Informationssicherheit/Digitalisierung - Einführung eines Information Security Management Systems (ISMS)

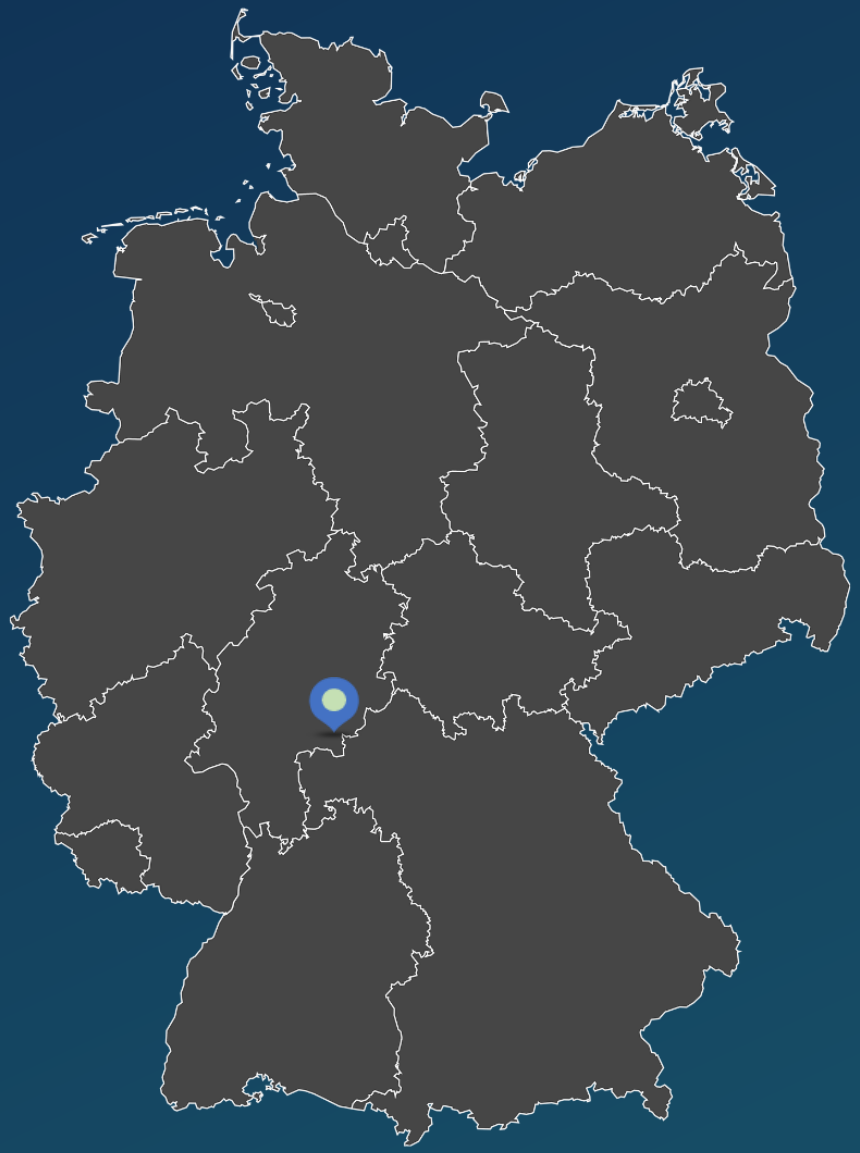
06.11.2024 (Kreissparkasse Schlüchtern)
Referent: Niklas Veith

Agenda


Lage der IT-Sicherheit
Informationssicherheit
Rolle des ISB
Informationssicherheit und Datenschutz
Zusammenfassung
Ende

Über uns – de-bit

- Mehr als 100 Spezialisten
- Seit 25 Jahren
- Standorte in Gelnhausen, Mannheim, Berlin
- Partnerschaft mit der Hochschule Fulda
- Informationssicherheit, Auditierung, Datenschutz, IT-Service, Schulungen



Über uns – de-bit

Sicherheitskonzepte für Kommunikations- und Datenaustauschnetze für Landes- und Bundesbehörden

Sicherheitskonzepte für Spionage- und Drohnenabwehr und Geheimschutzbetreuung

Drei zertifizierte BSI-Auditteamleiter auf der Basis von IT-Grundschutz

Freigegebene Prüfstelle für kritische Infrastrukturen vom BSI

Lage der IT-Sicherheit

>2000
Schwachstellen in Softwareprodukten / Monat
15% davon kritisch

21.000
Infizierte Systeme wurden vom BSI an deutsche Provider gemeldet

250.000
Neue Schadprogrammvarianten / Tag

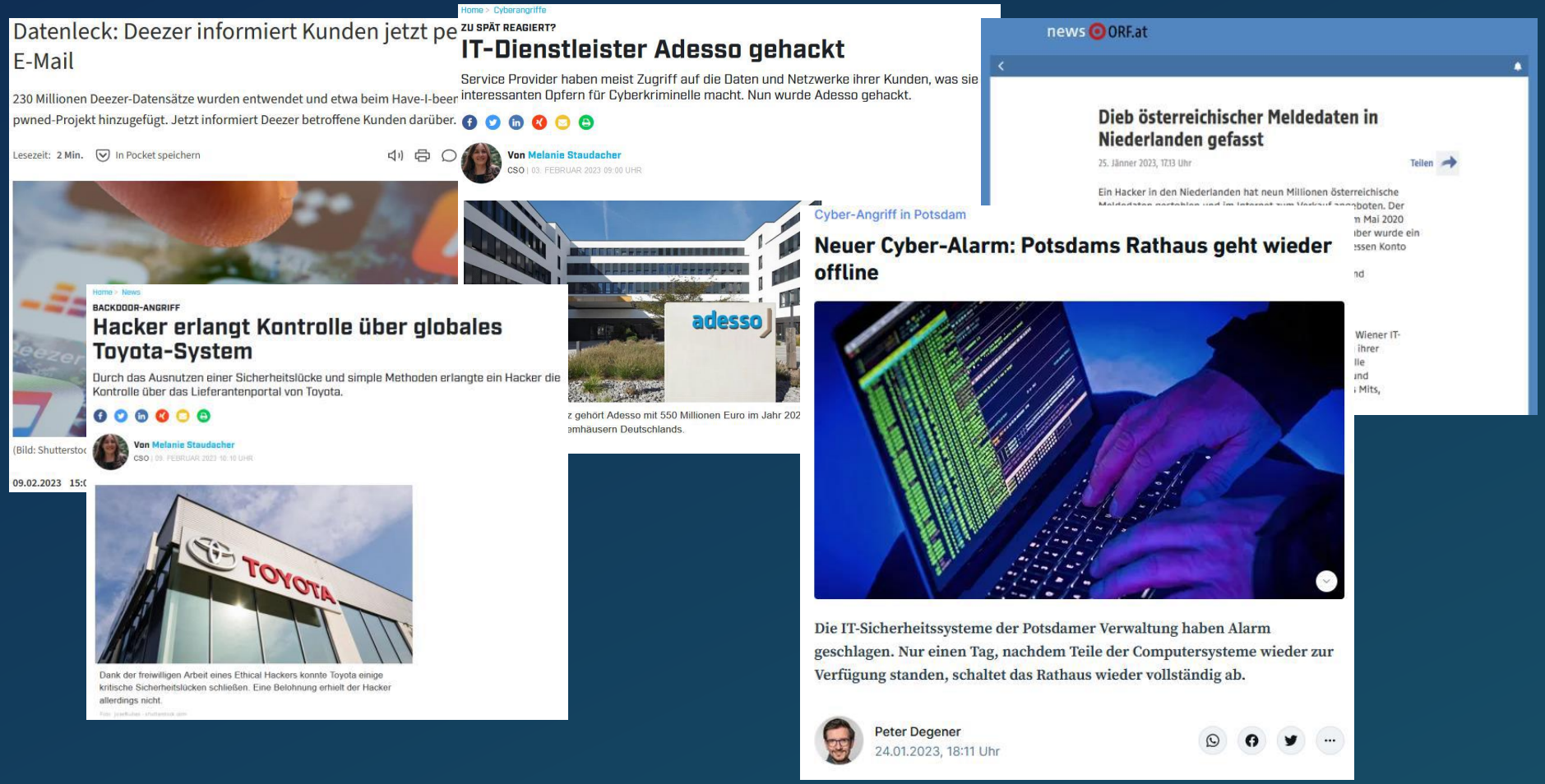
775
E-Mails mit Schadprogrammen wurden pro Tag abgefangen

66%
Aller Emails waren Cyberangriffe
(34% Erpressung, 32% Betrug)

370
Webseiten wurden wegen Schadprogrammen pro Tag gesperrt

Quelle: BSI - Die Lage der IT-Sicherheit in Deutschland, 2023

Informationssicherheitsvorfälle - News



Schäden für die Wirtschaft

Am Beispiel von Crowdstrike

Reaktion vom Gesetzgeber

Erkennung der Relevanz:

Informationssicherheit ist entscheidend für den Schutz von Daten und Infrastruktur

Gesetzliche Grundlagen:

Einführung von Verpflichtungen (z. B. DSGVO, IT-Sicherheitsgesetz)

Schutz kritischer Infrastrukturen:

Erhöhte Anforderungen an Sektoren, die für die öffentliche Versorgung wichtig sind (z. B. Energie, Gesundheit, Telekommunikation).

Kontrollen und Sanktionen:

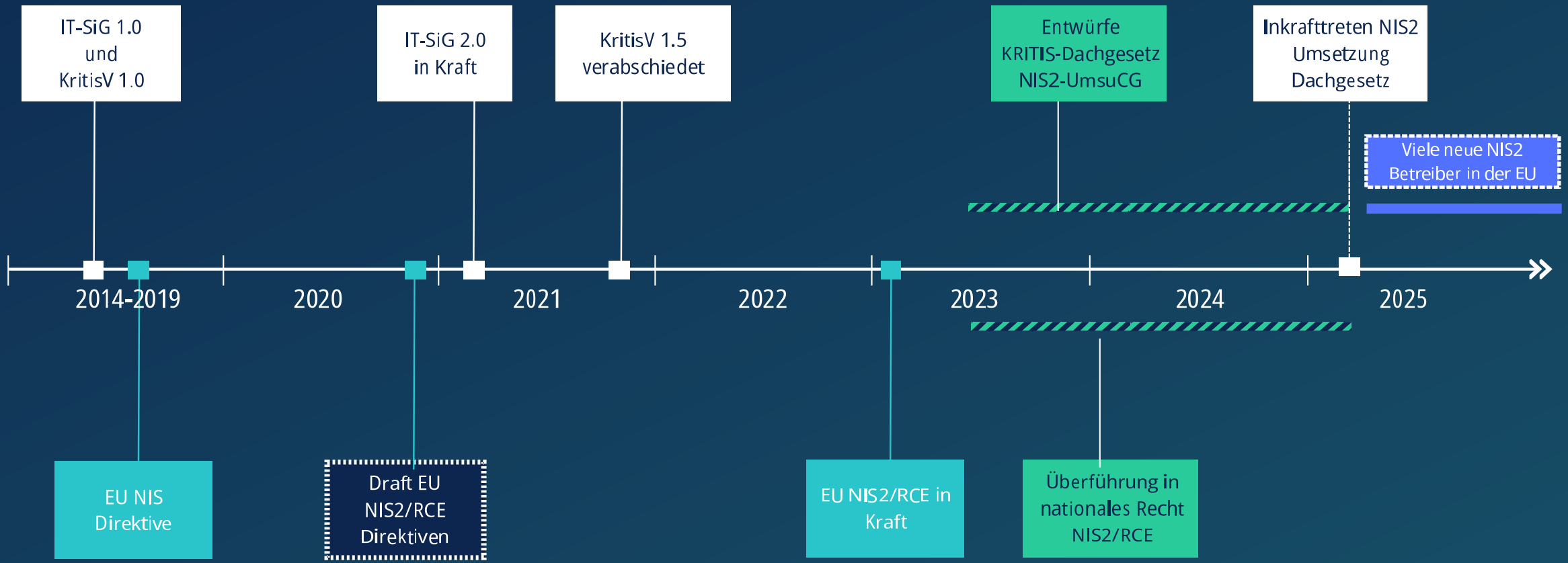
Regelmäßige Überprüfungen und Sanktionen bei Nichteinhaltung, um die Umsetzung sicherzustellen.

EU-Richtlinie 2022/2555 (NIS-2-Richtlinie)

Einführung und Inkrafttreten

- Network and Information Security (NIS2) seit Anfang 2023 in Kraft auf EU-Ebene
- Mindestharmonisierende Richtlinie für Cybersicherheit auf EU-Ebene
- Staaten müssen NIS-2 durch nationale Gesetze verbindlich machen

Reaktion vom Gesetzgeber



Übersicht: Pflichten für Betreiber

- Voraussichtliche Pflichten für Betreiber

Pflicht	Betreiber kritischer Anlagen (BSI-KritisV)	Besonders wichtige Einrichtung	Wichtige Einrichtung
Geltungsbereich	Anlage(n)	Unternehmen?	Unternehmen?
Maßnahmen Risikomanagement §30	✓	✓	✓
Höhere Maßstäbe für KRITIS §31	✓		
Besondere Maßnahmen SzA §31	✓		
Registierung §33 §34	✓	✓	✓
Meldepflichten §32	✓	✓	✓
Nachweise §39	✓		
Informationsaustausch §6	✓	✓	✓
Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitung §38	✓	✓	✓

Risikomanagement-maßnahmen §30

Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitung §38

Anforderungen an „Geschäftsleiter“:

- Geschäftsleiter **müssen** die TOMs nach §30 umsetzen und dessen Umsetzung überwachen
- Die Geschäftsleiter **müssen** regelmäßig an Schulungen teilnehmen
  - Der Umfang und die Dauer der Schulungen ist noch nicht bekannt
- Die Teilnahme an Schulungen muss durch den Geschäftsführer persönlich erfolgen

Geschäftsleitung: Haftung

- Haftung der Geschäftsführer:
  - Geschäftsführer haften dem Unternehmen gegenüber
  - Das Unternehmen darf bei Verschulden der Geschäftsführung nicht auf Ersatzansprüche verzichten
  - Das Unternehmen muss den Anspruch geltend machen solange der Geschäftsführer nicht zahlungsunfähig ist
  - Eine persönliche Haftung kommt in Betracht, wenn das Gesellschaftsrecht keine Haftung vorsieht.

Informations sicherheit

Allgemeine Informationen

Informationssicherheit
Allgemeines

Schutz vor:
Verlust, Missbrauch, Unberechtigtem Zugriff

Informationen:
Daten, die einen Wert für eine Organisation haben
Unternehmensdaten, Technische Informationen, Wissen

Maßnahmen zur Sicherheit

Technisch

- Firewalls
- Verschlüsselung
- Zugangskontrollen

Organisatorisch

- Schulungen
- Sicherheitsrichtlinien
- Notfallpläne

Informationssicherheit
Schutzziele

- Sicherstellung der Schutzziele: **CIA Triad**
  - Vertraulichkeit *(Confidentiality)*
    - Nur berechtigte Personen haben Zugriff
  - Integrität *(Integrity)*
    - Daten sind korrekt und unverändert
  - Verfügbarkeit *(Availability)*
    - Daten sind jederzeit verfügbar und zugänglich

Informationssicherheit
PDCA-Zyklus

- IT-Sicherheit ist ein hochindividueller, durch den Plan-Do-Check-Act-(PDCA)-Kreislauf dynamisierter Prozess des betrieblichen Risikomanagements
- Kontinuierlicher Verbesserungsprozess (KVP)

Warum Informationssicherheit?

Schutz vor Cyberangriffen:

Hacking und Datendiebstahl nehmen exponentiell zu

Schutz der Privatsphäre:

Persönliche und vertrauliche Daten sicher halten

Einhaltung gesetzlicher Vorschriften:

Compliance-Anforderungen

Vertrauen aufbauen:

Geschäftspartner erwarten sicheren Umgang mit Informationen

Gefahren bei mangelnder Informationssicherheit

Informationssicherheits-managementsystem (ISMS)

Allgemeine Informationen

Definition ISMS

„Ein Informationssicherheitsmanagementsystem (ISMS) ist ein strukturiertes System von Richtlinien und Maßnahmen, das den Schutz und die Kontrolle sensibler Informationen sicherstellt, indem es deren Vertraulichkeit, Integrität und Verfügbarkeit gewährleistet.“

Aufbau ISMS

- Grundlage für den Schutz sensibler Informationen
- Systematische Vorgehensweise zur:
  - Erkennung, Bewertung und Behandlung von Risiken
- Klare Rollen und Verantwortlichkeiten
- Richtlinien und Prozesse
  - Festlegung und Etablierung von Betriebsabläufen
- Vorfallmanagement
  - Meldung und Bewältigung von Sicherheitsvorfällen
- Überwachung und Bewertung
  - Kontinuierlicher Verbesserungsprozess

Inhalte ISMS

Sicherheitsmaßnahmen für IT-Systeme

- Technische und organisatorische Risikomanagementmaßnahmen

Lieferkettensicherheit

- Sicherheitsanforderungen an Lieferanten und Dienstleister

Mitarbeiter und Schulungen

- Förderung von Sicherheitsbewusstsein

Notfallplanung und Krisenmanagement

- Konzepte zur Aufrechterhaltung von kritischen Geschäftsprozessen

ISO/IEC 27001 Einführung

Einführung in ein Information Security Management System (ISMS)

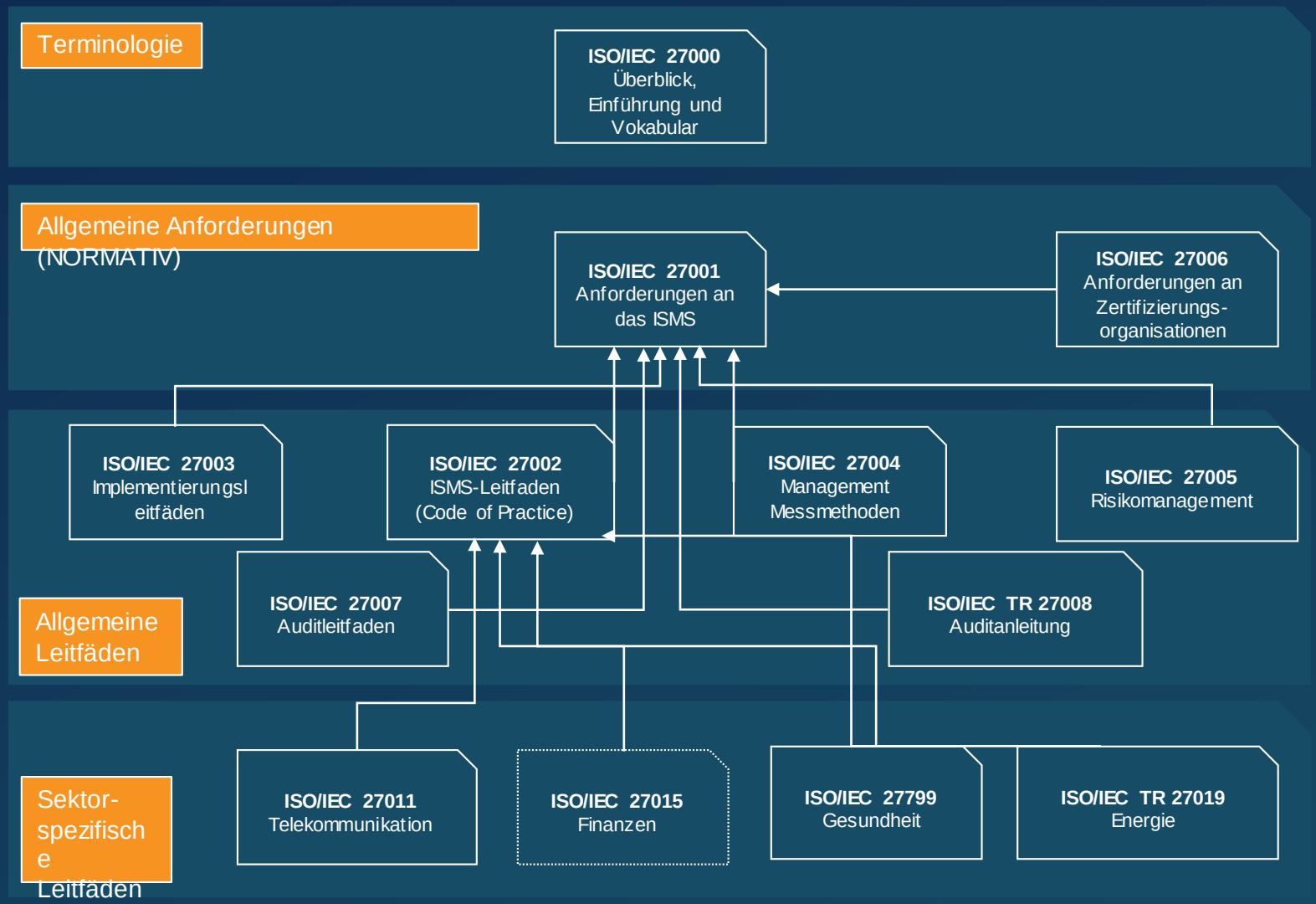
Einführung ISO/IEC 27001

- Internationaler Standard für Informationssicherheits-Managementsysteme (ISMS)
- Systematischer Ansatz für ISMS
  - Ziel: Risikomanagement
- Anwendbar für alle Arten von Organisationen unabhängig von Größe und Branche
- Gliederung analog zu anderen ISO-Normen für Managementsysteme (z.B. ISO 9001)

Einführung ISO/IEC 27001

- Kapitel 4-10
  - Definiert Anforderungen an ein ISMS
- Annex A
  - Risikomanagementmaßnahmen mit Maßnahmenzielen
    - Normativ, einzelne Maßnahmen können ausgeschlossen werden
      - „Statement of Applicability“
- ISO 27002 (Leitfaden ca. 100 Seiten) Umsetzungshinweise

Normenreihe ISO 27000 – Überblick



Unterstützende Standards

- **ISO/IEC 27010** Intersector Communication
- **ISO/IEC 27013** Integrated implementation of 27001 and 20000-1
- **ISO/IEC 27014** Governance Framework
- **ISO/IEC 27031** Business Continuity
- **ISO/IEC 27032** Cyber Security
- **ISO/IEC 27033** Network Security
- **ISO/IEC 27034** Application Security
- **ISO/IEC 27035** Security Incident Management
- **ISO/IEC 27036** Outsourcing
- **ISO/IEC 27037** Digital Evidence

ISO 27001 / 27002– Überblick

ISO/IEC 27001:2022(E) – 2024(DE)

Information security, cybersecurity and privacy protection
— Information security management systems
— Requirements

ISO/IEC 27002:2022(E) – 2024(DE)

Information security, cybersecurity and privacy protection
— Information security controls

IT-Grundschutz

Einführung in ein Information Security Management System (ISMS) nach IT-Grundschutz

Bundesamt
für Sicherheit in der
Informationstechnik

Überblick BSI Standards

BSI-Standard 200-1:	Managementsysteme für Informationssicherheit (ISMS)
BSI-Standard 200-2:	IT-Grundschutz-Methodik
BSI-Standard 200-3:	Risikomanagement
BSI-Standard 200-4:	Business Continuity Management

IT-Grundschutz
Allgemeine Informationen

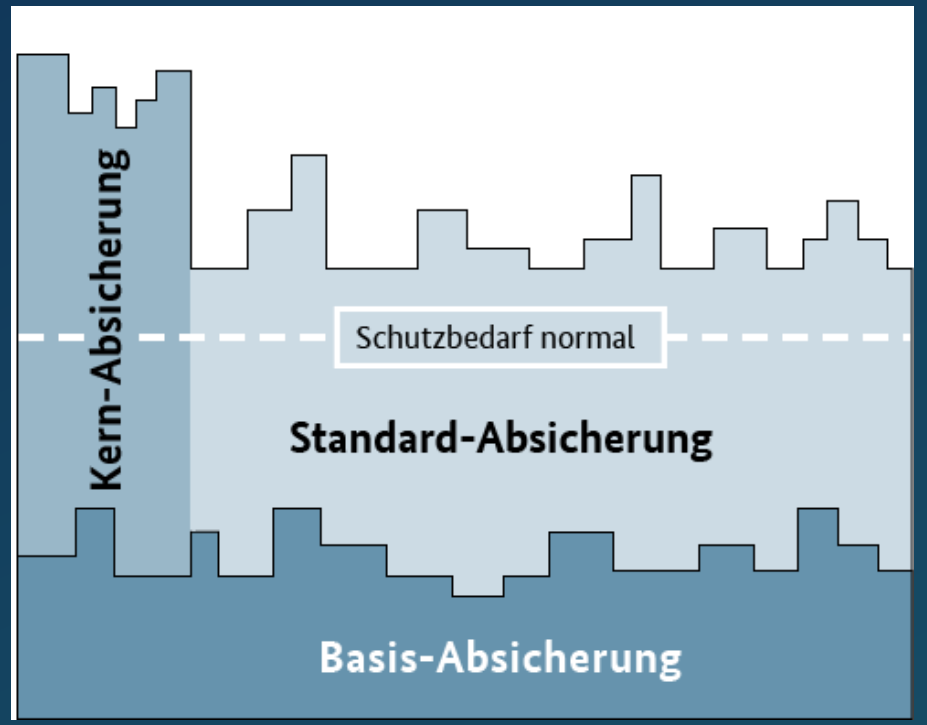
Bundesamt für Sicherheit in der Informationstechnik

- Nationaler Standard für Informationssicherheits-Managementsysteme (ISMS) vom Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Orientiert sich an der ISO/IEC 27001
- Modularer Aufbau durch IT-Grundschutz-Bausteine
  - Ziel: Risikomanagement durch klare Sicherheitsanforderungen

IT-Grundschutz
Wahl der Absicherung

Bundesamt für Sicherheit in der Informationstechnik

- Standardabsicherung
  - Umfassende und tiefgehende Absicherung
  - Alle Bereiche einer Institution sollen angemessen und umfassend geschützt werden
- Kernabsicherung
  - Absicherung der „Kronjuwelen“
  - Geltungsbereich eingeschränkt
- Basisabsicherung
  - Absicherung stellt das Minimum dar
  - Nichtanwendung von Basis-Anforderungen nicht möglich
  - Basis-Absicherung nicht zertifizierbar



IT-Grundschutz

Vorteile vom IT-Grundschutz im Vergleich zur ISO/IEC 27001 - nativ

Bundesamt für Sicherheit in der Informationstechnik

- Spezifischer als die ISO/IEC 27001
- Genauere Angaben zur Umsetzung einzelner Maßnahmen
- Hoher Sicherheitswert durch erweiterte Betrachtung des Unternehmens
- Hohe Anerkennung von IT-Grundschutz-Zertifikaten bei öffentlichen Auftraggebern
- Individuellere Bewertung der Risiken
- Laufende Aktualisierung des Standards der somit auf aktuelle Bedrohungen reagieren kann

IT-Grundschutz

Nachteile vom IT-Grundschutz im Vergleich zur ISO/IEC 27001 - nativ

- Aufwendigere Implementierung im Vergleich zur ISO/IEC 27001
  - Ca. Faktor 4
- Geringere Anerkennung bei internationalen Kunden
- Anforderungen aus dem Grundschutz Kompendium sind durch ihre Komplexität und Menge schwieriger umzusetzen
- Jährliche Überprüfung aller modellierten Bausteine des IT-Grundschutzes
  - Dadurch auch erhöhte Aufwände

ISO/IEC 27001

Vorteile

- Flexibler Ansatz bei der Umsetzung
- International anerkannte Norm
- Weniger Umsetzungsaufwand bei großen Unternehmen

Nachteile

- Weniger spezifisch als der IT-Grundschutz
- Bisher geleistet Arbeit zum IT-Grundschutz ist nicht in Gänze nutzbar für die ISO
- Der Auditaufwand der Erstzertifizierung und Aufrechterhaltung des Zertifikates ist deutlich höher

Unterschiede

ISO/IEC 27001	IT-Grundschutz
Allgemeiner Ansatz	Setzt sich tief mit technischen und organisatorischen Aspekten auseinander
ISO 27001 + 27002 ~ 230 Seiten	IT-Grundschutz Kompendium über 800 Seiten
Vollumfängliche Risikoanalyse	Risikoanalyse nur wenn erhöhter Schutzbedarf, nicht umgesetzte Anforderung oder selbsterstellter Baustein

Rolle des ISB

Rolle des Informationssicherheitsbeauftragten

Rolle des ISB

Risikomanagement

Behandlung aller Risiken im Unternehmen

Business Continuity Management

Alle Maßnahmen zur Geschäftsfortführung im Krisenfall

Informationssicherheit

Schutz sämtlicher Informationswerte (Daten, Ausdrucke, Mitarbeiter, Kunden, Know-How, Gebäude)

Informationssicherheitsbeauftragte ***ISB***

Künstliche Intelligenz

Sichere Einführung und Nutzung von KI in Unternehmen

KI -Beauftragte ***(KI-B)***

Unternehmenssicherheit

Arbeitsschutz, Personenschutz

IT-Security

Schutz der IT-Infrastruktur

Datenschutz

Schutz personenbezogener Daten

Datenschutzbeauftragte ***(DSB)***

Datenschutzkoordinator ***(DSK)***

Rolle des ISB

Steuert und unterstützt den Informationssicherheitsprozess

Unterstützt die Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit

Koordiniert Erstellung des Sicherheitskonzepts, Notfallvorsorgekonzepts, Teilkonzepte, System-Sicherheitsrichtlinien u. weitere Richtlinien und Regelungen

Initiiert und überprüft die Realisierung von Sicherheitsmaßnahmen

Überwacht die Dienstleistersteuerung

Unterschiede zwischen Datenschutz und Informationssicherheit

Aspekt	Datenschutz	Informationssicherheit
Zielsetzung	Schutz personenbezogener Daten vor unbefugtem Zugriff und Missbrauch.	Schutz aller Informationen (personenbezogen, geschäftlich, technisch) vor Verlust, Diebstahl und Beschädigung.
Regulatorische Rahmenbedingungen	Geprägt durch Gesetze wie die Datenschutz-Grundverordnung (DSGVO) und nationale Datenschutzgesetze.	Geprägt durch Standards wie ISO/IEC 27001 und IT-Grundschutz des BSI.
Fokus	Konzentration auf die Rechte von Individuen und die Verarbeitung personenbezogener Daten.	Konzentration auf die Vertraulichkeit, Integrität und Verfügbarkeit aller Informationen.

Informationssicherheit und Datenschutz

- Datenschutz
  - Fokus auf Schutz personenbezogener Daten und Einhaltung der Datenschutzgrundverordnung (DSGVO)
  - Grundsatz: „Protokolliere so viel wie nötig.“
- Informationssicherheit:
  - Fokus auf Erhaltung aller Schutzziele von Informationen
  - Grundsatz: „Protokolliere so viel wie möglich.“
- Synergie
  - Technische und organisatorische Risiken in der Informationssicherheit sind oftmals auch Datenschutzrelevant

Informationssicherheit und Datenschutz Synergien

Datenverschlüsselung	Verschlüsselung von personenbezogenen Daten schützt nicht nur die Vertraulichkeit, sondern erfüllt auch Datenschutzanforderungen.
Schulung und Sensibilisierung	Gemeinsame Schulungsprogramme für Mitarbeiter, die sowohl Sicherheits- als auch Datenschutzrichtlinien abdecken, fördern ein umfassendes Bewusstsein.
Risikomanagement	Bei der Durchführung von Risikoanalysen werden sowohl Sicherheitsrisiken als auch Datenschutzrisiken identifiziert und bewertet.
Vertragliche Regelungen mit Dritten	Verträge mit Dienstleistern sollten sowohl Sicherheitsanforderungen als auch Datenschutzbestimmungen enthalten, um die Datenintegrität zu gewährleisten.

Zusammenfassung

Durch ein ISMS:

- ✓ Gesetzeskonformität
- ✓ Erhöhung der Informationssicherheit
- ✓ Erhöhung des Datenschutzes
- ✓ Risikomanagement
- ✓ Sichere Zusammenarbeit mit Lieferanten
- ✓ Stärkung des Kunden- und Mitarbeitervertrauens
- ✓ Fortlaufende Verbesserung




Danke

Niklas Veith, www.de-bit.de

Niklas.Veith@de-bit.de

DEBIT