Deloitte.

Cyber Security als Aufgabe von Vorstand und Aufsichtsrat

April 2025

Einführung

Ihr Deloitte-Team für heute

Cornelia Tauber

Partner

Audit Industry

ctauber@deloitte.de

Ingo Dassow

Partner

Automotive Cybersecurity

idassow@deloitte.de

EILMELDUNG

"ZERO-DAY"-ANGRIFF AUF AMERIKA

BREAKING NEWS

"ZERO DAY" ATTACK ON AMERICA

USA GLOBAL

HD

Die Realität der heutigen Cyberlandschaft

Beispiel: Die Transformation der Automobilbauer zu Mobilitätsanbietern wird durch eine Vielzahl von Regeln der UNECE zur Produktsicherheit begleitet. Ohne Cyber keine Fahrzeugzulassung

Fahrzeug-Ecosystem

- Backend/App
- Supplier
- Factory
- Aftermarket Devices

Risk Input

Risk Treatment

Lifecycle Governance und Strategie

Verständnis von Bereitschaft und Reife in Cyber Security

Cyber Security Strategie

Cyber Security Governance
- Cyber-Sicherheitsorganisation (3 Verteidigungslinien)
- Rollen und Kompetenzen
- Richtlinien für die Cybersicherheit von Fahrzeugen
- Cybersicherheitskultur
- Bewertungen und Überwachung der Einhaltung von Cybersicherheitsvorschriften
- Cybersicherheitszertifizierung und -pflege – wo zutreffend
- Kontinuierliche Verbesserung

Fahrzeug Risk Management
- Identifizierung und Klassifizierung von Bedrohungsszenarien
- Analyse des Angriffswegs•
- Bewertung der Durchführbarkeit des Angriffs
- Risikobestimmung
- Bewertung, Entscheidung und Minderung von Risikobehandlungen
- Überwachung und Berichterstattung zur Risikoverfolgung

Erforderliche Kompetenzen für die Automobilindustrie

Secure Development Life Cycle
- Lebenszyklus der Entwicklung sicherer Fahrzeuge
- Bedrohungsanalyse
- Sichere Codierungstechniken
- Mehrschichtige Sicherheit
- Vulnerability Analyse

Vulnerability Management & Cyber Security Testing
- Testumfang & Vorgehensweise inkl. Supplier Beteiligung
- Organisatorische Rollen
- Teststrategien, Planung und Spezifikationen
- Testdokumentation
- Prozess zur Behebung von Mängeln
- Vulnerability Reporting & Tracking inkl. Supplier Vulnerabilities

Supplier Security Management
- Vendor Management
- Cyber Security Supplier Bewertungsprozess
- Cyber Security Verträge/ SLAs für Risikofaktoren
- Cyber Security Anforderungen an Komponenten, Logistik und Versand

Asset Management
- Asset Repository Pflege
- Vulnerability Database
- Lieferanteninformationen
- Kundeninformationen

Fahrzeug Security Monitoring
- Threat Intelligence
- Vulnerability Management
- Intrusion Detection
- Incident Analyse & Kategorisierung
- Log management for post-incident Analyse & Forensik
- Lessons Learned Prozesse

Fahrzeug - Incident Management
- Fahrzeug Incident Service
- Fahrzeug Incident Response Service Katalog
- Fahrzeug Incident Response Prozedur
- Fahrzeug Incident Monitoring & Reporting
- Fahrzeug Incident Forensics

Service input | **Service input** | **Service input**

Die Realität der heutigen Cyberlandschaft

Ausgeklügelte Bedrohungsakteure und die niedrige Eintrittsbarriere in die Cyberkriminalität haben die Bedrohungslandschaft erheblich vergrößert

#1 Risiko

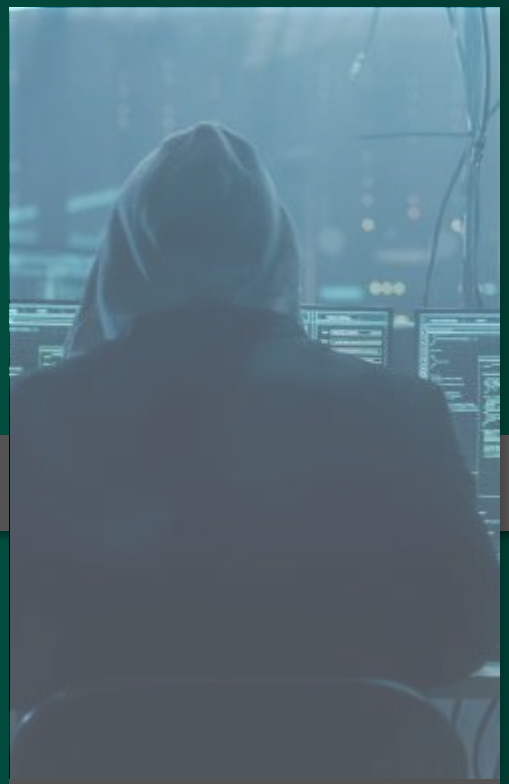
Cybervorfälle stehen weltweit an erster Stelle der Top-10-Geschäftsrisiken[1]

266 Mrd.€

geschätzter Schaden durch Cyberangriffe in Deutschland[2]

OT & PS

Betriebstechnologie (OT) und Produktsicherheit (PS) sind die Top-Domains mit Verbesserungsbedarf[3]



Ransomware

stellt die größte Bedrohung für deutsche Unternehmen dar[4]

[1]Source: Allianz, "*Allianz Risk Barometer: Cyber-Attacken als weltweites Top-Risiko 2024*", 2024.
[2]Source: Bitkom, "*Angriffe auf die deutsche Wirtschaft nehmen zu*", 2024.
[3]Source: Statista, "*Welche Tätigkeiten hat das Cybersicherheitsteam...*", 2024.
[4]Source: BSI, "*Ransomware -- Facts and defensive strategies*", 2024.

Regulatives Umfeld zur Begegnung der Bedrohungen

NIS2, DORA und CRA sind aktuelle Beispiele für Vorgaben zur Umsetzung in den Unternehmen unterschiedlicher Branchen

Die NIS-2-Richtlinie ist eine EU-Verordnung, die die Cyber- und Informationssicherheit von Unternehmen und Institutionen regelt.

Ziel der Richtlinie Verbesserung der Cybersicherheit in der EU, Schutz kritischer Infrastrukturen, Erhöhung der Resilienz und Reaktionsfähigkeit gegenüber Cyberangriffen.

DORA ist eine Verordnung der Europäischen Union, die die digitale Widerstandsfähigkeit von Finanzunternehmen stärken soll.

Sie bezieht sich auf EU-Finanzdienstleistungen und konzentriert sich auf die Aufrechterhaltung der Cybersicherheit.

Die Cyberresilienz-Verordnung (Cyber Resilience Act, CRA) ist eine EU-Verordnung, die die Cybersicherheit von vernetzten Produkten verbessern soll.

Sie gilt für alle Produkte mit digitalen Elementen, die in der EU erhältlich sind und hat als Ziel die Risiken für Verbraucher, Unternehmen und öffentliche Einrichtungen zu minimieren.

Der Einsatz künstlicher Intelligenz in der EU wird durch das KI-Gesetz, das weltweit erste umfassende KI-Gesetz, geregelt, um bessere Bedingungen für die Entwicklung und Nutzung dieser innovativen Technologie zu gewährleisten.

Er legt Regeln für die Entwicklung, Nutzung und den Betrieb von KI-Systemen fest.

Diskurs: Überblick zu NIS-2 Direktive

Die NIS-2-Direktive der EU erweitert den bestehenden Rechtsrahmen um spezifische Anforderungen an Organisationen und Unternehmen im Bereich der Cybersicherheit und -resilienz

Umsetzung der NIS-2-Direktive in Deutschland

EU-NIS-2-Direktive

Mit der NIS-2 wird ein EU-Rahmen für Mindeststandards im Bereich der Cybersicherheit geschaffen. Sie ersetzt die NIS-Direktive aus dem Jahr 2016 und hat einen größeren Anwendungsbereich und mehr Verpflichtungen.

NIS-2-Umsetzungsgesetz (NIS-2UmsuCG)

Das NIS-2UmsuCG liegt derzeit als 7th Gesetzesentwurf in der neuesten Fassung vom 07/2024 (Kabinettsentwurf) vor. Größere Änderungen sind derzeit nicht zu erwarten.

Inkrafttreten am 16. Januar 2023

Nationale Umsetzung bis zum März 2025

2023 2024 2025

Überblick über die NIS-2-Anforderungen für betroffene Unternehmen

Die NIS-2-Direktive schafft klare Verpflichtungen für die betroffenen Unternehmen und verpflichtet die Unternehmensleitung, die Umsetzung der erforderlichen Maßnahmen zu genehmigen und zu überwachen:

- Art. 21 Maßnahmen: Geeignete und verhältnismäßige technische, betriebliche und organisatorische Maßnahmen*
- Art. 23 Meldung: Meldung von Sicherheitsvorfällen mit erheblichen Auswirkungen an die zuständigen Behörden und CSIRTs
- Art. 27 Anmeldung: Anmeldung bei den zuständigen Behörden bis zum 17. Januar 2025

Sanktionen und Haftung: bis zu 7 Mio. (10 Mio.) EUR oder 1,4 (1,7) % des Umsatzes. Darüber hinaus interne Haftung der Unternehmensleitung im Falle eines Verstoßes gegen die Genehmigungs- und Überwachungspflicht **

Diskurs: Die wichtigsten regulatorischen Themen und ihre Auswirkungen auf das Management

Die Geschäftsleitung muss ein umfassendes Verständnis der rechtlichen Anforderungen und der Anforderungen an die Cybersicherheit entwickeln und sicherstellen, dass die Organisation diese einhält

	Risikobesitz	Vollstreckung	Sicherheitsanforderungen	Sicherheit der Lieferkette	Berichterstattung über Vorfälle
Verantwortlichkeit des Geschäftsführers	**Die Leitungsorgane** werden für die Behandlung von Cybersicherheitsfragen und die Förderung einer Cybersicherheitskultur **verantwortlich** gemacht. Die Leitungsorgane haften persönlich (§38 Kabinettsentwurf NIS-2). Die Leitungsorgane sollten **ihr Engagement zeigen.** **Die Leitungsorgane** müssen regelmäßig an **Schulungen** teilnehmen**, um** ausreichende **Kenntnisse** und Fähigkeiten **im Bereich der Informationssicherheit zu erwerben.**	Die Behörden können gegen **Wesentliche Unternehmen** Geldbußen in Höhe von bis zu **10 Mio. EUR oder 2 %** des gesamten weltweiten Jahresumsatzes des Unternehmens verhängen. **Die aktive Zusammenarbeit** mit den nationalen Behörden ist von entscheidender Bedeutung.	Die Unternehmensleitung ist an **der Ausarbeitung von Sicherheitsmaßnahmen zu beteiligen** und **muss die** angenommenen **Strategien** und **Maßnahmen für das Risikomanagement** der Informationssicherheit **genehmigen.** Es sollten Verfahren zur **Bewertung der Wirksamkeit von Sicherheitsmaßnahmen** sichergestellt werden. Die Leitungsorgane sind verpflichtet, **Sicherheitsschulungen für ihre Mitarbeiter zu fördern und anzubieten.**	Verwaltungsorgane sollten **die Sicherheit der Lieferkette genehmigen.** **Strategie definieren und die Schnittstellen** zwischen Beschaffung, Lieferkette und Informationssicherheit sicherstellen. Die Unternehmen sollten **ihre Lieferkette mit der gebotenen Sorgfalt prüfen** und die Qualität der Informationssicherheits-praktiken ihrer Lieferanten persönlich bewerten.	Verwaltungsorgane haben **Berichtspflichten.** Die Unternehmen sollten den zuständigen Behörden bereits **innerhalb von 24 Stunden** nach dem Auftreten erheblicher Zwischenfälle eine erste Meldung übermitteln. **BCM sollte gewährleistet sein.** Es sollte ein Plan für das Management des Geschäftsbetriebs während und nach einem Sicherheitsvorfall vorhanden sein.

Diskurs: Die wichtigsten regulatorischen Themen und ihre Auswirkungen für den Aufsichtsrat

Die neue Regulatorik bringt eine bedeutende Neuerung, indem sie die Verantwortung für Cybersicherheit direkt auf die Geschäftsführung und den Aufsichtsrat von Unternehmen überträgt

	Risikobesitz	Schulungen und Sensibilisierung	Berichterstattung über Vorfälle	Zusammenarbeit mit der Geschäftsführung	Generell
Verantwortlichkeit des Aufsichtsrats	**Strategische Überwachung:** • Sicherstellen, dass eine robuste Cybersicherheitsstrategie im Unternehmen implementiert ist und regelmäßig überprüft wird. • Kontrolle der Ressourcenzuweisung für Cybersicherheit, z. B. Personal, Technologien und Budgets. **Überprüfung der Compliance:** • Nachweis der Einhaltung: Sicherstellen, dass das Unternehmen alle NIS-2 Vorgaben einhält. • Einforderung von regelmäßigen Berichten zur Cybersicherheit von der Geschäftsführung. **Risikomanagement:** • Kontrolle, ob die Geschäftsführung ein angemessenes Risikomanagementsystem etabliert hat, das Cyberrisiken identifiziert, bewertet und adressiert.	**Verpflichtung zur Teilnahme an Schulungen** zu Cybersicherheit und NIS-2, um die eigene Kompetenz und die des Vorstands in diesem Bereich sicherzustellen.	**Vor einem Vorfall:** Sicherstellen, dass ein effektiver Notfallplan für Sicherheitsvorfälle existiert und regelmäßig getestet wird. **Nach einem Vorfall:** Überprüfung, ob die Reaktion gemäß den gesetzlichen Anforderungen durchgeführt wurde (z. B. Meldung an Behörden innerhalb von 24 Stunden).	**Aufsichtsräte müssen mit der Geschäftsführung eng zusammenarbeiten**, um sicherzustellen, dass: • eine Kultur der Cybersicherheit im Unternehmen etabliert wird. • regelmäßige Audits und Tests zur Einhaltung der NIS-2 durchgeführt werden • der Austausch mit relevanten Behörden und Partnern im Rahmen der Direktive erfolgt.	**Die NIS-2 Direktive verlangt von Aufsichtsräten,** dass sie aktiv die Verantwortung für Cybersicherheit und Compliance übernehmen. Sie sollten strategisch und operativ sicherstellen, dass: • das Unternehmen die Vorgaben der Direktive einhält • Cyberrisiken effektiv gemanagt werden • eine angemessene Reaktion auf Vorfälle gewährleistet ist.

Ganzheitliche Betrachtung der Cybersicherheit: Strategischer Wert

Unternehmen müssen den strategischen Wert von Cyber zur Sicherung ihrer Operationen kontinuierlich bewerten

Von der **Cyber(sicherheit)** als **Back-Office-Kostenstelle** mit Schwerpunkt auf **Bedrohungen** und **Unsicherheit**

Cyber als **Werttreiber** durch **Differenzierung, Einnahmensicherung** und **Kostenvermeidung**

Strategischer Wert von Cyber

Aufrechterhaltung der Geschäftsfunktionalität

Cyber ist erforderlich, um **"die Lichter am Leuchten zu halten"**, indem **betriebliche** und **unterstützende Prozesse** (z. B. Produktionslinie und MES[1]) vor Unterbrechungen **geschützt werden.**

Widerstandsfähige kritische Operationen

Cyber ist erforderlich, um **sicherzustellen, dass kritische Vorgänge** gegen Cyber-Bedrohungen **resistent sind** (z. B. Kundendienst: Durchführung von Wartungsarbeiten).

Verbesserung der Differenzierungsmöglichkeiten

Cyber **schützt differenzierende Fähigkeiten**, die **der Schlüssel zum Erfolg auf dem Markt** sind (z. B. robuste Produktion und Lieferung, Zertifizierungen).

Einzigartiges Nutzenversprechen

Cyber ist ein **Unterscheidungsmerkmal** für Kunden, das einen **nachhaltigen Wettbewerbsvorteil** schafft (z. B. die sichersten Produkte).

[1] MES – Manufacturing Execution System

Wie Unternehmen sich vor Cyberkriminalität schützen können

Unternehmen sollten einen strategischen Ansatz zur Cybersicherheit ihres Unternehmens verfolgen

Rollen und Verantwortlichkeiten in der Organisation definieren

Z. B. CISO, OT-Sicherheitsbeauftragter, Produktsicherheits-beauftragter, lokale Rollen

Bewertung des aktuellen Stands der Cybersicherheit in IT, OT und Produkten

Die tatsächlichen Risiken für Ihr Unternehmen kennen und Ihre Maßnahmen entsprechend ausrichten, mit implementierten Maßnahmen und Sicherheitskontrollen und lokaler Sicherheitsreife

Definition des Soll-Zustand auf der Grundlage der Geschäftsanforderungen

Cybersicherheit als wichtiges Unterscheidungsmerkmal von Produkten, wobei auch die gesetzlichen Anforderungen bekannt sind und eingehalten werden, um die Verpflichtungen zu verstehen und zu erfüllen

Implementierung von Cybersecurity Maßnahmen

Z. B. Architektur, Netzwerksegmentierung, Sicherheitskontrollzentrum, sichere Softwareentwicklung, Produktüberwachung

Der Aufsichtsrat benötigt ein Verständnis für die Herausforderungen der Informationssicherheit

Im Folgenden werden zehn Fragen aufgeführt, die ein Aufsichtsrat oder Prüfungsausschuss stellen kann, um sich ein umfassendes Bild der Cybersicherheitssituation zu machen

01 Welche spezifischen Cyber-Risiken hat das Unternehmen identifiziert, und wie wurden diese priorisiert?

02 Wie sieht die Strategie des Unternehmens zur Minderung von Cyberrisiken aus, und wie wird deren Effektivität regelmäßig überprüft und bewertet?

03 Welche Prozesse verwendet das Management, um die wertvollsten Vermögenswerte (auch "Kronjuwelen" genannt) zu identifizieren, die durch einen Angriff gefährdet werden könnten?

04 Wann wurde die letzte umfassende Cyber-Risikobewertung durchgeführt, und welche wesentlichen Änderungen und Verbesserungen wurden seitdem implementiert?

05 Inwieweit umfasst die Risikobewertung auch Risiken im Zusammenhang mit der Betriebstechnologie (OT), und wie werden diese Risiken gemanagt?

Der Aufsichtsrat benötigt ein Verständnis für die Herausforderungen der Informationssicherheit

Im Folgenden werden zehn Fragen aufgeführt, die ein Aufsichtsrat oder Prüfungsausschuss stellen kann, um sich ein umfassendes Bild der Cybersicherheitssituation zu machen

06 Welche Verfahren und Kontrollen hat das Unternehmen implementiert, um Cyber-Risiken im Zusammenhang mit Drittanbietern, Dienstleistern und Partnern zu minimieren?

07 Was ist der detaillierte Ansatz des Unternehmens für die Reaktion auf einen Ransomware-Angriff, und welche spezifischen Schritte sind im Incident-Response-Plan enthalten?

08 Wie lang ist die geplante Wiederherstellungszeit für die wichtigsten Geschäftsabläufe im Falle eines Cyber-Angriffs, und welche Maßnahmen sind implementiert, um diese Zeit zu minimieren?

09 Wie oft wird der Cyber-Risiko-Reaktionsplan in der gesamten Organisation bis hin zur Vorstandsebene geübt und getestet, und welche spezifischen Szenarien werden dabei abgedeckt?

10 Wie werden Sicherheitsaspekte in die Entwicklung neuer Verfahren und Systeme integriert, insb. in die Anwendungsentwicklung, und welche Sicherheitsstandards sind Teil des Entwicklungsprozesses?

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/de/UeberUns to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Legal advisory services in Germany are provided by Deloitte Legal. Our people deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte’s approximately 457,000 people worldwide make an impact that matters at www.deloitte.com/de.

This communication contains general information only, and none of Deloitte GmbH Wirtschaftsprüfungsgesellschaft or Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.