Entscheider aus Unternehmen der D-A-CH-Region beteiligt. Es handelt sich dabei um Verantwortliche aus allen relevanten Unternehmensbereichen, vom C-Level über die Fachbereiche bis hin zum IT-Bereich. Befragt wurden insbesondere Unternehmen aus dem produzierenden Gewerbe.

Die Konjunktur in Deutschland lahmt derzeit stärker als in anderen europäischen Volkswirtschaften. Das hat auch damit zu tun, dass der Industriesektor hierzulande eine noch deutlich größere Bedeutung hat als anderswo. Chemie, Stahlproduktion, Maschinenbau, Automobilindustrie – das sind die Säulen der deutschen Wirtschaft. Gerade sie ächzen unter anhaltend hohen Energiekosten.

Wo über Massenentlassungen oder Werkschließungen diskutiert wird, da bleibt wenig Raum für große Investitionsprogramme, die für das Industrial Internet of Things (IIoT) notwendig wären. Und was ist mit denen, die schon frühzeitig ihre IIoT-Hausaufgaben gemacht haben? Haben diese jetzt mehr Entscheidungsspielraum? Wie die Studie zeigt, ist der Reifegrad bei der IIoT-Umsetzung insgesamt noch als eher gering einzustufen, aber immerhin: In etwas mehr als der Hälfte der befragten Unternehmen findet das Industrial

IoT Anwendung. Ein Anfang ist definitiv gemacht, und die ersten Erfahrungen mit IIoT sind absolut ermutigend.

Als wichtigste IIoT-Anwendungsszenarien werden die Steuerung bzw. Automatisierung der Produktion sowie Predictive Maintenance genannt und eine Mehrheit von Unternehmen erreicht seine primären Ziele bei der Einführung von IIoT-Anwendungen: Sechs von zehn Unternehmen steigern durch den Einsatz von IIoT die Produktionseffizienz und vier von zehn Unternehmen verbessern die Produktqualität. Und das, obwohl jeweils 40 Prozent der Unternehmen durch Fachkräftemangel und Datensicherheits- und Datenschutzbedenken gebremst wurden.

Apropos Sicherheit: Die von der NIS2-Richtlinie betroffenen Unternehmen haben vor allem mit dem Aufbau einer (internen) Sicherheitsorganisation (53%) und einer kontinuierlichen OT-Risikobewertung (47%) reagiert. Und: Die Unternehmen setzen auf standardisierte IIoT-Schnittstellen. Allen voran sind hier ERP-Systeme (47%) zu nennen, die eine Art Datendrehscheibe für die Produktion darstellen.

Weitergehende Details zu diesen genannten Themen finden Sie nun in diesem Studienreport mit den wichtigsten Ergebnissen der Industrial IoT-Studie 2025.

Wir wünschen Ihnen viele spannende Erkenntnisse.

Automatisierung der Produktion als wichtigste IIoT-Anwendung, Fachkräftemangel und Sicherheitsbedenken bremsen aus

Automatisierung und Steuerung der Produktion sowie Predictive Maintenance sind die wichtigsten Einsatzszenarien des IIoT in Unternehmen. Größte Herausforderungen bei der Umsetzung sind der Mangel an qualifiziertem Personal und Bauchschmerzen bei Datensicherheit und Datenschutz.

Wichtigste IIoT-Anwendung in Unternehmen ist aktuell die Produktionsautomatisierung und -steuerung (53 Prozent), insbesondere in den großen Unternehmen (58 Prozent). Dahinter folgen Predictive Maintenance (45 Prozent), sprich Zustandsüberwachung und vorausschauende Wartung, sowie Supply Chain Management und Logistik (44 Prozent).

Weitere wichtige Anwendungsfälle für das Industrial Internet of Things sind Energie- und Ressourcenmanagement (41 Prozent), Anlagen- und Maschinenüberwachung (38 Prozent) sowie Qualitätskontrolle und -sicherung (36 Prozent).

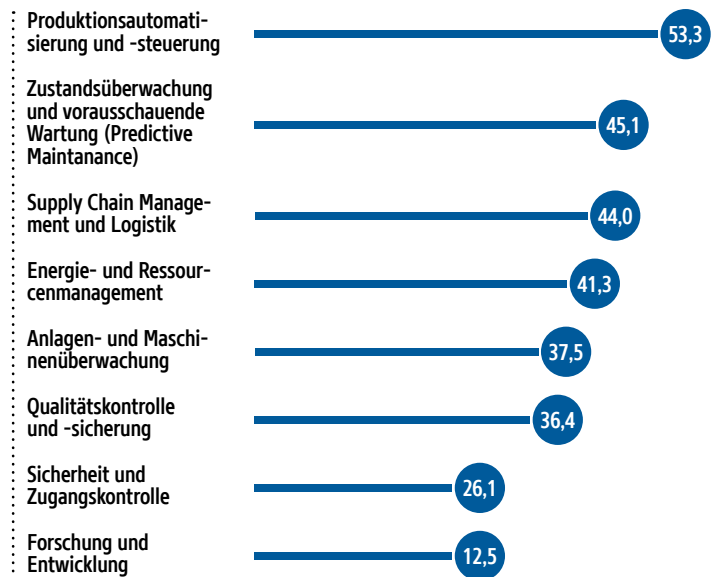
All diese Einsatzszenarien stehen direkt oder indirekt mit der Effizienz der Produktion und dem Einsparen von Kosten/Ressourcen in Verbindung. Angesichts der hohen Energiekosten überrascht auch der hohe Wert für Energiemanagement nicht.

Als größte Herausforderungen bei der Umsetzung dieser IIoT-Anwendungen nannten 41 Prozent der Befragten den Mangel an qualifiziertem Personal, 40 Prozent Bedenken bei Datensicherheit und Datenschutz. In etwas mehr als einem Drittel der Unternehmen stellen die hohen Investitionskosten sowie die Komplexität der Integration in bestehende Systeme Hürden für das IIoT dar.

Hinzu kommen technologische Kompatibilitätsprobleme, Schwierigkeiten bei der Datenanalyse und -interpretation und Bedrohungen der industriellen Cybersicherheit durch Angreifer.

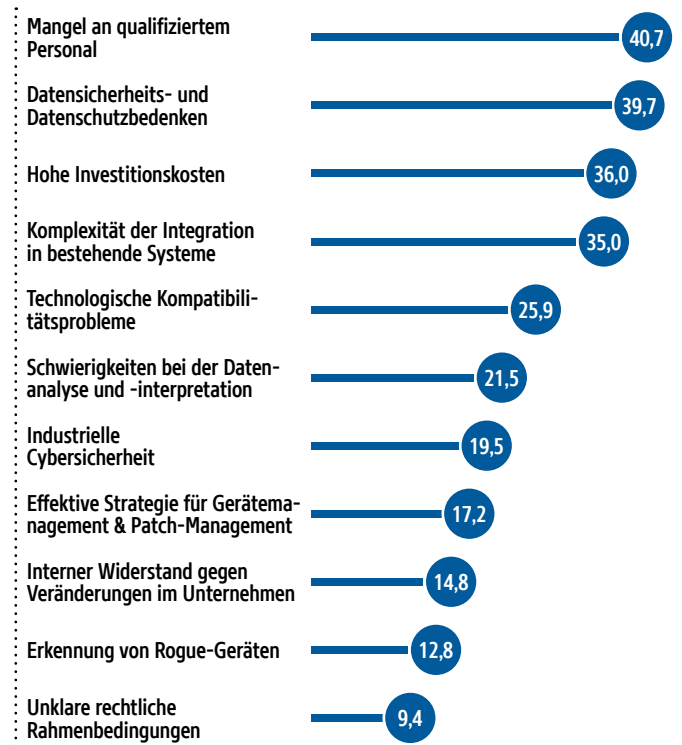
Auf welchen Gebieten kommt das IIoT in Ihrem Unternehmen zum Einsatz?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen mit ersten IIoT-Pilotprojekten bis hin zu Unternehmen, die bereits einen breiten Roll-out umgesetzt haben. Basis: n = 185



Was sind aus Ihrer Sicht in Ihrem Unternehmen die größten Herausforderungen beim Einsatz des Industrial IoT?

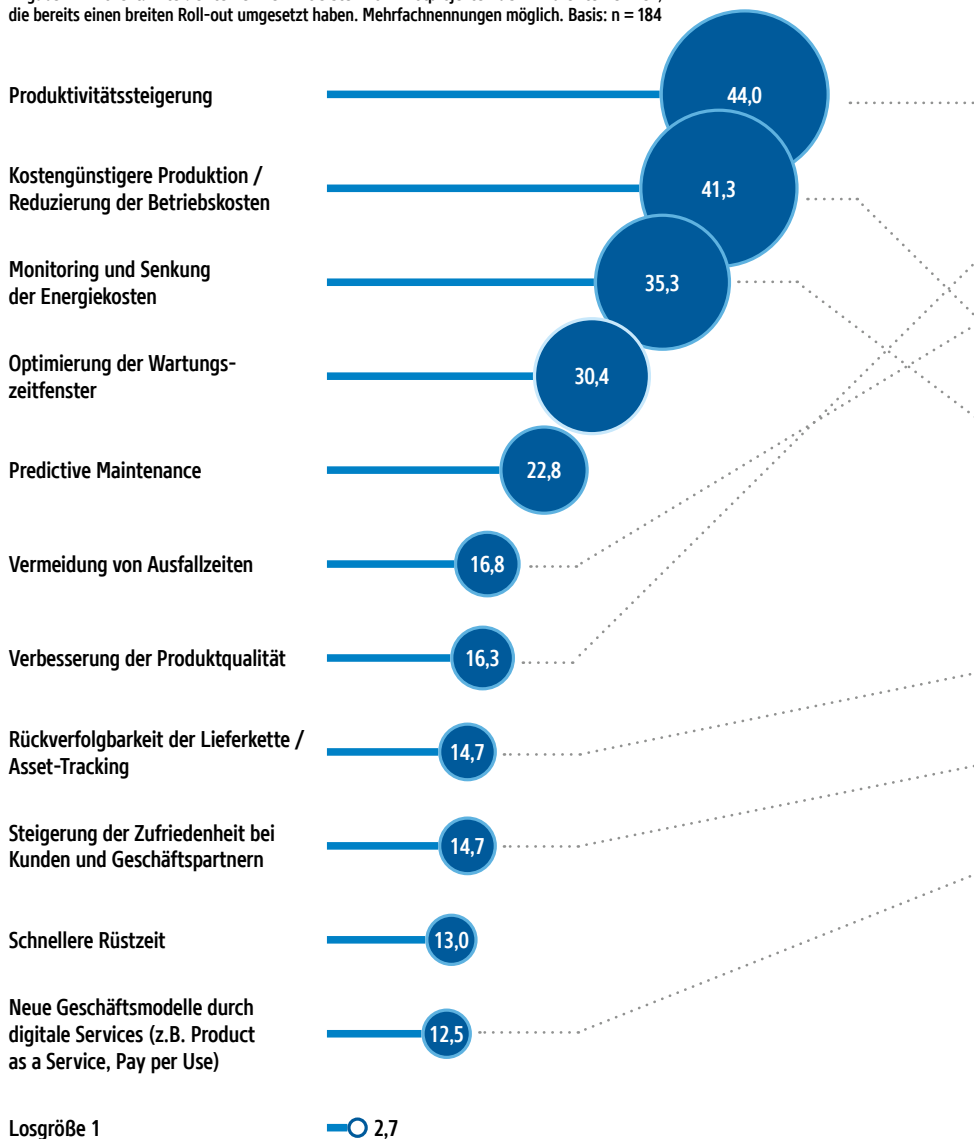
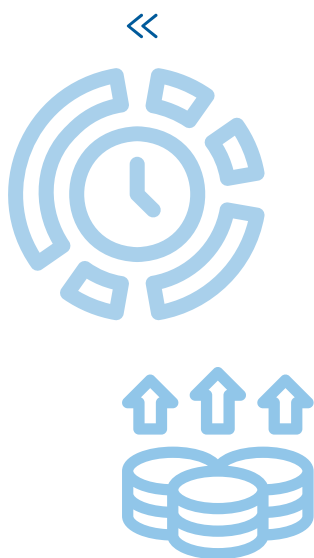
Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 297



Was sind (waren) die primären Ziele Ihres Unternehmens bei Einführung der IIoT-Anwendungen?

Angaben in Prozent. Filter: Unternehmen mit ersten IIoT-Pilotprojekten bis hin zu Unternehmen, die bereits einen breiten Roll-out umgesetzt haben. Mehrfachnennungen möglich. Basis: n = 184

>>
Optimierte Prozesse und
Kostensparen stehen
absolut im Vordergrund.

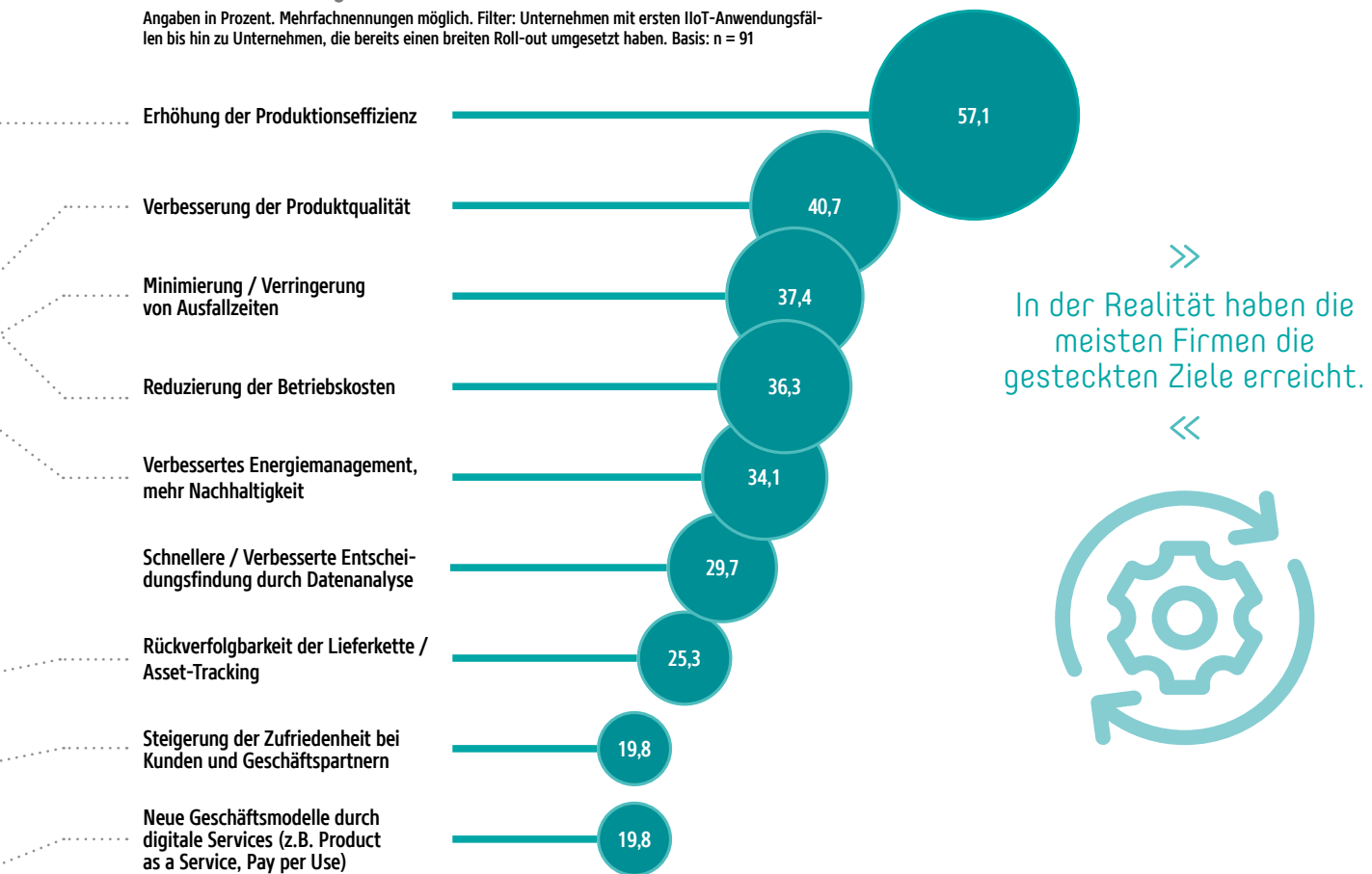


Wichtigste Vorteile: Effizienz in der Produktion und höhere Produktqualität

Die meisten Firmen haben ihre primären Ziele bei der Einführung von IIoT-Anwendungen erreicht. Sie profitieren vor allem von einer effizienteren Produktion und verbesserten Produkten. Die Entwicklung neuer Geschäftsmodelle steht im Hintergrund.

Welche Vorteile haben Sie durch den Einsatz von IIoT in Ihrem Unternehmen festgestellt?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen mit ersten IIoT-Anwendungsfällen bis hin zu Unternehmen, die bereits einen breiten Roll-out umgesetzt haben. Basis: n = 91



„Was sind (waren) die primären Ziele Ihres Unternehmens bei Einführung der IIoT-Anwendungen? Nennen Sie bitte maximal drei Ziele.“

Bei den Antworten auf diese Frage landen Themen rund um die effiziente Produktion vorn: Produktivitätssteigerung (44 Prozent), kostengünstigere Produktion/Reduzierung der Betriebskosten (41 Prozent), Monitoring und Senkung der Energiekosten (35 Prozent), Optimierung der Wartungszeitfenster (30 Prozent) oder Predictive Maintenance (23 Prozent).

Auf dem letzten Platz bei den Zielen für IIoT-Projekte stehen neue Geschäftsmodelle durch digitale Services (z.B. Product as a Service, Pay per Use) mit nur 13 Prozent (20 Prozent größere Unternehmen).

Das heißt: Optimierte Prozesse und Kosten sparen stehen absolut im Vordergrund, die

Erschließung neuer Geschäftsmodelle durch das IIoT ist zweitrangig.

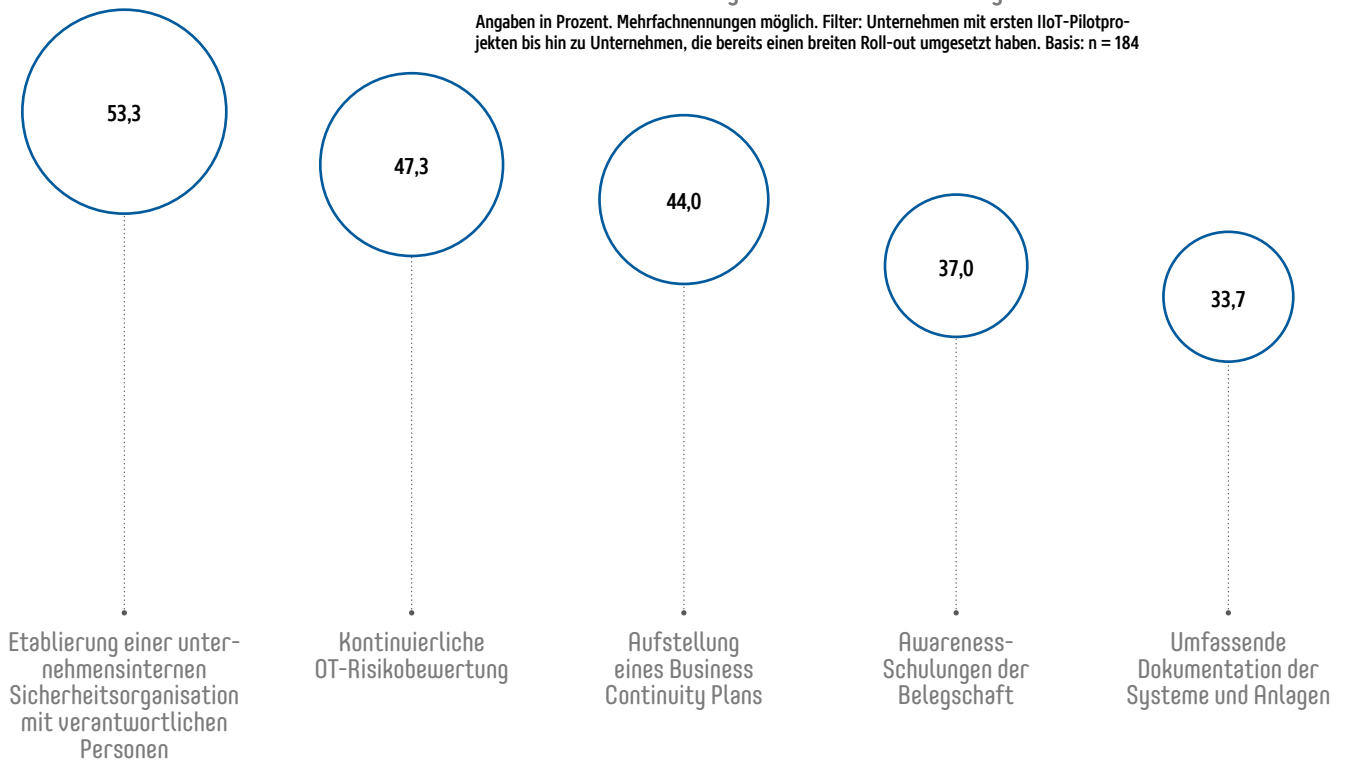
In der Realität haben die meisten Firmen die gesteckten Ziele erreicht. 57 Prozent der Firmen konnten mit ihren IIoT-Anwendungen ihre Produktionseffizienz erhöhen, 41 Prozent ihre Produktqualität steigern. Interessante Diskrepanz: Bei den Zielen nannten nur 16 Prozent der Befragten verbesserte Produkte.

Jeweils rund ein Drittel der Unternehmen konnte mit Hilfe des IIoT die Ausfallzeiten minimieren, Betriebskosten reduzieren oder das Energiemanagement verbessern.

Zukunftsorientierte Themen wie höhere Kundenzufriedenheit oder die Erschließung neuer Businessmodelle landen mit jeweils 20 Prozent auf den beiden letzten Plätzen.

Welche der folgenden organisatorischen OT-Schutzmaßnahmen haben Sie zur Einhaltung der NIS2-Richtlinie umgesetzt?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen mit ersten IIoT-Pilotprojekten bis hin zu Unternehmen, die bereits einen breiten Roll-out umgesetzt haben. Basis: n = 184



Von NIS2 betroffen: Sicherheitsorganisation und SOC als wichtigste organisatorische oder technische OT-Schutzmaßnahmen

Die NIS2-Richtlinie fordert von den betroffenen Firmen umfangreiche Maßnahmen zum Schutz vor Cyberangriffen. Viele Firmen haben dafür bereits eine interne Sicherheitsorganisation oder ein Security Operation Center (SOC) aufgebaut.

Die europäische NIS2-Richtlinie (Network and Information Security) zielt auf die Verbesserung der Cybersecurity und des Schutzes kritischer Infrastrukturen ab. Sie tritt wohl im ersten Halbjahr 2025 in Kraft. Ob ein Unternehmen unter die NIS2-Vorgaben fällt, hängt von seiner Branche, Unternehmensgröße und dem Jahresumsatz ab. Auch für produzierende Firmen ist die NIS2 relevant.

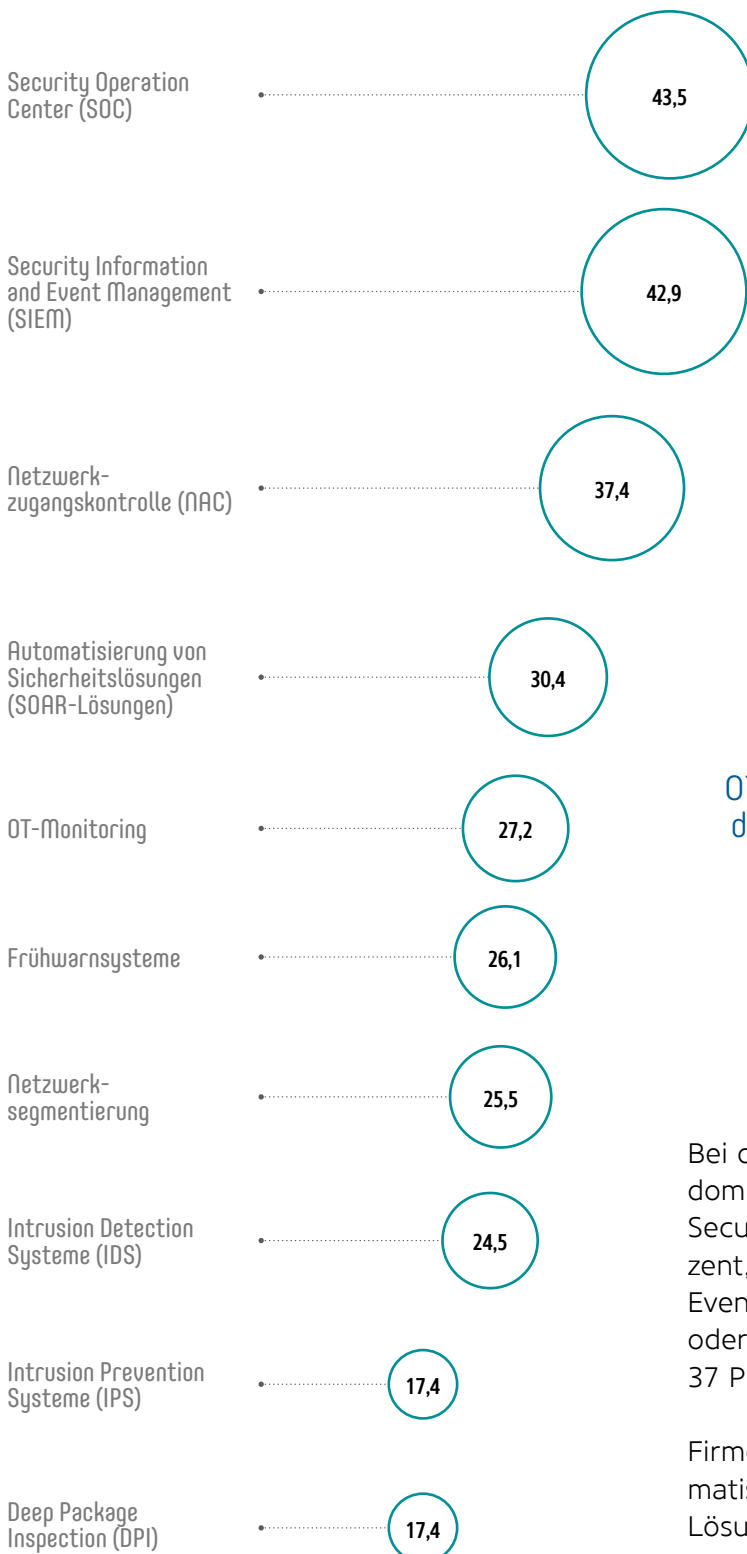
Die befragten Unternehmen der IIoT-Studie haben bereits organisatorische und technische OT-Schutzmaßnahmen zur Einhaltung der NIS2-Anforderungen umgesetzt.

Bei den organisatorischen Schutzmaßnahmen haben 53 Prozent eine unternehmensinterne Sicherheitsorganisation mit verantwortlichen Personen etabliert, 47 Prozent bewerten ihre OT-Risiken kontinuierlich, 44 Prozent haben einen Business-Continuity-Plan aufgestellt.

Weitere wichtige organisatorische Maßnahmen sind Awareness-Schulungen der Belegschaft, die umfassende Dokumentation der Systeme und Anlagen (Asset Management) sowie Patch-Management und Sicherheitsupdates.

Welche der folgenden technischen OT-Schutzmaßnahmen haben Sie zur Einhaltung der NIS2-Richtlinie eingeführt beziehungsweise umgesetzt?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen mit ersten IIoT-Pilotprojekten bis hin zu Unternehmen, die bereits einen breiten Roll-out umgesetzt haben. Basis: n = 184



»
Die befragten Unternehmen der IIoT-Studie haben bereits organisatorische und technische OT-Schutzmaßnahmen zur Einhaltung der NIS2-Anforderungen umgesetzt.
«

Bei den technischen OT-Schutzmaßnahmen dominieren Themen wie die Einrichtung eines Security Operation Centers (SOC) mit 44 Prozent, Lösungen zum Security Information and Event Management (SIEM) mit 43 Prozent oder zur Netzwerkzugangskontrolle (NAC) mit 37 Prozent.

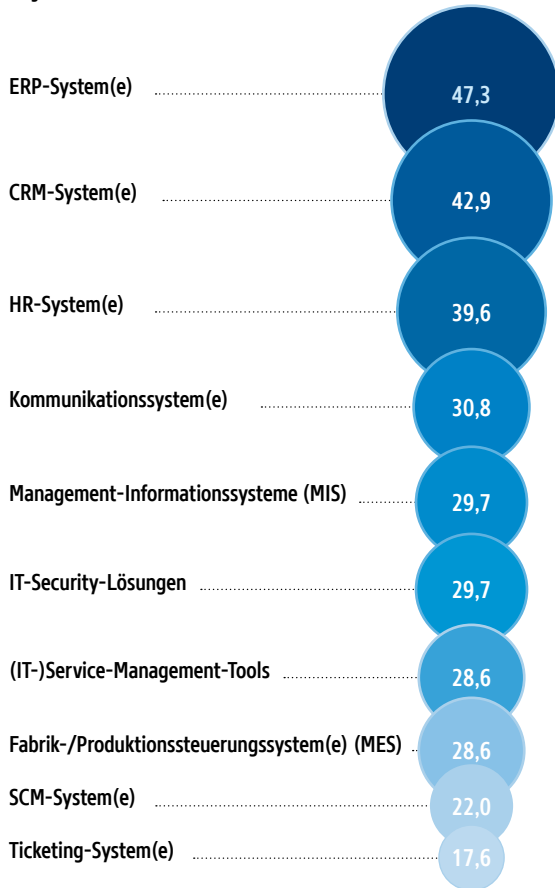
Firmen schützen sich zudem durch die Automatisierung von Sicherheitslösungen (SOAR-Lösungen), OT-Monitoring, Frühwarnsysteme, Netzwerksegmentierung oder Intrusion Detection Systeme (IDS) beziehungsweise Intrusion Prevention Systeme (IPS).

4 Vernetzung mit anderen Systemen: Mehrheit der Firmen setzt auf standardisierte IIoT-Schnittstellen

Sei es ERP, CRM oder HR – Unternehmen vernetzen ihre IIoT-Anwendungen verstärkt über standardisierte IIoT-Schnittstellen mit anderen Systemen.

In welchen anderen Systemen Ihres Unternehmens gibt es Schnittstellen zu Ihrem Industrial IoT?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen mit ersten IIoT-Anwendungsfällen bis hin zu Unternehmen, die bereits einen breiten Roll-out umgesetzt haben. Basis: n = 91



Die häufigsten Anwendungen im Unternehmen mit Schnittstellen zum Industrial IoT sind ERP-Systeme (47 Prozent), die eine Art Datendreh-scheibe für die Produktion bilden. Relativ knapp dahinter liegen Schnittstellen des IIoT-Systems zu CRM-Systemen (43 Prozent) und HR-Systemen (40 Prozent).

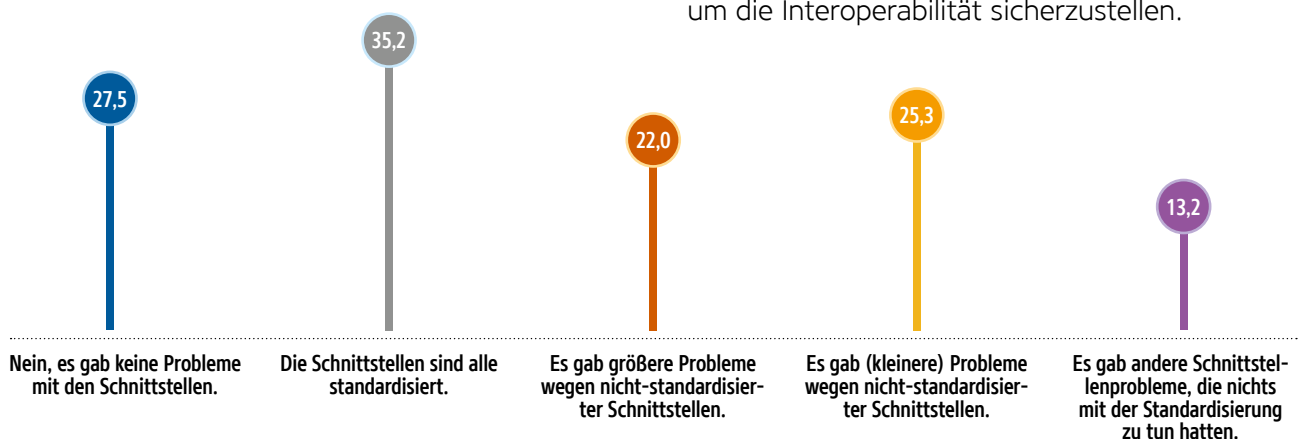
Mit etwas Abstand, nahezu gleichauf bei etwa rund 30 Prozent, folgt ein Quintett an Anwendungen: Kommunikationssysteme, Management-Informationssysteme (MIS), IT-Security-Lösungen, (IT-)Service-Management-Tools und Fabrik-/Produktionssteuerungssystem(e) (MES).

22 Prozent der Unternehmen haben IIoT-Schnittstellen zu ihrem Supply-Chain-Management-System, 18 Prozent zu ihren Ticketing-Systemen eingerichtet.

Allerdings verzeichnen 47 Prozent der Firmen kleinere bis größere Probleme (25 bzw. 22 Prozent) wegen nicht-standardisierter Schnittstellen. In 13 Prozent gab es andere Schnittstellenprobleme, die nichts mit der Standardisierung zu tun hatten. Und positiv, dass es bei immerhin 28 Prozent keine Probleme mit den Schnittstellen gab.

Gibt (oder gab) es Probleme mit diesen Schnittstellen, weil diese nicht standardisiert waren?

Angaben in Prozent. Filter: Unternehmen, die über eine oder mehrere IIoT-Schnittstellen verfügen. Mehrfachnennungen möglich. Basis: n = 91



Der Hauptgrund: Mittlerweile sind in 56 Prozent der Firmen alle Schnittstellen standardisiert (bei den großen Firmen 63 Prozent). 35 Prozent planen den Aufbau standardisierter Schnittstellen, um die Interoperabilität sicherzustellen.

So gelingt Digitalisierung im Mittelstand

Die Studie zeigt: Große Unternehmen haben aktuell die Nase vorn beim Thema IIoT. Die Experten und Expertinnen von Avanade geben vier konkrete Tipps, wie mittelständische Unternehmen hier Schritt halten können.

Fokus auf Effizienz

IIoT nachhaltig in Produktionsprozesse zu implementieren, erfordert weit mehr als eine rein technische Umsetzung. Unternehmen müssen von Anfang an auch die wirtschaftlichen Zielsetzungen eines solchen Projekts ins Auge fassen – und dann konsequent darauf hinarbeiten. Genau darin liegt die Spezialität von Avanade. Wir behalten den Business Value unserer Kunden jederzeit im Blick. Zusammen mit unseren Kunden analysieren wir, welche Szenarien den größten Impact haben, und priorisieren die Maßnahmen auf dem Weg dorthin. Das Resultat sind pragmatische Lösungen, die schnell umgesetzt werden und für einen zeitnahen Return on Investment sorgen.

Erfahrung zählt sich aus

Obwohl viele der befragten Unternehmen ihre Kompetenz beim Thema IIoT als hoch einschätzen, möchten die wenigsten bei der Umsetzung auf einen erfahrenen Partner verzichten. Avanade bringt den nötigen externen Sachverstand mit, der internes Know-how im Unternehmen sinnvoll ergänzt. Die Basis dafür sind Erfahrungen aus zahlreichen IIoT-Projekten, die wir für große und mittelständische Produzenten in der DACH-Region bereits umgesetzt haben. Dadurch verfügen wir über Templates, Frameworks und Assets, die eine reibungslose Implementierung von IIoT-Anwendungen in eine bestehende Prozesslandschaft erleichtern. Zusätzlich können wir wertvolle Insights liefern, um neue Perspektiven zu eröffnen und Stakeholder im Unternehmen zu überzeugen.

Sicherheit geht vor

Die Studie zeigt deutlich: Sicherheitsbedenken sind aktuell einer der großen Bremsklötze beim Thema IIoT. Viele Unternehmen sind unsicher, wie sie ihre wertvollen Daten und auch ihre Maschinen zuverlässig vor Angreifern schützen. Avanade berücksichtigt bei der Implementierung von IIoT-Anwendungen stets auch das Thema Security. So sind produzierende Unternehmen bestens aufgestellt bei den Themen Sicherheit, Compliance und der Einhaltung gesetzlicher Standards wie der NIS2-Richtlinie. Zusätzlich beraten wir interne Sicherheitsexperten, unterstützen beim Aufbau eines Secure Operation Center, schulen Mitarbeitende oder stellen einen Business-Continuity-Plan auf.

Integration hat viele Facetten

IIoT-Projekte erfordern ein hohes Maß an Vernetzung. Dazu gehört im ersten Schritt natürlich die Verbindung von IT und OT. Hier unterstützt Avanade bei der Wahl der Hardware, der Implementierung der Software und der Orchestrierung beider Welten. Wir verbinden das IIoT-System mit ERP-, CRM- oder HR-Anwendungen und helfen, Daten zusammenzuführen, zu standardisieren und intelligent verfügbar zu machen. Mit Hilfe von künstlicher Intelligenz eröffnen wir Unternehmen zusätzliche Möglichkeiten der Effizienzsteigerung. Ebenso kümmern wir uns um die Anbindung unterschiedlicher Standorte oder Partnerfirmen.



„Wir behalten die strategischen Ziele eines IIoT-Projekts im Blick und führen auch konkret die Implementierung auf dem Shopfloor durch.“

Guido Burchartz,
Avanade Industry Lead Products,
D-A-CH

Avanade Deutschland

Tel.: +49 6173 9463 800
germany@avanade.com
www.avanade.de

Avanade Österreich

Tel.: +43 676 844 111 0
austria@avanade.com
www.avanade.at

Avanade Schweiz

Tel.: +41 43 430 43 43
switzerland@avanade.ch
www.avanade.ch

Studiensteckbrief

- Herausgeber** CIO, CSO und COMPUTERWOCHE
- Studienpartner** Avanade Deutschland GmbH
- Grundgesamtheiten** Oberste (IT-)Verantwortliche in Unternehmen der DACH-Region: Beteiligte an strategischen (IT-)Entscheidungsprozessen im C-Level-Bereich und in den Fachbereichen (LoBs); Entscheidungsbefugte sowie Experten und Expertinnen aus dem IT-Bereich und dem Produktionsbereich
- Teilnehmergenerierung** Persönliche E-Mail-Einladung über die exklusive Unternehmensdatenbank von CIO, CSO und COMPUTERWOCHE sowie – zur Erfüllung von Quotenvorgaben – über externe Online-Access-Panels
- Gesamtstichprobe** 315 abgeschlossene und qualifizierte Interviews
- Untersuchungszeitraum** 11. bis 18. November 2024
- Methode** Online-Umfrage (CAWI)
- Fragebogenentwicklung und Durchführung** Custom Research Team von CIO, CSO und COMPUTERWOCHE in Abstimmung mit dem Studienpartner

Impressum

**Studienkonzept/
Fragebogenentwicklung:**
Matthias Teichmann

**Endredaktion/
CvD Studienberichtsband:**
Matthias Teichmann, Armin Rozsa

Analysen/Kommentierungen:
Jürgen Mauerer, München

**Hosting/Koordination
Feldarbeit:**
Armin Rozsa

Studienpartner:

Avanade Deutschland GmbH
Campus Kronberg 1
61476 Kronberg
Telefon: +49 6173 9463 800
E-Mail: germany@avanade.com
Web: www.avanade.com

Grafik:
Christine Plote, Starnberg

Umschlaggestaltung unter
Verwendung einer Illustration
von © shutterstock.com/
Anne Rodrigo

Lektorat:
Elke Reinhold, München

Ansprechpartner:
Matthias Teichmann
matthias.teichmann@foundryco.com

Herausgeber:

**Foundry
(formerly IDG Communications)**

Anschrift:
IDG Tech Media GmbH
Georg-Brauchle-Ring 23
80992 München
Telefon: +49 89 36086 0
Fax: +49 89 36086 118

Vertretungsberechtigter:
Jonas Triebel, Geschäftsführer

Registergericht:
Amtsgericht München, HRB 99110

Umsatzsteueridentifikationsnummer:
DE 811 257 834

Weitere Informationen unter:
www.foundryco.com

Alle Angaben in diesem Ergebnisband wurden mit größter Sorgfalt zusammengestellt. Trotzdem sind Fehler nicht ausgeschlossen. Verlag, Redaktion und Herausgeber weisen darauf hin, dass sie weder eine Garantie noch eine juristische Verantwortung oder jegliche Haftung für Folgen übernehmen, die auf fehlerhafte Informationen zurückzuführen sind. Der vorliegende Ergebnisberichtsband, einschließlich all seiner Teile, ist urheberrechtlich geschützt. Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen, auch auszugsweise, bedürfen der schriftlichen Genehmigung durch den Herausgeber.