IDC

Eine IDC Infografik, gesponsert von Utimaco

IIoT erfolgreich und sicher umsetzen

Industrial IoT in Deutschland

2022

Für **3 von 10** Industrieunternehmen sind momentan die wichtigsten operativen Prioritäten, **Ausfallzeiten zu verringern** und die **Geschäftskontinuität zu erhöhen.**

Dabei können Industrial IoT und die Vernetzung von IT und OT (Operational Technology) durch robuste datenbasierte Entscheidungen und agilere Produktionsprozesse helfen.

Gleichzeitig schafft IIoT die Basis für neue Geschäftsmodelle und enge Collaboration mit anderen Unternehmen.

75 %

...der befragten Unternehmen haben sich schon mit anderen zu **Industry Ecosystems** zusammengeschlossen.

Für mehr Stabilität und Resilienz können sie in diesen:

- → **gemeinsam Daten, Anwendungen, Anlagen oder Prozesse nutzen**
- → **zusammen datenbasierte Produkte, Services und Geschäftsmodelle aufbauen**

Cybersecurity ist ein häufiges Hindernis für IIoT-Projekte

Für **23 %** gehören der Schutz von **geistigem Eigentum** und **Cybersecurity** zu den **größten Hindernissen** bei der Teilnahme an **Industry Ecosystems.**

Für **21 %** der Industrieunternehmen gehören **Sicherheitsbedenken** zu den größten **Herausforderungen** bei der generellen **IIoT-Umsetzung.**

Die IIoT-Sicherheitsbedenken sind vielfältig

Top-3-Cybersecurity-Herausforderungen bei IIoT

28 % Mangelnde Kommunikation zwischen IT- und OT-Teams über gemeinsame Gefahren

26 % Schutz von IIoT-Daten in Bewegung und Ruhe

23 % Mangelnder Überblick über IIoT-Endpunkte im Netzwerk

69 % der Industrieunternehmen stimmen zu, dass die **Verbesserung der OT-Sicherheit** Motivation für die **Integration von IT und OT** ist.

Die Zusammenarbeit von IT und OT ist notwendig: Absicherung von IIoT mit IT-Lösungen kann große Risiken bergen

Beispiel: Remote Access – Monitoring, Wartung oder Steuerung von OT aus der Ferne

42 % nutzen dafür nur **herkömmliche IT-Lösungen** wie VPNs, Firewalls, NAC, das öffentliche Internet und andere IT-basierte Behelfslösungen.

31 % nutzen stattdessen **spezielle IIoT- oder OT-Lösungen** und moderne Ansätze auf Basis von **SDN, SASE oder ZTNA.**

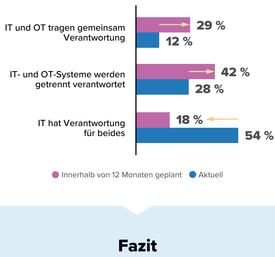
21 % haben noch keinen Remote Access eingerichtet.

6 % Weiß nicht

Die IT ist noch zu oft allein für die Cybersecurity von IT- und OT-Umgebungen zuständig

Die geteilte oder gemeinsame Verantwortung für IIoT-Cybersecurity kann dabei helfen:

- → **mangelnde Kommunikation zu verbessern**
- → **gegenseitige Vorbehalte abzubauen**
- → **IT- und OT-Fachwissen in die Absicherung einfließen zu lassen**
- → **den Einsatz von zweckentfremdeten IT-Security-Lösungen zu reduzieren**



Fazit

- **Betrachten Sie aktuelle Krisen nicht als IIoT-Hürden, sondern überlegen Sie, wie IIoT zu besseren, schnelleren Entscheidungen und mehr Agilität beitragen könnte.**
- **Forcieren Sie die IT/OT-Integration, denn sie ist Basis für effektive Zusammenarbeit zwischen IT und OT und damit auch ganzheitliche industrielle Cybersicherheit.**
- **Evaluieren Sie Ihre IIoT-Security. Zweckentfremdete IT-Security-Lösungen stellen ein Risiko dar. Neue Ansätze wie ZTNA oder SASE und spezielle IIoT-Security-Solutions sind für optimalen Schutz notwendig.**

IDC hat 250 Unternehmen aus industriellen und industrienahen Branchen mit mehr als 100 Mitarbeitern im Januar und Februar 2022 befragt, um Einblicke in die aktuelle Entwicklung und Herausforderungen bei der Umsetzung von IIoT zu erlangen.
Alle Abbildungen wurden auf die wichtigsten Erkenntnisse gekürzt.

Quelle: IDC Studie „Industrial IoT in Deutschland 2022", April 2022

IT-Security gesponsert von

utimaco