Gesetze und Zuständigkeiten in der IT-Sicherheit

IT-Sicherheit

ITT-Net-IS

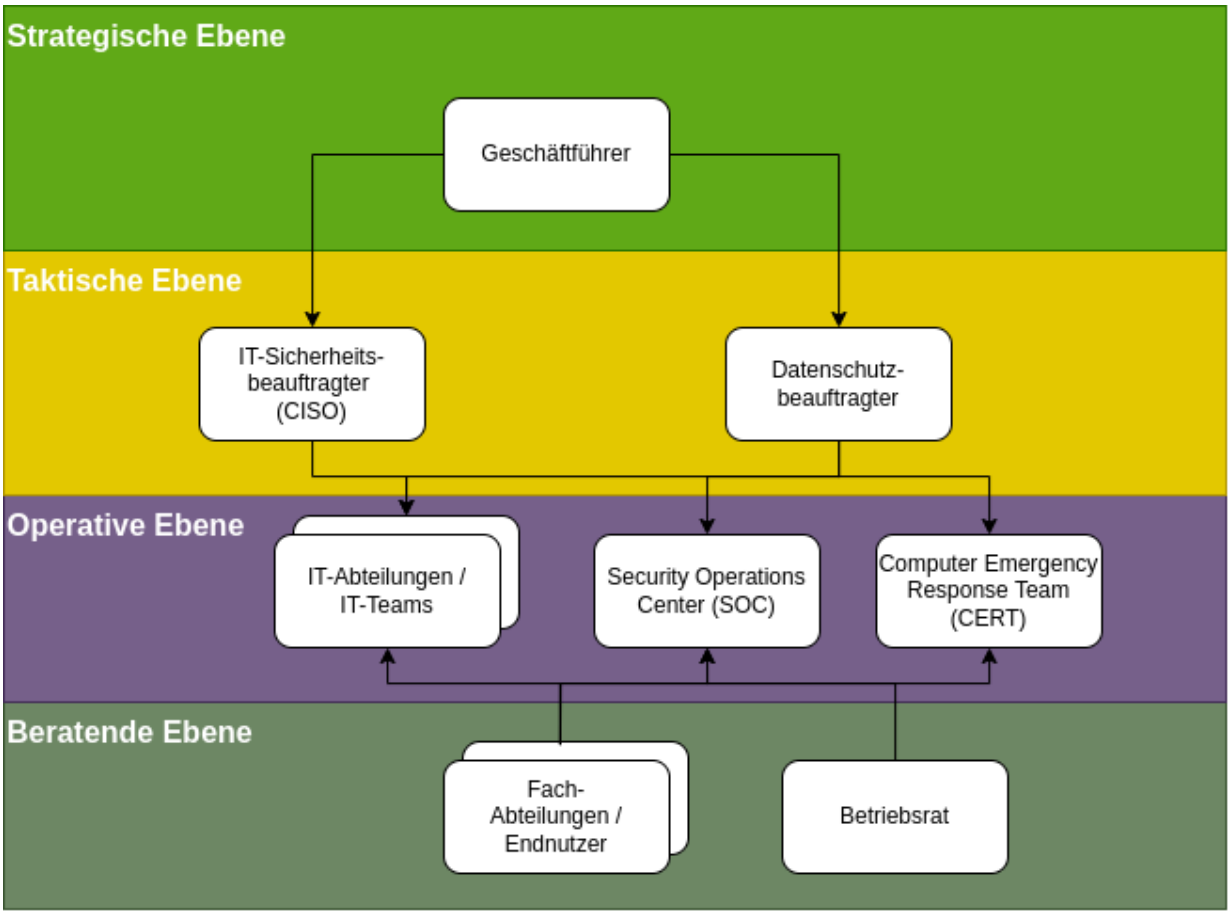
15. März 2025

1 Überblick

Dieses Modul behandelt die gesetzlichen Rahmenbedingungen und Zuständigkeiten im Bereich der IT-Sicherheit. Es werden relevante Gesetze, Standards und organisatorische Strukturen vorgestellt, die für die Implementierung und Aufrechterhaltung einer angemessenen qIT-Sicherheit in Unternehmen und Organisationen notwendig sind.

2 Verantwortliche Stellen und Zuständigkeiten

In einem gut strukturierten Sicherheitsmanagement sind verschiedene Rollen und Verantwortlichkeiten klar definiert:



2.1 Geschäftsführung

- Trägt die Gesamtverantwortung für die IT-Sicherheit
- Stellt notwendige Ressourcen bereit
- Verabschiedet die IT-Sicherheitsleitlinie
- Haftet persönlich für Verstöße gegen gesetzliche Vorschriften

2.2 IT-Sicherheitsbeauftragter (CISO - Chief Information Security Officer)

- Entwickelt und koordiniert das Sicherheitskonzept
- Berichtet direkt an die Geschäftsführung
- Überwacht die Umsetzung von Sicherheitsmaßnahmen
- Berät in Sicherheitsfragen
- Führt Risikoanalysen durch
- Erarbeitet Notfallpläne

2.3 Datenschutzbeauftragter

- Überwacht die Einhaltung des Datenschutzrechts
- Berät bei datenschutzrechtlichen Fragen
- Prüft Verfahren zur Verarbeitung personenbezogener Daten
- Ist weisungsfrei und berichtet direkt an die Geschäftsleitung

2.4 IT-Abteilung

- Setzt technische Sicherheitsmaßnahmen um
- Betreibt die Systeme nach Sicherheitsvorgaben
- Reagiert auf Sicherheitsvorfälle
- Führt regelmäßige Updates und Backups durch

2.5 Fachabteilungen/Benutzer

- Melden Sicherheitsvorfälle
- Halten sich an Sicherheitsrichtlinien
- Tragen durch ihr Verhalten wesentlich zur Gesamtsicherheit bei

2.6 Betriebsrat

- Vertritt die Interessen der Mitarbeiter bei Sicherheitsrichtlinien
- Muss bei überwachungsrelevanten Maßnahmen einbezogen werden

2.7 Security Operations Center (SOC)

Ein SOC ist eine zentrale Einheit, die für die kontinuierliche Überwachung und Verbesserung der IT-Sicherheitslage zuständig ist:

- 24/7-Überwachung der Systeme
- Erkennung von Sicherheitsvorfällen
- Analyse und Reaktion auf Vorfälle
- Forensische Untersuchungen
- Regelmäßige Sicherheitstests

Notes

- **24/7-Überwachung:** Permanente Kontrolle von IT-Systemen, um Bedrohungen frühzeitig zu erkennen.
- **Forensische Untersuchungen:** Analyse von Sicherheitsvorfällen zur Identifikation von Ursachen und Tätern.
- **Sicherheitstests:** Regelmäßige Tests zur Identifikation und Behebung von Sicherheitslücken.

2.8 Computer Emergency Response Team (CERT)

Ein CERT oder CSIRT (Computer Security Incident Response Team) ist darauf spezialisiert, auf IT-Sicherheitsvorfälle zu reagieren:

- Sofortmaßnahmen bei Sicherheitsvorfällen
- Unterstützung bei der Wiederherstellung von Systemen
- Analyse von Angriffsvektoren
- Informationsaustausch mit anderen CERTs

Notes

- **Angriffsvektoren:** Wege und Methoden, über die ein Angriff auf ein IT-System erfolgen kann.
- **Informationsaustausch mit anderen CERTs:** Zusammenarbeit mit anderen Sicherheitsorganisationen zur schnelleren Bedrohungserkennung.

3 Gesetze und Standards zur Informationssicherheit

In der digitalen Welt gewinnen Gesetze und Standards zur IT-Sicherheit an Bedeutung. Angesichts wachsender Cyberbedrohungen sind die rechtlichen Anforderungen verschärft worden, da IT-Sicherheit nicht nur eine technische, sondern auch eine unternehmerische und gesellschaftliche Verantwortung ist.

Notes

Unternehmen müssen nationale und internationale Vorschriften einhalten, die oft nur Mindeststandards definieren. Verstöße können hohe Strafen, Haftung für Führungskräfte und Reputationsverluste nach sich ziehen. Neben gesetzlichen Vorgaben spielen internationale Standards eine wichtige Rolle, da sie strukturierte Ansätze zur Informationssicherheit bieten und Vertrauen schaffen. Im Folgenden werden zentrale gesetzliche Regelungen und Standards vorgestellt.

3.0.1 Datenschutz-Grundverordnung (DSGVO)

- Europäische Verordnung zum Schutz personenbezogener Daten
- Verpflichtet zur Implementierung technischer und organisatorischer Maßnahmen
- Meldepflicht bei Datenschutzverletzungen (72 Stunden)
- Hohe Bußgelder bei Verstößen (bis zu 4% des weltweiten Jahresumsatzes)

3.0.2 NIS2-Richtlinie (Netzwerk- und Informationssicherheit)

- Nachfolger der ersten NIS-Richtlinie aus 2016
- In Kraft seit Januar 2023 mit Umsetzungsfrist bis Oktober 2024
- Erweitert den Anwendungsbereich auf weitere Sektoren (Energieversorgung, Verkehr, Finanzdienstleistungen, Gesundheitswesen, öffentliche Verwaltung, Raumfahrt, IKT-Dienstleistungen, u.v.m.)
- Unterscheidet zwischen ”wesentlichen” und ”wichtigen” Einrichtungen mit unterschiedlichen Anforderungen
- Stärkere Harmonisierung des Sicherheitsniveaus in der EU
- Umfassende Meldepflichten für Cybersicherheitsvorfälle
- Verpflichtung zur Einrichtung von Risikomanagementmaßnahmen
- Deutlich höhere Bußgelder als bei NIS1 (bis zu 10 Millionen Euro oder 2% des weltweiten Jahresumsatzes)
- Stärkere Management-Verantwortung: Die Leitungsorgane müssen Cybersicherheitsschulungen absolvieren und haften persönlich für Verstöße

3.0.3 IT-Sicherheitsgesetz (IT-SiG 2.0)

- Regelt insbesondere den Schutz kritischer Infrastrukturen
- Meldepflicht für Sicherheitsvorfälle
- Verpflichtung zur Implementierung angemessener Sicherheitsmaßnahmen
- Erweiterte Befugnisse für das BSI (Bundesamt für Sicherheit in der Informationstechnik)
- Wird durch die nationale Umsetzung der NIS2-Richtlinie weiterentwickelt

3.0.4 Branchenspezifische Regelungen

- Bankensektor: MaRisk (Mindestanforderungen an das Risikomanagement)
- Gesundheitswesen: Patientendatenschutzgesetz
- Telekommunikation: Telekommunikationsgesetz (TKG)
- Energiesektor: Energiewirtschaftsgesetz (EnWG)

3.1 Internationale Standards und Frameworks

Im Bereich der IT-Sicherheit haben sich verschiedene internationale Standards und Frameworks etabliert, die Organisationen bei der systematischen Umsetzung von Sicherheitsmaßnahmen unterstützen.

Notes

Diese Standards bieten bewährte Vorgehensweisen, Methoden und Kontrollmechanismen, die über gesetzliche Mindestanforderungen hinausgehen und auf internationalen Best Practices basieren.

Anders als Gesetze sind die meisten Standards **nicht verpflichtend**, werden aber oft von Kunden, Partnern oder Aufsichtsbehörden erwartet und können einen Wettbewerbsvorteil darstellen.

Notes

Eine Zertifizierung nach anerkannten Standards signalisiert nach außen, dass ein Unternehmen Informationssicherheit ernst nimmt und systematisch angeht.

3.1.1 ISO/IEC 27001

- Internationaler Standard für Informationssicherheits-Managementsysteme (ISMS)
- Systematischer Ansatz zur Verwaltung vertraulicher Informationen
- Basis für Zertifizierungen
- Umfasst Anforderungen an Planung, Umsetzung, Überwachung und Verbesserung

3.1.2 NIST Cybersecurity Framework

- Von der US-amerikanischen Behörde NIST entwickeltes Rahmenwerk
- Besteht aus den Kernelementen: Identifizieren, Schützen, Erkennen, Reagieren, Wiederherstellen
- Flexibel anpassbar an Unternehmensgrößen und -typen

3.1.3 ITIL (Information Technology Infrastructure Library)

- Framework für IT-Service-Management
- Enthält Best Practices für IT-Sicherheit im Kontext des Servicemanagements
- Umfasst Prozesse wie Incident Management und Problem Management

4 Weiterführende Ressourcen

- BSI für Bürger
- BSI-Grundschutz-Kompendium
- Allianz für Cybersicherheit
- DSGVO-Volltext
- NIS2-Richtlinie
- BSI zu NIS2