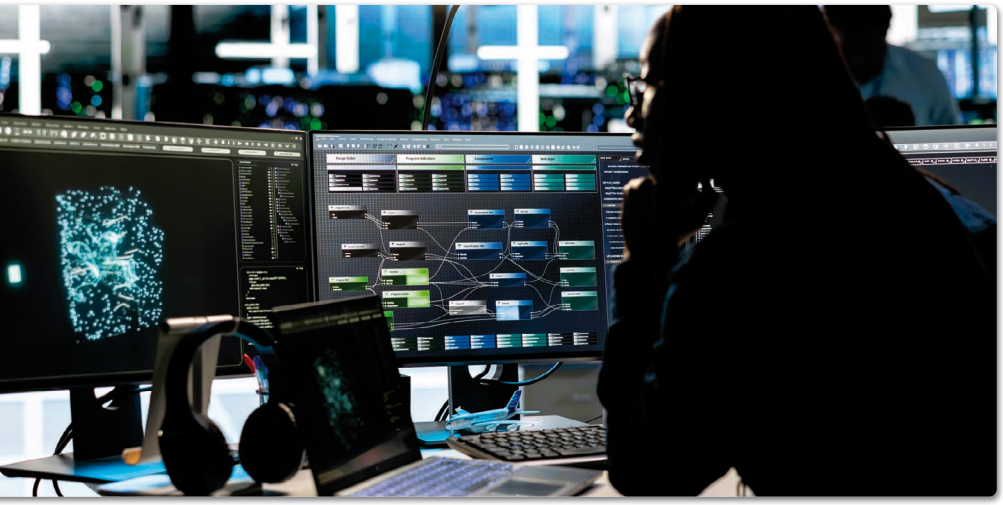
NIS2-Umsetzung ab 2026

Industrielle Fertigung besonders betroffen



Überwachung vernetzter Systeme: NIS2 verlangt durchgängige Kontrolle © Obrela/Freepik

Mit Verspätung hat die Bundesregierung die Umsetzung von NIS2 beschlossen. Ab 2026 tritt das Cybersicherheits-Gesetz nun auch in Deutschland vollständig in Kraft. Besonders für Industrieunternehmen – von der Fertigung bis zum Maschinenbau – steigt damit der Handlungsdruck entlang komplexer Liefer- und Produktionsketten deutlich.

Eine der gravierendsten Änderungen von NIS2 betrifft den deutlich erweiterten Geltungsbereich: Neben klassischen KRITIS-Betreibern rücken nun auch zahlreiche Industrie-, Technologie- und Dienstleistungsbranchen in den Fokus. Insgesamt sind damit rund 30.000 Unternehmen in Deutschland erfasst.

Die Richtlinie unterscheidet dabei zwischen „wesentlichen“ und „wichtigen“ Einrichtungen. Wesentlich sind Organisationen, deren Ausfall die Grundversorgung oder die öffentliche Sicherheit unmittelbar gefährdet. Wichtig sind dagegen Unternehmen, deren Ausfall kritisch, aber nicht sofort versorgungsrelevant ist – etwa Medizintechnik-, Elektronik- oder Maschinenbauer, Lebensmittelproduzenten oder Forschungseinrichtungen.

Fünf Sektoren, die NIS2 besonders fordert

Entscheidend ist jedoch weniger die Frage, ob ein Unternehmen unter NIS2 fällt, sondern wie stark es die neuen Vorgaben spürt. Branchen mit verteilten OT-Systemen, tiefen Dienstleisterketten oder hohen Versorgungsrisiken stehen vor besonders hohem Aufwand. In der Umsetzung zeigt sich: Fünf Sektoren trifft es deutlich härter als den Rest – aufgrund ihrer Strukturen, Abhängigkeiten und operativen Kritikalität.

- **Energieversorgung**
  Der Energiesektor ist durch die Energiewende einer der am stärksten digitalisierten OT-Bereiche. Smart-Meter-Gateways, automatisierte Laststeuerung, digitale Netzleittechnik und tausende dezentrale Erzeuger treffen auf jahrzehntealte OT-Anlagen – eine Angriffsfläche, die gezielt ausgenutzt wird. Stadtwerke spüren den Druck besonders: kleine Teams, begrenzte Budgets und verteilte Anlagen führen dazu, dass NIS2 vor allem Transparenz in OT-Netzen und frühzeitige Bedrohungserkennung verlangt.
- **Gesundheitssektor**
  Ransomware-Gruppen nutzen die hohe digitale Abhängigkeit in Kliniken aus. Malware gefährdet nicht nur Daten, sondern unmittelbar Menschenleben, während veraltete Medizingeräte und unklare Asset-Landschaften zusätzliche Risiken schaffen. Für Kliniken bedeutet NIS2 vor allem: MedTech-Umgebungen sichtbar machen und privilegierte Zugänge strikt kontrollieren.
- **Finanzsektor**
  Die Finanzbranche bleibt eines der lukrativsten Ziele: Angriffe auf Zahlungsprozesse, API-Ketten und ausgelagerte Dienste treffen auf komplexe, historisch gewachsene IT-Architekturen. NIS2 fordert hier vor allem strengere Audits von Dienstleistern, Härtung privilegierter Zugänge und kontinuierliches Monitoring kritischer Zahlungsströme.
- **Transport**
  Transport zählt zu den „wesentlichen Einrichtungen“. Kombinationen aus Alt-Systemen, hoher Zuliefererzahl und selten aktualisierten Anwendungen erhöhen das Risiko. NIS2 macht die Koordination und Dokumentation zahlreicher Schnittstellen zur zentralen Herausforderung.

Industrie im Visier der Angreifer

In der fertigenden Industrie sind Stillstände, Lieferunterbrechungen und lange Wiederanlaufzeiten längst reale Szenarien. Laut Digital Universe Report H1 2025 [1] entfallen 7% aller beobachteten Vorfälle auf diesen Sektor. Das sind rund 800 Angriffe allein im ersten Halbjahr 2025 und damit eine kontinuierlicher Angriffswelle im Wochentakt. Die Spannbreite reicht von kompromittierten Bediener-Accounts über Manipulationen an Maschinenabläufen bis zu Eingriffen in Logistikprozesse oder unerlaubten Änderungen an Steuerungssystemen. Die Motive reichen von finanziellen Interessen bis hin zu gezielter Betriebsspionage.

Ein Kernproblem: Klassische OT wurde nie für das Internet gebaut. Viele Steuerungen laufen seit Jahrzehnten, sind kaum patchbar oder basieren noch auf Windows XP Embedded. Gleichzeitig hängen heute IIoT-Sensorik, Cloud-Dienste, MES- und ERP-Systeme im selben Netzwerk – oft ohne klare Segmentierung.

NIS2 erhöht den Druck für Hersteller

Besonders für industrielle Fertiger verschärft NIS2 die Lage, denn Produktionslinien, Zuliefererverbünde und Remote-Wartungszugänge erzeugen eine Angriffsfläche, die sich kaum vollständig kontrollieren lässt. Das zeigt auch eine aktuelle Studie des Digitalverbands Bitkom [2] in Deutschland: 28% der befragten Unternehmen berichten darin von Angriffen auf ihre Zulieferer oder von einem entsprechenden Verdacht innerhalb der letzten zwölf Monate. In 41% dieser Fälle hatte der Cybersicherheitsvorfall direkte Folgen auf Lieferkette, Produktion und Reputation.

Autor:
Stefan Bange
Managing Director Germany
Obrela
www.obrela.com

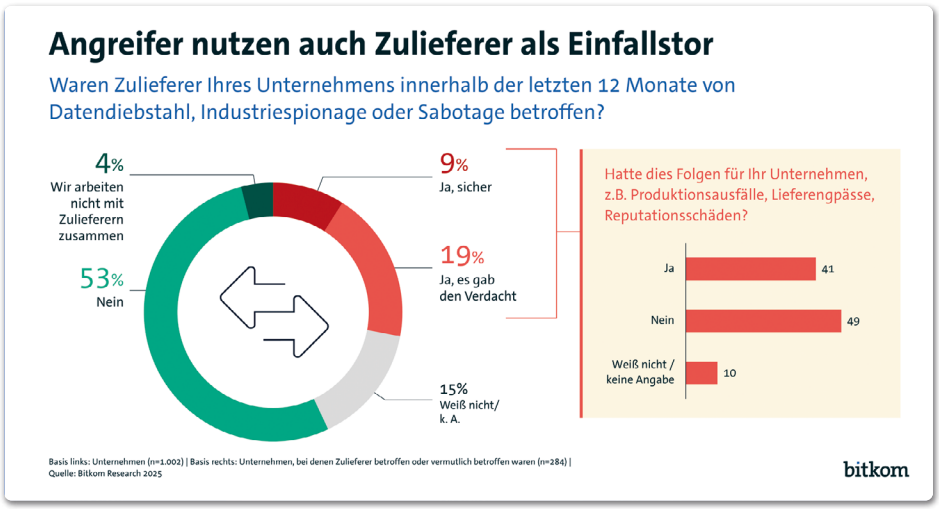
Jede Störung wirkt sich damit nicht nur operativ, sondern auch wirtschaftlich aus: Liefertermine geraten ins Wanken, internationale Kundenketten erwarten Nachweise über Sicherheitsstandards, und Maschinenstillstände verursachen schnell sechsstellige Kosten.

Hinzu kommt die wachsende Zahl digitaler Integrationen – von Predictive-Maintenance-Plattformen bis zu smarten Materialflüssen. Damit rückt die gesamte Produktionsumgebung in den Fokus: Asset-Transparenz, kontinuierliche Überwachung, gesicherte OT-Updates, Lieferkettenkontrollen und Protokollierung von Eingriffen werden zu verpflichtenden Kernprozessen. Für Maschinen- und Anlagenbauer bedeutet NIS2 zudem, dass auch sie als Dienstleister auditierbar werden und ihre Remote-Zugänge, Serviceprozesse und Softwarebereitstellung nachweislich absichern müssen.

Best Practices für NIS2: Grundlagen

Für die Umsetzung von NIS2 sind einige grundlegende Sicherheitsmaßnahmen unverzichtbar. Sie bilden das Fundament für eine wirksame Risiko¬steuerung, klare Prozesse und eine nachweisbare Compliance. Das folgende Set an Best Practices fasst die zentralen Schritte zusammen, die Unternehmen branchenübergreifend berücksichtigen sollten.

- **Strukturiertes Risiko-Management etablieren**
  Organisationen sollten formale Richtlinien zur Risikoanalyse und Informationssicherheit definieren und diese kontinuierlich über ein zentrales Framework überwachen, etwa durch Managed Risk & Controls (MRC).
- **Robustes Incident Handling sicherstellen**
  Klare Prozesse, getestete Abläufe und ein kontinuierliches Monitoring sind nötig, um Vorfälle schnell zu erkennen und zu beheben. Managed Detection Response(MDR)-Dienste unterstützen Echtzeit-Detektion und Reaktion.
- **Business Continuity und Disaster Recovery fest verankern**
  Unternehmen benötigen einen formalisierten Business Continuity Plan (BCP; Notfallplan), regelmäßige Backup-Tests und klare Wiederanlaufstrategien, um auch unter Belastung handlungsfähig zu bleiben.
- **Cyberrisiken in der Lieferkette aktiv managen**
  Durchgängige Risikoanalysen, definierte Sicherheitsanforderungen für Zulieferer und regelmäßige Sicherheitsprüfungen von Integrationen minimieren Schwachstellen entlang der Supply Chain.
- **Sichere Entwicklung und Systempflege gewährleisten**
  Sicherheitsanforderungen müssen in Beschaffung und Entwicklung verankert, Schwachstellen regelmäßig getestet und Patch- sowie Vulnerability-Management kontinuierlich betrieben werden.
- **Wirksame Kontrolle der Sicherheitsmaßnahmen überprüfen**
  KPIs, kontinuierliche Risikoüberprüfung und Echtzeit-Einblicke in die Wirksamkeit von Kontrollen helfen, die eigene Sicherheitslage messbar und auditierbar zu halten.



Managed Security statt Alleingang

NIS2 wird für viele Unternehmen vor allem eines: ein Ressourcenproblem. Organisationen scheitern nicht an der Technik, sondern an fehlender Transparenz, begrenzten Teams und der Vielzahl an Schnittstellen. NIS2 verlangt durchgängiges Monitoring und schnelle Reaktionsfähigkeit – Anforderungen, die viele Unternehmen nur mit externen Partnern rund um die Uhr abdecken können.

Security-as-a-Service-Modelle bieten hier eine realistische Entlastung. Externe Partner übernehmen Aufgaben wie MDR, MRC, die Pflege zentraler Sicherheitsrichtlinien sowie die Bewertung neuer Schwachstellen. So entstehen klare Verantwortlichkeiten, ein durchgängiger Überblick über Risiken und eine Reaktionsfähigkeit, die rund um die Uhr funktioniert. Das sind alles Voraussetzungen, die NIS2 jetzt verpflichtend macht und viele Organisationen aus eigener Kraft nur schwer erfüllen können.

Wer schreibt

Stefan Bange ist seit mehr als 15 Jahren im Bereich IT-Sicherheit und Cybersicherheit tätig, wobei sein Fokus auf MSSP, Compliance und Threat Intelligence Services liegt. Als Geschäftsführer Deutschland unterstützt er Unternehmen dabei, ihre Cybersecurity-Operation zu stärken und mit den Managed Security Services von Obrela Sicherheitsrisiken effektiv zu minimieren.◀

Quellen

[1] Obrela: Digital Universe Report H1 2025; www.obrela.com/de/report/digitales-universum-bericht-h1-2025-bericht/

2] Bitkom: IT-Sicherheit: Angreifer nehmen Zulieferer ins Visier; www.bitkom.org/Presse/Presseinformation/IT-Sicherheit-Angreifer-Zulieferer