In
Industrie

Fe
Fertigung

indevis

DAS CYBERSECURITY-PLAYBOOK FÜR UNTERNEHMEN AUS DER INDUSTRIE & FERTIGUNG

Eine Checkliste für Geschäftsführer (CEO), Chief Information Officer (CIO), Chief Information Security Officer (CISO) und OT Security-Verantwortliche

Warum dieses Playbook?

Ein Cyberangriff kann in Sekunden vernichten, wofür Sie Jahre gearbeitet haben.
Unternehmen aus der Industrie und Fertigungsbranche operieren in einem Umfeld, in dem die Zuverlässigkeit der Infrastruktur, stabile Lieferketten und etwaige Produktionsausfälle über Erfolg und Misserfolg entscheiden. Die oftmals unterschätzte Gefahr: Ein einziger erfolgreicher Angriff kann enorme Schäden durch Produktionsstopps oder Prozessunterbrechungen verursachen.

Laut dem IBM Cost of Data Breach Report 2025[1] liegt der globale Durchschnitt der Kosten für ein Datenleck bei **3,7 Mio. Euro**. Der durchschnittliche Schaden bei Vorfällen in deutschen **Industrieunternehmen** liegt bei **6,67 Mio. Euro** – der höchste Wert aller untersuchten Branchen. Bitkom[2] meldet zudem, dass **81 % der deutschen Unternehmen** bereits Opfer von Cyberangriffen wurden – der gesamtwirtschaftliche Schaden: rund **267 Mrd. Euro** jährlich.

Die Historie zeigt: Insolvenzen nach Cyberangriffen nehmen deutlich zu, Unternehmen sind oft binnen weniger Wochen bis Monate existenziell gefährdet. Denn Produktionsunterbrechungen treffen direkt die Bilanz. Neben den finanziellen und operativen Risiken dürfen Unternehmen aus der Industrie & Fertigung zudem die zunehmenden regulatorischen Verpflichtungen nicht außer Acht lassen, die Cybersicherheit heute zwingend vorschreiben.

Cybersicherheit ist daher nicht mehr optional, sondern eine notwendige Investition gegen Bedrohungsakteure.

Für Entscheidungsträger ist es heute wichtiger denn je zu erkennen: Mangelnde Cyber-Resilienz stellt ein existenzielles Risiko für die deutsche Industrie dar.

Die Incident-Response- und Threat-Intelligence-Teams von indevis haben hunderte Angriffe analysiert und daraus die wichtigsten Lehren gezogen – einschließlich Maßnahmen, die sich Unternehmen im Nachhinein gewünscht hätten. Dieses Playbook fasst diese Erkenntnisse zusammen und bietet eine praxisorientierte Anleitung, wie sich Unternehmen aus der Industrie & Fertigung auf Cyber-Vorfälle vorbereiten, sie bewältigen und überstehen können.

Neben einer fünfstufigen Checkliste, die Ihnen hilft, Cyber-Resilienz systematisch aufzubauen, erhalten Sie mit der Cyber-Sicherheitsampel ein Instrument zur schnellen Bewertung des Sicherheitsstatus Ihres Unternehmens.

Business Impact: Cybersecurity als strategischer Wettbewerbsvorteil

Cybersecurity hat sich vom reinen IT-Thema zum strategischen Bewertungs- und Überlebensfaktor entwickelt. Fehlende Sicherheitsmaßnahmen führen nicht nur zu hohen Schadenskosten, sondern gefährden Lieferketten und Produktionsabläufe:

MKS Instruments verpasste beispielsweise aufgrund einer Betriebsunterbrechung durch einen Cyberangriff Umsatzziele in Höhe von **170 Mio. Euro**, und auch der Zulieferer Applied Materials spürte durch diesen Angriff auf die Lieferkette Effekte bis **215 Mio. Euro**.[3]

Noch kritischer sind Ransomware-Angriffe, die die gesamte IT-Infrastrukturen lahmlegen. Dann steht das Geschäft still: Keine Aufträge, keine Produktion, keine Rechnungen. Ein aktuelles Beispiel ist die Fasana GmbH: Nach einem Angriff im Mai 2025 stand der Betrieb zwei Wochen still, es entstanden über **2 Mio. Euro** Umsatzverlust, bereits im Juni musste das Unternehmen **Insolvenz** anmelden.[4]

43 %

der durch einen Ransomware-Angriff kompromittierten Daten sind nicht wiederherstellbar (Veeam Software Ransomware Trends Report 2024)[6]

20%

der Unternehmen geben an, dass ein schwerwiegender Cyberangriff sie nahezu in die Insolvenz geführt hätte (Hiscox Cyber Readiness Report 2022)[7]

Umgekehrt steigert nachweisbare Compliance, etwa durch ISO 27001, das Vertrauen von Kunden, Geschäftspartnern und Investoren. Studien zeigen: Für Unternehmen sind etablierte Cybersecurity-Standards entscheidend für das operative Überleben.[5]

„Einhundert Prozent Cybersicherheit gibt es nicht und wird es nie geben. Die Frage ist deswegen nicht ob, sondern wann ein erfolgreicher Cyberangriff stattfindet. Wir müssen das Cybersicherheitsniveau in Deutschland daher insgesamt substantiell erhöhen."[8]

Claudia Plattner, BSI-Präsidentin

Cybersecurity in 5 Schritten

Cyber-Resilienz ist heute ein zentraler Pfeiler verantwortungsvoller Unternehmensführung – besonders für Unternehmen aus Industrie und Fertigung.
Wer Cyber-Risiken wirksam steuern will, muss sie nicht isoliert betrachten, sondern fest im strategischen Steuerungsrahmen des Unternehmens verankern. Genau hier setzt unsere Checkliste an: Sie bietet Entscheidungsträgern einen klaren, praxisnahen Fahrplan, um Cyber-Resilienz strukturiert aufzubauen, Risiken zu minimieren und Wettbewerbsvorteile durch sichere Lieferketten und Produktionsabläufe zu nutzen.

1. Cyber-Risiken in die Unternehmensführung integrieren

Cyber-Resilienz beginnt im Management. Damit Sicherheitsfragen nicht isoliert in der IT betrachtet werden, sollte die Entscheiderriege ein Governance-Modell etablieren, in dem Cyber-Risiken als fester Bestandteil der Unternehmenssteuerung verankert sind. Die Verantwortung für Cybersicherheit muss klar zugewiesen, regelmäßig überprüft und in Vorstandssitzungen sichtbar gemacht werden.

Kernmaßnahmen zur Umsetzung:

Durchführung einer Cyber-Resilience- / Risikoanalyse (CRA)

- Einschätzung der Sicherheitslage mittels Threat-Led Profiling
- Gap-Analyse zur Abdeckung bestehender Risiken durch die Cyber-Versicherung
- Penetrationstests zur Validierung der Verteidigungsmechanismen
- Klassifizierung technischer Risiken nach der OWASP Top 10 Infrastructure Security Risks, z. B. unzureichende Zugangskontrollen, fehlende Netzwerksegmentierung, unsichere Standardkonfigurationen, schwaches Patch-Management
- Bewertung der identifizierten Bedrohungen anhand von Eintrittswahrscheinlichkeit und wirtschaftlichem Schaden

Einführung eines quartalsweisen Cyber-Reportings zur

- Analyse der aktuellen Bedrohungslage
- Bewertung von Erkennungsleistung und Resilienzgrad
- Aktualisierung von Notfallplänen und Reaktionsrichtlinien

2. Cyber-Resilienz-Strategie entwickeln

Eine gute Strategie erkennt nicht nur Risiken – sie priorisiert, schützt, reagiert und stellt im Ernstfall alles wieder her. Das Ziel ist eine Resilienzarchitektur, die dem Prinzip folgt: „Identify, Protect, Detect, Respond, Recover."

Vorgehensweise:

Risikoanalyse und Bedrohungsbewertung durchführen

- Risiken identifizieren und quantifizieren
- Finanzielle, operative und reputationsbezogene Auswirkungen erfassen
- Berichte als Grundlage für Investitionsentscheidungen nutzen (NCSC-Empfehlungen)

Prioritäten und Ressourcen festlegen

- Höchste Risiken priorisieren und ressourcenschonend adressieren
- Investitionsumfang und Budgetplanung mit dem Board abstimmen

Strategie mit Geschäftszielen verbinden

- Sicherheitsvision für den Exit festlegen
- Gap-Analyse zwischen Ist- und Soll-Zustand durchführen
- Wertvollste Assets identifizieren und absichern
- BCDR-Pläne (Business Continuity & Disaster Recovery) aktualisieren und regelmäßig testen

3. Schulungen & Awareness auf Managementebene

Kontinuierliche Schulungen stellen sicher, dass das Management und die wichtigsten Teams Cyber-Risiken besser einschätzen und im Ernstfall angemessen reagieren können.

Vorgehensweise:

- Regelmäßige Management-Trainings zu aktuellen Cyber-Bedrohungen und regulatorischen Pflichten durchführen
- Awareness-Programme für alle Mitarbeitenden etablieren, mit Fokus auf Phishing, Passwortsicherheit und Incident-Reporting
- Spezialisierte Vertiefungstrainings für Hochrisikobereiche wie IT, Recht und Finanzen anbieten
- Einen Cyber-Verantwortlichen ernennen, der Zuständigkeiten definiert und regelmäßig an das Board berichtet

4. Incident-Response-Bereitschaft herstellen

Eine vorbereitete und getestete Incident-Response-Strategie ermöglicht es, Schäden zu begrenzen und Ausfallzeiten zu minimieren, wenn ein Angriff eintritt.

Vorgehensweise:

- Incident-Response-Plan (IR) entwickeln und regelmäßig durch Simulationen (z. B. Tabletop-Übungen) testen
- Krisenkommunikation vorbereiten: interne und externe Kommunikationswege (Kunden, Medien, Behörden) definieren
- Externe Incident-Response-Dienste frühzeitig vertraglich sichern und in Notfallprozesse einbinden
- Nach Tests Lessons Learned dokumentieren und Pläne fortlaufend optimieren

5. Kontinuierlich überwachen und anpassen

Da sich Bedrohungen und regulatorische Anforderungen ständig ändern, muss die Cybersicherheitsstrategie laufend überprüft und angepasst werden.

Vorgehensweise:

- 24/7-Überwachung über MDR (Managed Detection and Response) / SOC (Security Operations Center)-Services etablieren, um Angriffe frühzeitig zu erkennen
- Regelmäßige Schwachstellenscans und Audits durchführen und Prioritäten dynamisch anpassen
- KPIs wie Reaktionszeit und Wiederherstellungszeit messen und verbessern
- Neue Vorgaben (z. B. NIS-2, DSGVO, IT-SiG) fortlaufend integrieren

Neue Cybersecurity-Pflichten: Was Sie jetzt beachten müssen

In der DACH-Region steigen die regulatorischen Anforderungen an Cybersicherheit – mit direkter Auswirkung auf Unternehmenswert und Haftungsrisiken.

Strengere Pflichten

- Mit **NIS-2** sind nun noch mehr Unternehmen zu verbindlichem Cyber-Risikomanagement, inkl. präventiver Maßnahmen und kontinuierlicher Überwachung verpflichtet.
- Im Falle eines Cyberangriffs gelten strenge Meldepflichten ähnlich wie bei der DSGVO (Datenschutz-Grundverordnung).
- Gefordert sind einheitliche europäische Mindeststandards: u. a. technische Schutzmaßnahmen, Notfallpläne, regelmäßige Audits und Risikobewertungen.
- Die **DSGVO** regelt den Umgang mit personenbezogenen Daten, inklusive Meldepflichten bei Datenschutzverletzungen.
- Das **IT-Sicherheitsgesetz** enthält ergänzende Anforderungen für Betreiber kritischer Infrastrukturen (KRITIS), darunter insbesondere zusätzliche Nachweis- und Meldepflichten gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

Bis zu
20 Mio. €
oder 4 %
Umsatz

Sanktionen

- **Bußgelder:** Bis zu 10 Mio. Euro oder 2 % Umsatz nach NIS-2; bis zu 20 Mio. Euro oder 4 % Umsatz nach DSGVO
- **Aufsichtsmaßnahmen:** Prüfungen, Audits oder im Extremfall Betriebseinschränkungen durch Behörden
- **Reputationsrisiken:** Öffentlich gewordene Verstöße führen zu Vertrauensverlust und Kaufpreisabschlägen
- **Zivilrechtliche Folgen:** Schadenersatzforderungen von Kunden, Partnern oder Gesellschaftern
- **Persönliche Haftungsfolgen:** Geschäftsführung, Aufsichtsgremien und Beiräte haften persönlich, wenn sie ihrer Pflicht zur Umsetzung von Cyber-Sicherheitsmaßnahmen nicht nachkommen.

Für Industrie und Fertigung bedeutet diese neue Regulatorik: Cybersecurity ist nicht mehr nur IT-Thema, sondern zentraler Wert- und Risikofaktor. Wer die Anforderungen von NIS-2, DSGVO und dem IT-Sicherheitsgesetz ignoriert, riskiert nicht nur hohe Bußgelder und persönliche Haftung, sondern auch Unterbrechungen der Lieferkette, Produktionsausfälle und Reputationsschäden. Frühzeitige Compliance sichert nicht nur vor Sanktionen ab, sondern schafft Vertrauen bei Käufern, Geschäftspartnern und Investoren.

Ampel-Check für Unternehmenssicherheit

Die Cybersicherheitsampel ist ein kompaktes Bewertungsinstrument, um den Sicherheitsstatus von Portfoliounternehmen schnell und vergleichbar zu erfassen.
Sie basiert auf 10 Kernfragen zu entscheidenden Schutzmaßnahmen.
Wichtig: Kein „✓" ohne Nachweis akzeptieren! Nur belegte Antworten (z. B. Berichte, Policies, Screenshots) zählen in die Bewertung ein.

10-Fragen-Ampel-Check

1. Ist ein 24/7 Security Operations Center (SOC) oder Managed Detection & Response (MDR) aktiv? ☐

Nachweis: Vertrag, SLA-Berichte

2. Gibt es einen Incident-Response-Plan, der getestet wurde? ☐

Nachweis: IR-Plan, Protokoll der letzten Übung

3. Wurde in den letzten 12 Monaten ein Penetrationstest durchgeführt? ☐

Nachweis: vollständiger Report inkl. Findings

4. Liegt eine dokumentierte IT-/OT-Risikobewertung vor? ☐

Nachweis: Board-Abnahme, Gap-Analyse

5. Werden regelmäßig Awareness-Trainings für Mitarbeitende durchgeführt? ☐

Nachweis: Teilnehmerlisten, Schulungskonzepte

6. Ist Multifaktor-Authentifizierung (MFA) für kritische Systeme implementiert? ☐

Nachweis: Screenshots, Audit-Bericht

7. Ist eine Netzwerksegmentierung umgesetzt, um kritische Systeme zu isolieren? ☐

Nachweis: Architekturdiagramm

8. Existiert ein dokumentiertes Schwachstellen-Management? ☐

Nachweis: Compliance-Reports

9. Wurden Backup- und Recovery-Tests innerhalb der letzten 12 Monate durchgeführt? ☐

Nachweis: Testprotokoll, RTO/RPO

10. Besteht eine aktive und geprüfte Cyberversicherung inklusive Sublimits? ☐

Nachweis: Versicherungspolice

Bewertungssystem:

- Rot (<6 ✓): Kritisch – hohe Risiken, sofortige Maßnahmen erforderlich
- Gelb (6–8 ✓): Mittel – moderate Risiken, Handlungsbedarf, mittelfristig optimierbar
- Grün (9–10 ✓): Sehr gut – geringe Risiken, hohe Resilienz

Roadmap to Security

Die Roadmap to Security bietet Unternehmen aus Industrie und Fertigung einen klaren Fahrplan, um Cyber-Risiken zu erkennen, regulatorische Anforderungen umzusetzen und Wettbewerbsvorteile zu nutzen. Sie kombiniert vollständige Analysen mit konkreten Handlungsschritten und macht Cybersecurity zu einem steuerbaren Teil der Unternehmensstrategie und Katalysator der Wettbewerbsfähigkeit.

Die Roadmap umfasst:

Sicherheitsbewertung:
Umfassende Prüfung des aktuellen Cybersicherheits-Reifegrads des Unternehmens

Investitionsplanung:
5-Jahres-Plan für Cybersecurity-Maßnahmen mit CapEx/OpEx-Transparenz

Regulatorik-Check:
Identifikation relevanter Anforderungen aus NIS-2-Richtlinie

Ampelbericht & Maßnahmenplan:
Standardisierte Reifegradbewertung und priorisierte Handlungsschritte

Workshop mit dem Entscheider-Team:
Gemeinsame Abstimmung der Maßnahmen und Verantwortlichkeiten

Integration von IT- und OT-Sicherheit:
Berücksichtigung von Produktions- und IoT-Umgebungen

Nutzen für Entscheidungsträger

- Cyber-Resilienz ist keine IT-Initiative mehr, sondern sorgt für eine klare Faktenbasis für die Unternehmensstrategie und Investitionsentscheidungen
- Kostentransparenz und Planbarkeit durch 5-Jahres-Investitionsplanung
- Standardisierte Sicherheitsarchitektur mit messbaren KPIs auch für OT-/IoT-Koordination (z. B. Vorfallreaktionszeit, potenzielle Schadenshöhe, Compliance)
- Sorgt für Vertrauen bei Kunden und Investoren durch nachweisbare Cyber-Compliance

Ihr Partner für Cyber-Resilienz

Die **indevis GmbH** vereint technische Stärke, operative Verlässlichkeit und rechtliche Expertise, um Unternehmen und öffentliche Einrichtungen in einer zunehmend vernetzten Welt ganzheitlich zu schützen.

Unser Leistungsversprechen:

- Ein 24/7 Security Operations Center (SOC) mit Standort in Deutschland
- ISO-27001-zertifizierte Prozesse für höchste Sicherheits- und Compliance-Standards
- Incident Response & Digitale Forensik – schnelle Reaktion und Analyse im Ernstfall
- Regulatorik-Expertise: NIS-2 und DSGVO im Blick für Unternehmens-Compliance

SOS

Notfallkontakt (24/7): +49 (0) 89 45 24 24-112

Mehr erfahren – tiefer einsteigen:

Für weitere Informationen besuchen Sie uns auf unserer Website - einfach den QR-Code scannen oder über:

www.indevis.de/roadmap-to-security

SCAN ME

Bereit, Ihr Unternehmen cyber-resilient zu machen?

Warten Sie nicht auf den nächsten Angriff – handeln Sie jetzt.
Ob Gap-Analyse, Ampel-Check oder Roadmap-Entwicklung – wir zeigen Ihnen, wo Ihr Unternehmen heute steht und wie Sie Cybersecurity gezielt als Wettbewerbsvorteil einsetzen können.

sales@indevis.de

+49 (0) 89 45 24 24-100

indevis

Quellen

1. IBM (2025). Cost of a Data Breach Report 2025. https://www.ibm.com/de-de/reports/data-breach
2. Bitkom (2024). Studie Wirtschaftsschutz 2024. https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz
3. Dheeraj Rawal (2024): Cyber security 101 for the manufacturing Industry. How manufacturing companies can prepare against attacks with security and resilient Solutions. https://www.t06.de/in/en/insights/newsroom/expert-blogs/cyber-security-101-for-the-manufacturing-industry-1039292
4. Stern (2025). Erpresserbrief im Drucker: Hacker treiben Servietten-Fabrik in die Insolvenz, 16. Juni 2025. https://www.stern.de/wirtschaft/news/euskirchen--hacker-treiben-servietten-fabrik-fasana-in-die-insolvenz-35812104.html
5. Mirtsch, M., Koch, C., Dudek, G., & Blind, K. (2020). Die Nutzung und Wirkung der Norm ISO/IEC 27001 für Informationssicherheit in Unternehmen in Deutschland: Eine Studie im Rahmen der Initiative QI-FoKuS (Vol. 2). Bundesanstalt für Materialforschung und -prüfung (BAM). https://opus4.kobv.de/opus4-bam/frontdoor/index/index/docId/51792
6. Veeam Software (2024). Ransomware Trends Report 2024. https://go.veeam.com/ransomware-trends
7. Hiscox (2022): Cyber Readiness Report 2022. https://www.hiscox.com/documents/Hiscox-Cyber-Readiness-Report-2022.pdf
8. Plattner, Claudia (2024). Pressemitteilung: BSI will die „Cybernation Deutschland“ bauen. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2023/231010_it-sa_Cybernation.html