Grundlagen des Datenschutzes und der IT-Sicherheit (Teil 2a)

Vorlesung im Sommersemester 2025

an der Universität Ulm

von Bernhard C. Witt

2. Grundlagen der IT-Sicherheit

Grundlagen des Datenschutzes		Grundlagen der IT-Sicherheit	
✓	Geschichte des Datenschutzes	➔	Anforderungen zur IT-Sicherheit
✓	Datenschutzrechtliche Prinzipien		Mehrseitige IT-Sicherheit
✓	Technischer Datenschutz		Risiko-Management
✓	Schwerpunktthema: Aktuelles		Konzeption von IT-Sicherheit

Anforderungen zur IT-Sicherheit:

- Compliance
- Stand der Technik / internationale Standards
- Einflussfaktor Recht
- Einflussfaktor Technik
- Einflussfaktor Unternehmens-spezifika

Compliance (1)

Definition 8: Compliance

Übereinstimmung mit festgelegten Regeln

Zu den festgelegten Regeln zählen:

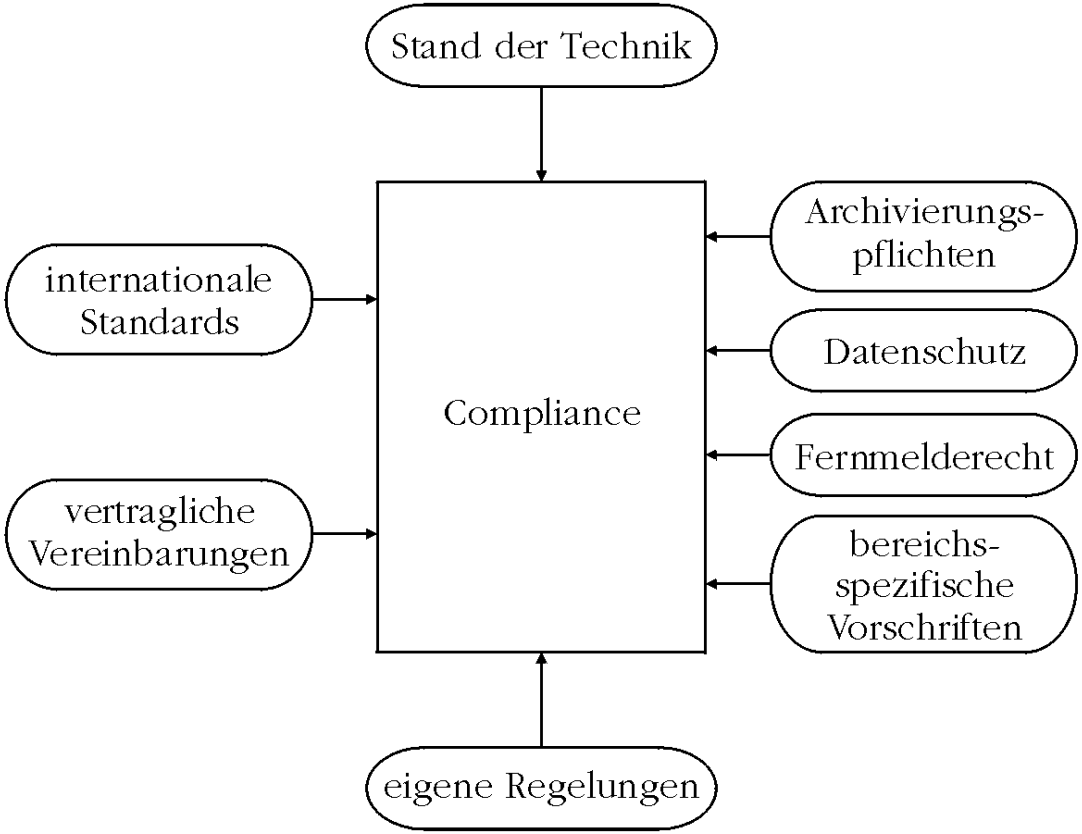
→ Rechtliche Regeln

→ Best practice Regeln (internationaler) Standards

→ Regeln aufgrund von Verträgen mit Kunden (insb. zu SLAs) oder Beschäftigten (Anstellungsverträge)

→ Interne Regeln (Richtlinien, Policies, Dienstanweisungen)

Compliance (2)



Stand der Technik

Definition 9: Stand der Technik

Entwicklungsstand technischer Systeme, der zur vorsorgenden Abwehr spezifischer Gefahren geeignet & der verantwortlichen Stelle zumutbar ist

→ Maßgeblich für Stand der Technik: Gefahrenprävention!
→ Maßnahmen zum Stand der Technik müssen aber zumutbar sein
→ Verhältnismäßigkeitsprüfung inhärent
→ Internationale Standards gute Referenz für Stand der Technik
→ Aber: Kein Automatismus für gerichtsfeste Compliance!
→ Best Practice Standards genießen jedoch einen höheren Schutz hinsichtlich nötiger Sorgfaltspflicht als andere Standards

Im Rahmen des **IT-Sicherheitsgesetzes** wird nach dessen Begründung unter „Stand der Technik“ verstanden der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt.

Compliance zu internationalen Standards

- **Umgang mit Informationen**
  → Informationssicherheitsmanagement (ISO/IEC 2700x)
  → Information Security Incident Management (ISO/IEC 27035-x)
  → IT Forensik (ISO/IEC 27037 & ISO/IEC 27041, 27042 & 27043)
- **Business Continuity Management**
  → Business Continuity Management (ISO 22301)
  → Business Continuity Management Guidance (ISO 22313)
  → Incident Preparedness & Operational Continuity (ISO/PAS 22399)
  → ICT Readiness for Business Continuity (ISO/IEC 27031)
- **Steuerung der IT**
  → Corporate Governance of IT (ISO/IEC 38500)
  → Governance of Information Security (ISO/IEC 27014)
- **Betrieb von IT-Services**
  → IT-Service-Management (ITIL bzw. ISO/IEC 20000-x)
  → Integriertes Management zu Informationssicherheit & IT-Services (ISO/IEC 27013)
  → Outsourcing finanzwirksamer IT-Services (ISA 402, ISAE 3402 & SSAE 16)
  → Information Security for Supplier Relationships (ISO/IEC 27036-x)
- **Betrieb von Netzwerken**
  → Netzwerksicherheit (ISO 7492-2, ISO/IEC 27033-x)
- **plus zahlreiche Standards zur Systemsicherheit**

Informationssicherheit

Definition 10: Informationssicherheit

Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Information (und ggf. weiterer Eigenschaften – nach ISO/IEC 27000)

→ Aufrechterhaltung von **Schutzzielen**

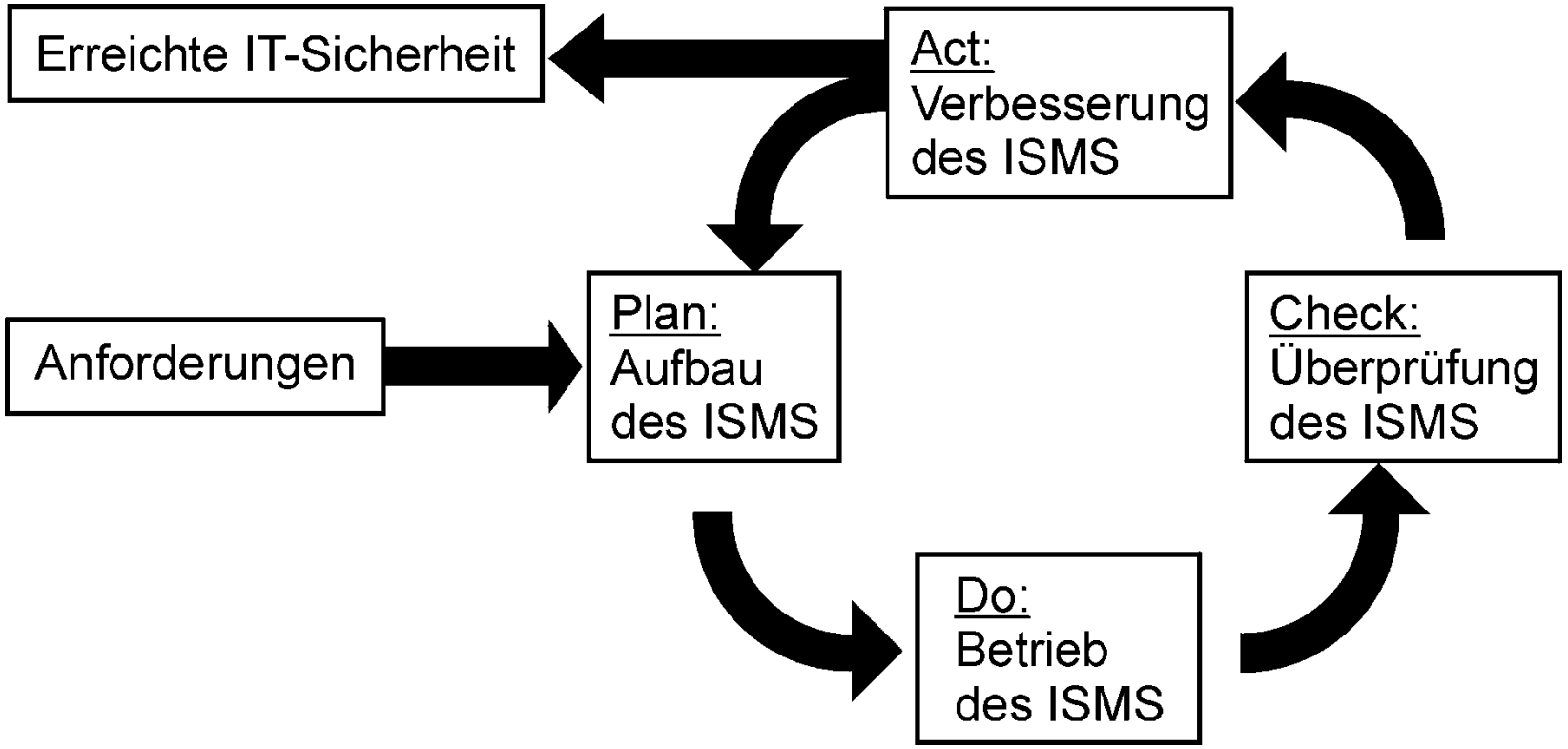
→ betrifft alle Informationen eines Unternehmens
Geschäftsgeheimnisse + Datengeheimnis

→ Information ist ein hoher Vermögenswert

→ Verknüpfung mit IT-Risiko-Management zwingend

→ Informationssicherheit ist Aufgabe des Managements

PDCA-Vorgehensmodell



ISMS = Informationssicherheitsmanagementsystem

Hinweise zum PDCA-Modell

- Basiert auf sog. **Deming Cycle** (Qualitätsverbesserungszyklus nach W. Edwards Deming)
- In der **PLAN**-Phase werden die Vorgaben und Anforderungen bestimmt (inkl. Zielsetzung!) und die Übereinstimmung der vorgefundenen Einstellungen hinsichtlich dieser Rahmen überprüft (1. Risk Assessment – zur Festlegung geplanter Maßnahmen)
- In der **DO**-Phase werden entsprechende technische und organisatorische Maßnahmen ergriffen, um die Vorgaben und Anforderungen zielgerichtet umzusetzen, und dabei insbesondere entsprechende Konfigurationen vorgenommen
- In der **CHECK**-Phase wird überprüft, inwiefern die getroffenen Maßnahmen dazu geeignet sind, die vorgegebenen Ziele zu erreichen (2. Risk Assessment – über Wirksamkeit der Controls)
- In der **ACT**-Phase werden im Sinne einer kontinuierlichen Verbesserung Konsequenzen aus der Überprüfung gezogen, der bestehende Status Quo neu bewertet und die Grundlage für den nächsten Durchlauf gelegt

Zum Managementsystem (1)

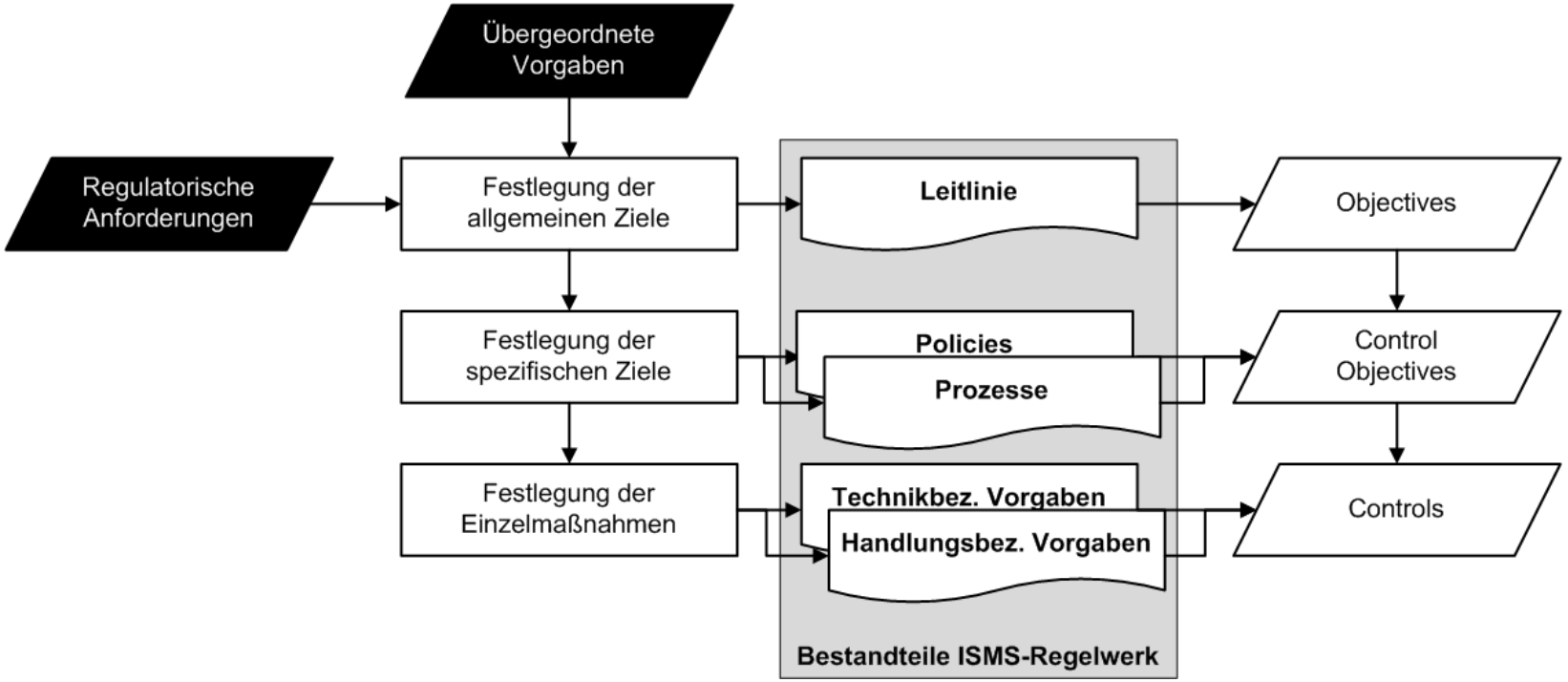
- **Managementsystem** = Satz zusammenhängender und sich gegenseitig beeinflussender Elemente einer Organisation, um Policies, Ziele (= zu erreichende Ergebnisse) und Prozesse zum Erreichen dieser Ziele festzulegen (nach ISO/IEC 27000) → mit Managementsystem wird Zielerreichung gesteuert
- Ziele und Umsetzungen können sich im Laufe der Zeit ändern
  → **Fortlaufende Verbesserung** nötig
- Ein **Informationssicherheitsmanagementsystem** (ISMS) umfasst:
  - Leitlinie zur Informationssicherheit (zur Festlegung übergeordneter Ziele des ISMS; von oberster Leitung formell ausgedrückt → „Politik“)
  - Verfahren (= Prozesse zur risikobasierten Steuerung und Aufrechterhaltung von Informationssicherheit; Prozess = Satz zusammenhängender und sich gegenseitig beeinflussender Tätigkeiten, der Eingaben in Ergebnisse umwandelt)
  - Richtlinien (= verbindliche Vorgaben zur Erreichung von Informationssicherheitszielen im Detail)
  - und damit verbundene Ressourcen und Tätigkeiten,
  - die jeweils von der Organisation gesteuert werden, um ihre Informationswerte (Primary Assets) zu schützen

Zum Managementsystem (2)

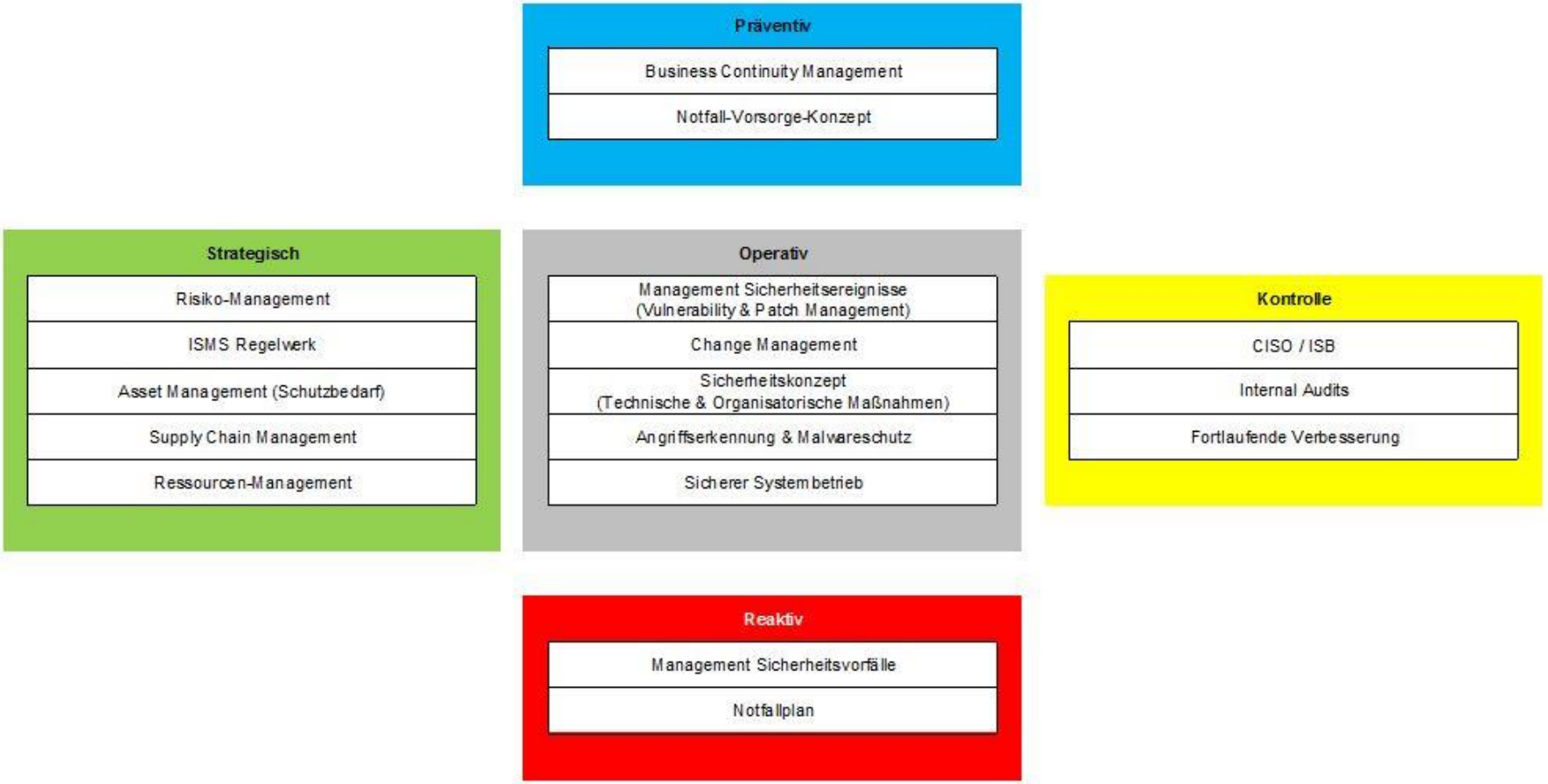
Wichtige Bestandteile eines Managementsystems:

- **Risikomanagementprozess**
  = systematische Anwendung von Managementrichtlinien, –verfahren und –praktiken auf die Tätigkeiten des Kommunizierens, Abstimmens und Festlegens des Kontextes sowie der Identifizierung, Analyse, Bewertung, Behandlung, Überwachung und Überprüfung von Risiken
- Ausreichende **Ressourcen und Kompetenzen**
- Ausreichendes **Bewusstsein**
- **Kommunikation** und Meldepflichten
- **Dokumentenlenkung** & Lenkung von Aufzeichnungen
- **Regelmäßige Bewertung** durch Kennzahlen über Sicherheitsleistung & Wirksamkeit des Managementsystems, Internes Audit über Konformität des Managementsystems (auf Basis eines Auditprogramms unter Auswahl eines stimmigen Stichprobenverfahrens) gegenüber relevanten Anforderungen und Managementbewertung
- Planung wirksamer Korrekturmaßnahmen unter Berücksichtigung von Ursachenanalysen & **Fortlaufende Verbesserung** des Managementsystems

Zusammenhang Ziele & deren Umsetzung im ISMS



Ebenen laufender Betrieb ISMS



Richtlinien nach ISO/IEC 27001

- Richtlinie für den zulässigen Gebrauch und einzuhaltende Verfahren für den **Umgang mit Information** und anderen damit verbundenen Werten
- Richtlinie zur **Kennzeichnung von Information**
- Richtlinie für die **Informationsübertragung**
- Richtlinie zur Kontrolle des physischen und logischen **Zugriffs auf Information** und damit verbundenen Werten
- Richtlinie zur **Handhabung von Informationssicherheitsvorfällen**
- Richtlinie für eine **aufgeräumte Arbeitsumgebung** hinsichtlich Unterlagen und Wechseldatenträgern sowie für Bildschirmsperren
- Richtlinie für **Datensicherungen** von Information, Software und Systemen; inkl. der Überprüfung von Datensicherungen
- Richtlinie zum **Einsatz von Kryptografie** und der Verwaltung kryptographischer Schlüssel
- Richtlinie für **sichere Entwicklung** von Software und Systemen
- Richtlinie zur **Netzwerksicherheit**

Verfahren nach ISO/IEC 27001 (1)

- Verfahren für den **Umgang mit Information** und damit verbundenen Werten, inkl. deren Rückgabe
- Verfahren zur **Kennzeichnung von Information** gemäß festgelegter Klassifizierung zur Vertraulichkeit, Integrität, Verfügbarkeit und relevanten Anforderungen interessierter Parteien
- Verfahren zur **Informationsübermittlung** für alle Arten von Übertragungseinrichtungen
- Verfahren zum **Management** des gesamten Lebenszyklus **von Identitäten**
- Verfahren zur Zuweisung und **Verwaltung von Authentifizierungsinformation**
- Verfahren zur **Informationssicherheit in Lieferantenbeziehungen**
- Verfahren zur Beherrschung der mit der **IKT-Produkt- und Dienstleistungslieferkette** verbundenen Informationssicherheitsrisiken
- Verfahren zur **regelmäßigen Überwachung**, Überprüfung und Bewertung der Informationssicherheitspraktiken der Lieferanten und der Erbringung von deren Dienstleistungen
- Verfahren für die **Nutzung von Cloud-Diensten**, inkl. Ausstieg
- Verfahren zur **Handhabung von Informationssicherheitsvorfällen**
- Verfahren für die **Reaktion auf Informationssicherheitsvorfälle**
- Verfahren zur Verstärkung und **Verbesserung der Informationssicherheitsmaßnahmen** durch Ableitung von Erkenntnissen aus Informationssicherheitsvorfällen
- Verfahren für das **Sammeln von Beweismaterial** im Zusammenhang mit Informationssicherheitsvorfällen

Verfahren nach ISO/IEC 27001 (2)

- Verfahren zur **Sicherstellung der IKT-Bereitschaft** auf der Grundlage von Business Continuity Zielen und IKT-Kontinuitätsanforderungen
- Verfahren zum **Schutz der Rechte an geistigem Eigentum**
- Verfahren zur **regelmäßigen Durchführung von unabhängigen Überprüfungen** der Vorgehensweisen für die Handhabung der Informationssicherheit
- Verfahren zur **regelmäßigen Überprüfung über die Einhaltung der Leitlinie zur Informationssicherheit und der themenspezifischen Richtlinien zur Informationssicherheit**
- Verfahren über **dokumentierte Bedienabläufe** an Informationsverarbeitungsanlagen
- Verfahren zur **Maßregelung bei Verstoß gegen die Leitlinie** zur Informationssicherheit
- Verfahren zum **Umgang mit Speichermedien**, inkl. Transport und Entsorgung
- Verfahren zur Einschränkung, Zuteilung, Gebrauch und **Verwaltung von privilegierten Zugangsrechten**
- Verfahren zur angemessenen **Verwaltung** des Lese- und Schreibzugriffs auf **Quellcode, Entwicklungswerkzeuge und Softwarebibliotheken**
- Verfahren zur **Handhabung technischer Schwachstellen** verwendeter Informationssysteme
- Verfahren zur Konfiguration, inkl. **Sicherheitskonfiguration**, von Hardware, Software, Diensten und Netzwerken
- Verfahren zur **Protokollierung** und Umgang mit Protokollinformation

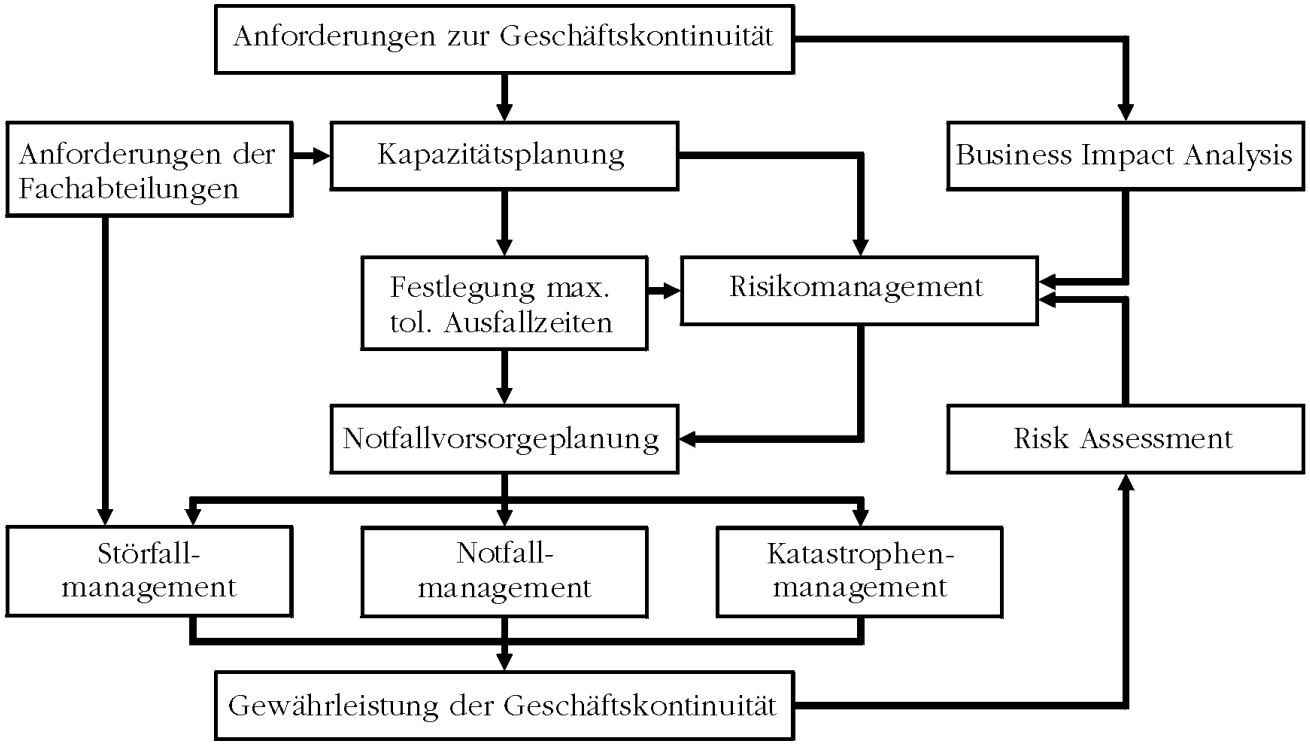
Verfahren nach ISO/IEC 27001 (3)

- Verfahren zur **Überwachung unüblichen Verhaltens** in Netzwerken, Systemen und Anwendungen unter Bewertung über potenzielle Informationssicherheitsvorfälle
- Verfahren zur **Überwachung des Gebrauchs von Hilfsprogrammen**, welche System- und Anwendungsschutzmaßnahmen umgehen können
- Verfahren zur **Installation von Software** auf Betriebssystemen
- Verfahren zum **Schutz von Information** in Systemen und Anwendungen, **die mit Netzwerken und Netzgeräten verbunden sind**
- Verfahren zur **Sicherheit von Netzwerkdiensten**
- Verfahren zur Verringerung der Gefährdung durch bösartige Inhalte über den **Zugang zu externen Websites**
- Verfahren zur Genehmigung einzuhaltender Anforderungen bei der **Entwicklung oder Beschaffung von Anwendungen**
- Verfahren zur Berücksichtigung festgelegter **Grundsätze für** die Analyse, Entwicklung und Pflege **sicherer Systeme**
- Verfahren zur **Sicherheitsprüfung im Entwicklungslebenszyklus**, inkl. Abnahme
- Verfahren zur Steuerung, Überwachung und Überprüfung von Aktivitäten im Zusammenhang mit **ausgegliederter Systementwicklung**
- Verfahren zum **Management von Änderungen** an Informationsverarbeitungseinrichtungen und Informationssystemen
- Verfahren zur Auswahl, Schutz und **Verwaltung von** Prüfinformation (**Testdaten**)

Business Continuity Management

- Grundlage: **ISO 22301** (Requirements) **& ISO 22313** (Guidance)
- **Gewährleistung der Geschäftskontinuität** mithilfe
  - **Business Impact Analysis** (BIA) → Identifikation kritischer und für den Fortbestand bedrohlicher Prozesse der gesamten Wertschöpfungskette (inkl. etwaiger Abhängigkeiten auch gegenüber Lieferanten) & Ermittlung der Folgen (Personenschaden, Complianceverstoß, Reputationsschaden, Finanzschaden, Qualitätseinbußen, Umweltschaden) → Priorisierung für Wiederanlauf
    Minimum Business Continuity Objective (MBCO) = Minimum funktionstüchtiger Ressourcen, um Geschäftsziele während einer Unterbrechung zu erfüllen
    Recovery Time Objective (RTO) = maximale Dauer bis zum Wiederanlauf
    Recovery Point Objective (RPO) = maximal akzeptabler Datenverlust
    (→ Backup-Zyklen & Redundanzen!)
  - **Business Continuity Plan** → Dokumentation der (strategischen, taktischen & operativen) Vorgehensweisen beim Eintreten eines Notfalls (= Notfallkonzept)
    Notfall *= außergewöhnliche Abweichung vom Normalbetrieb (→ unterscheidet sich von Störfällen, die im Rahmen des laufenden Betriebs beherrschbar sind, und von Katastrophen, die sich großflächig auswirken & i.d.R. staatlich reglementiert sind)*
  - Durchführung von **Notfallübungen** anhand stimmiger Szenarien

Absicherung der Geschäftskontinuität

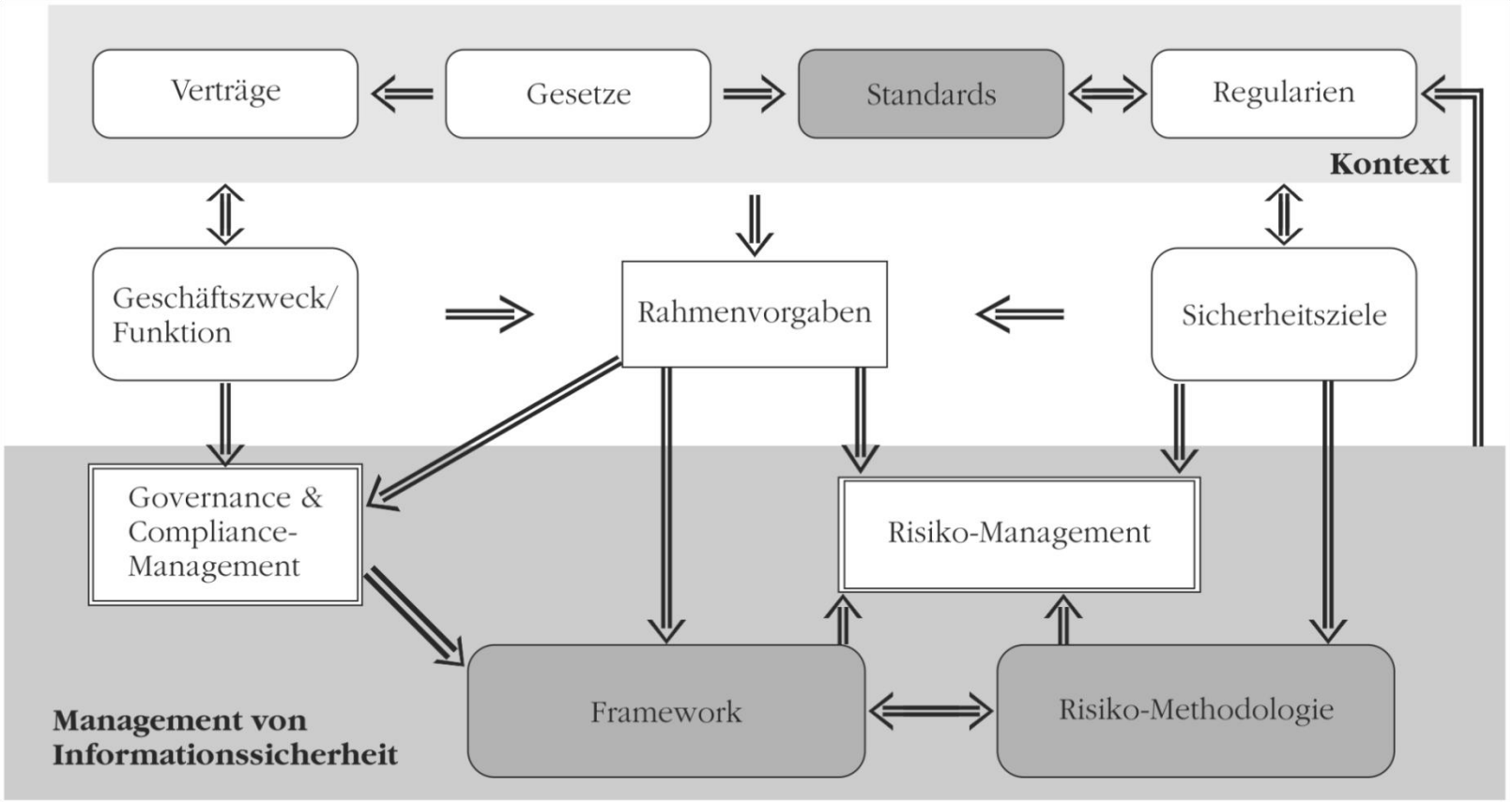


Datensicherung

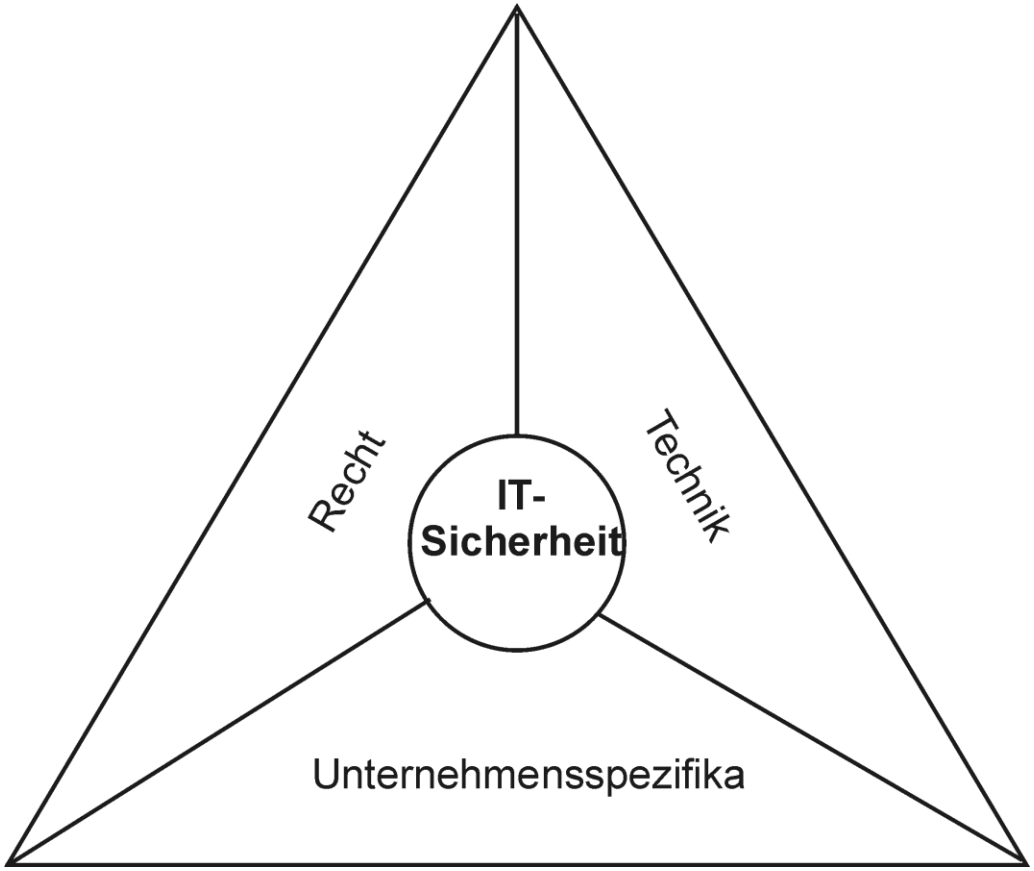
Im Rahmen der Rechtsprechung lassen sich folgende **Regelungen zur Datensicherung** ableiten:

- täglich hat wenigstens eine Differenzsicherung zu erfolgen und wöchentlich eine Vollsicherung (nach dem Urteil des OLG Hamm vom 01.12.2003; Az.: 13 U 133/03)
- der Erfolg einer Datensicherung ist zu überprüfen (nach dem Urteil des OLG Karlsruhe vom 07.11.1995; Az.: 3 U 15/95)
- bei einer Datensicherung muss die Wiederherstellbarkeit der gesicherten Daten auch bei einem Hardwaretausch überprüft werden (nach dem Urteil des LG Stuttgart vom 30.01.2002; Az.: 38 O 149/00 KfH)
- selbst bei manuellen Datensicherungen sind Vorkehrungen zur Vermeidung von Bedienfehlern zu treffen (nach dem Urteil des OLG Oldenburg vom 03.06.2003; Az.: 9 U 10/03)
- wurde für einen Nutzer dauerhaft für Nebenpflichten ein Mail-Account angelegt, müssen die auf diesem Account abgelegten Daten so lange vorgehalten werden, bis der Nutzer keine Verwendung für diese Daten mehr hat (nach dem Beschluss des OLG Dresden vom 05.09.2012; Az.: 4 W 961/12)

Zusammenhang für ISMS



Einflussfaktoren der IT-Sicherheit



Einflussfaktor Recht

Sorgfaltspflicht:

- KonTraG (§ 91 II AktG, § 43 I GmbHG)
  → Überwachungssystem zur Erkennung fortbestandsgefährdender Entwicklungen
- Haftungsrecht (§ 276 BGB, § 100 UrhG)
- Geschäftsgeheimnisse (GeschGehG)
  → setzt berechtigtes Interesse an Geheimhaltung voraus
- Buchführungspflichten (§§ 238 I & 257 HGB, §§ 145-147 AO, GoBD)
- Schutz vor Angriffen (§§ 202a, 202c, 268, 269, 303b & 305a StGB)

Datenschutz & Fernmeldegeheimnis: siehe Teil 1 der LV

Straftaten mit Computerbezug

§ 201 StGB: Verletzung der Vertraulichkeit des Wortes
§ 201a StGB: Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen
§ 202a StGB: Ausspähen von Daten
§ 202b StGB: Abfangen von Daten
§ 202c StGB: Vorbereiten des Ausspähens und Abfangens von Daten
§ 203 StGB: Verletzung von Privatgeheimnissen
§ 206 StGB: Verletzung des Post- oder Fernmeldegeheimnisses
§ 263a StGB: Computerbetrug
§ 268 StGB: Fälschung technischer Aufzeichnungen
§ 269 StGB: Fälschung beweiserheblicher Aufzeichnungen
§ 270 StGB: Täuschung im Rechtsverkehr bei Datenverarbeitung
§ 271 StGB: Mittelbare Falschbeurkundung
§ 274 StGB: Urkundenunterdrückung
§ 303a StGB: Datenveränderung
§ 303b StGB: Computersabotage
§ 305a StGB: Zerstörung wichtiger Arbeitsmittel
§ 317 StGB: Störung von Telekommunikationsanlagen

Umgang mit § 202c StGB

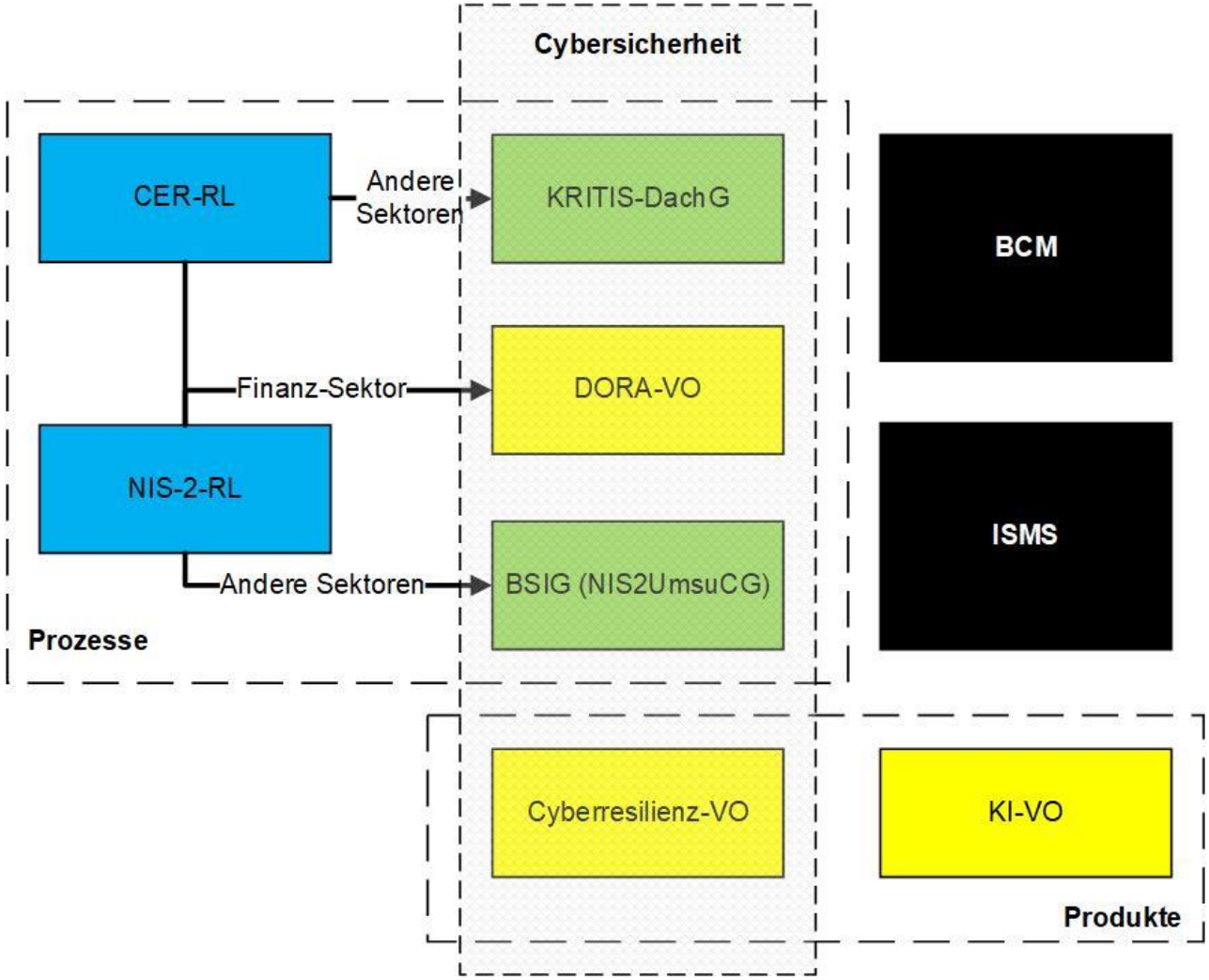
§ 202c StGB: Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Folgen für die Administration der IT-Sicherheit:

- Die Einstufung als Straftat setzt Vorsatz voraus. Insofern steht die Tätigkeit der IT-Administration mit dem Ziel der Gewährleistung der IT-Sicherheit keineswegs unter Strafe. Allerdings ist es hierzu zweckmäßig, die Methoden der Angreifer und damit insbesondere die Wirkungsweise der sog. „Hackertools“ zu kennen.
- Der IT-Administration kann daher angeraten werden, sich sowohl die „Beschaffung“ als auch den Einsatz von „Hackertools“ durch die Geschäftsleitung genehmigen zu lassen, so dass deren Einsatz nicht unbefugt erfolgt.
- Entsprechende „Hackertools“ sind gegen unbefugten Zugriff zu schützen.
- Über den durchgeführten Einsatz ist ein Protokoll zu erstellen, das ebenfalls gegen unbefugten Zugriff abzusichern ist.

Cybersicherheitsrecht



IT-Sicherheitsgesetz (1)

- Im Zuge des IT-Sicherheitsgesetzes (wirksam seit 2015) wurden besondere Vorschriften für **kritische Infrastrukturen** erlassen. Dazu zählen Einrichtungen, Anlagen oder Teile davon aus den Sektoren
  - Energie,
  - Informationstechnik und Telekommunikation,
  - Transport und Verkehr,
  - Gesundheit,
  - Wasser,
  - Ernährung sowie
  - Finanz- und Versicherungswesen,

  die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.
- *2021 erweitert um Siedlungsabfallentsorgung & „Unternehmen im besonderen öffentlichen Interesse “*

IT-Sicherheitsgesetz (2)

- Für diese Sektoren wurden im Rahmen der **BSI-KritisV** bestimmt, dass folgende Anlagen zur Erbringung einer kritischen Dienstleistung unter das IT-Sicherheitsgesetz fallen:
  → betriebsnotwendige Anlagen
  → für den Betrieb bedeutsame Nebeneinrichtungen
  [2021 um IT-Bezug erweitert]
- Für die einzelnen Sektoren wurden in der BSI-KritisV einerseits qualitative Kriterien (Auflistung kritischer Dienstleistungen) als auch branchenspezifische Schwellenwerte (quantitative Kriterien; Versorgung von 500.000 Personen) benannt
- Betreiber kritischer Infrastrukturen haben nach § 8a Abs. 1 BSIG angemessene organisatorische und technische Vorkehrungen **zur Vermeidung von Störungen** der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse unter Einhaltung des Stands der Technik zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind

IT-Sicherheitsgesetz (3)

- Organisatorische und technische Vorkehrungen gelten im Kontext von kritischen Infrastrukturen nur dann als angemessen, wenn der dafür **erforderliche Aufwand nicht außer Verhältnis zu den Folgen** eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Infrastruktur steht
  - → Begründungspflicht für das Nichtergreifen von Schutzvorkehrungen, die nach Stand der Technik üblich sind
  - → Folgen für Ausfall / Beeinträchtigung gesamtwirtschaftlich / gesellschaftlich
  - → Begründung i.d.R. nur über kompensatorische Maßnahmen möglich
- Betreiber kritischer Infrastrukturen haben mind. alle 2 Jahre die Erfüllung der Anforderungen aus § 8a Abs. 1 BSIG nachzuweisen (unter Benennung von aufgedeckten Sicherheitsmängeln!)
- Erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit, die zu einem Ausfall oder eine Beeinträchtigung der Funktionsfähigkeit betriebener kritischer Infrastrukturen führen können oder geführt haben, sind dem BSI unverzüglich zu melden

IT-Sicherheitsgesetz (4)

- Von den Betreibern einer kritischen Infrastruktur wird nach der Begründung des IT-Sicherheitsgesetzes insbesondere erwartet:
  - Betrieb eines Information Security Managements, welches u.a. die Sicherheitsorganisation festlegt und durch ein IT-Risikomanagement flankiert wird
  - Identifikation und Management kritischer Cyber-Assets
  - Betrieb von Maßnahmen zur Angriffsprävention und –erkennung
  - Implementierung eines Business Continuity Managements
  - Umsetzung branchenspezifischer Sicherheitsstandards
- Eine Störung liegt vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken
- Erheblich und damit meldepflichtig sind IT-Störungen, die nicht bereits automatisiert oder mit wenig Aufwand mithilfe der nach Stand der Technik ergriffenen Maßnahmen abgewehrt werden können
  → neuartige, außergewöhnliche oder aufwandsintensive Störungen

IT-Sicherheitsgesetz (5)

Verschärfungen im Rahmen IT-Sicherheitsgesetz 2.0:

- **Zugriff** auf Informationen sowie informationsverarbeitende Systeme, Komponenten & Prozesse **ausschließlich durch autorisierte Personen oder Programme** unter Einhaltung von Sicherheitsstandards zur Gewährleistung der informationstechnischen Grundwerte & Schutzziele
- Festlegung einsetzbarer **kritischer Komponenten** (IT-Produkte) & Anzeigepflicht über deren geplanten erstmaligen Einsatz
- Zusätzlich verpflichtet: **Unternehmen im besonderen öffentlichen Interesse**, darunter auch Zulieferer mit wesentlicher Bedeutung
- Speicherung von **Protokolldaten** für 18 Monate zur Abwehr von aus Schadprogrammen resultierenden Gefahren, davon letzte 3 Monate zur automatisierten Auswertung
- Zusätzliche **Kontrollrechte für das BSI** hinsichtlich Sicherheitslücken & Schadprogrammen
- Einsatz von **Systemen zur fortwährenden Angriffserkennung** mit automatischer Erfassung & Auswertung geeigneter Parameter & Merkmale
- Nicht richtig oder nicht vollständig erbrachte Nachweise bußgeldbewehrt unter **Anhebung des Bußgeldes** auf bis zu 1 Mio €

EU-NIS2-Richtlinie (1)

Weitere Verschärfungen durch EU-NIS2-Richtlinie (muss bis 10/24 ins IT-SiG):

- Deutlich **erweiterter Kreis verpflichteter Einrichtungen** (~ 6-fach!)
  - Weitere Sektoren Chemie, verarbeitendes Gewerbe (Medizinprodukte, DV-Geräte, elektrische Ausrüstung, Maschinenbau & Fahrzeugbau), Anbieter digitaler Dienste (Suchmaschinen, soziale Netzwerke), Anbieter verwalteter IT-Dienste, Anbieter verwalteter Sicherheitsdienste, Forschung & Weltraum
  - Bundesministerien
  - Statt Schwellwerte nach BSI-KritisV nun in KRITIS-Sektoren mit > 49 Beschäftigte oder > 10 Mio. € Jahresumsatz (= mittlere Unternehmen lt. EU)
- **Risiken** für die Sicherheit der Netz- und Informationssysteme **müssen beherrschbar** (!) **sein & Risikoexposition der Einrichtung berücksichtigen**
- **Beeinträchtigung** der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit (= Sicherheitsvorfall) ist **zu verhindern oder möglichst gering zu halten**
- **Jede (!) Gefahr eines Sicherheitsvorfalls** ist **zu ermitteln**
- Verhinderung von, Aufdeckung von, Reaktion auf, Wiederherstellung nach und Minderung der (wirtschaftlichen & gesellschaftlichen) Folgen von Sicherheitsvorfällen durch **operative Maßnahmen**
- ISO/IEC 27000 Reihe explizit Referenz

EU-NIS2-Richtlinie (2)

Weitere Verschärfungen durch EU-NIS2-Richtlinie (muss bis 10/24 ins IT-SiG):

- **Maßnahmen** müssen **auf gefahrenübergreifendem** (!) **Ansatz** beruhen, inkl.:
  - Konzepte zur **Risikoanalyse** & **Sicherheit der Informationssysteme**
  - **Bewältigung von Sicherheitsvorfällen**
  - **Aufrechterhaltung des Betriebs** mittels Backups, Wiederherstellung nach einem Notfall & Krisenmanagement
  - **Sicherheit der Lieferkette** (!)
  - **Absicherung** Erwerb, Entwicklung & Wartung von **Netz- und Informationssystemen**; inkl. Offenlegung von Schwachstellen
  - Konzepte & Verfahren zur **Bewertung der Wirksamkeit von Maßnahmen** zum Risikomanagement hinsichtlich Schutz vor Beeinträchtigungen
  - Verfahren zur „**Cyberhygiene**“ (**=** Updates, Passwortänderungen, Zugriffsschutz Admins, Datensicherung, …) & **Schulungen** zur Cybersicherheit
  - Konzepte & Verfahren zu **Kryptographie & Verschlüsselungen**
  - **Sicherheit des Personals**, Konzepte zur **Zugriffskontrolle** & Management von Anlagen
  - **Multi-Faktor-Authentifizierung** oder kontinuierliche Authentifizierung, **gesicherte Sprach-, Video- & Textkommunikation** + Notfallkommunikation

Hersteller-Pflichten für Produkte mit digitalen Elementen (1)

Art. 6 Cyberresilienz-VO**: Produkte mit digitalen Elementen werden nur auf dem Markt bereitgestellt, wenn einerseits**

- **diese den grundlegenden Anforderungen in Anhang I Teil I genügen**,
- die Produkte **ordnungsgemäß installiert**, gewartet und bestimmungsgemäß verwendet werden sowie
- erforderliche **Sicherheitsaktualisierungen installiert** werden

und andererseits Verfahren nach Anhang I Teil II bestehen.

- Art.13 Abs. 1**: Hersteller gewährleisten, dass ihr in Verkehr gebrachtes Produkt mit digitalen Elementen gemäß Anhang I, Teil I konzipiert, entwickelt und hergestellt worden ist.**
- Art. 13 Abs. 4: Hersteller dokumentiert die durchgeführte Bewertung der Cybersicherheitsrisiken in der **technischen Dokumentation**.
- Art. 13 Abs. 6**: Hersteller** meldet festgestellte Schwachstellen an die Stelle, die das Produkt herstellt bzw. wartet, und **behandelt und behebt festgestellte Schwachstellen.**
- Art. 13 Abs. 8: Hersteller legt **Unterstützungszeitraum** entsprechend der vorgesehenen Dauer der voraussichtlichen Nutzung des Produkts fest.

Hersteller-Pflichten für Produkte mit digitalen Elementen (2)

- Art. 13 Abs. 9: Hersteller gewährleistet, dass während des Unterstützungszeit-raums bereitgestellte **Sicherheitsaktualisierungen mindestens 10 Jahre nach Inverkehrbringen** des Produkts (bzw. für die verbleibende Dauer des Unterstützungszeitraums) **verfügbar bleibt**.
- Art. 13 Abs. 12**: Hersteller weisen durch Konformitätsbewertung nach, dass das Produkt mit digitalen Elementen den grundlegenden Anforderungen in Anhang I Teil I genügt.**
- Art. 13 Abs. 19: Hersteller stellen sicher, dass das **Enddatum** des festgelegten Unterstützungszeit-raums zum Zeitpunkt des Kaufs **in leicht zugänglicher Weise** klar und verständlich **angegeben** ist.

Grundlegende Anforderungen Anhang I Teil I

Z. 2 lit. a: Produkt mit digitalen Elementen wird **ohne bekannte ausnutzbare Schwachstellen** auf dem Markt **bereitgestellt**

Z. 2 lit. c: Es ist **sichergestellt**, dass **Schwachstellen durch Sicherheitsaktualisierungen behoben** werden können, die innerhalb eines angemessenen Zeitraums installiert werden sowie über einen klaren und **benutzerfreundlichen Opt-out-Mechanismus** verfügen

Z. 2 lit. d: Produkt bietet geeignete **Kontrollmechanismen zum Schutz vor unbefugtem Zugriff** und meldet einen möglicherweise unbefugten Zugriff

Z. 2 lit. e: Produkt schützt **Vertraulichkeit** gespeicherter, übermittelter oder anderweitig verarbeiteter personenbezogener oder sonstiger Daten (z.B. durch Verschlüsselung)

Hersteller-Pflichten für Produkte mit digitalen Elementen (3)

Grundlegende Anforderungen Anhang I Teil I

- Z. 2 lit. f: Produkt schützt **Integrität** gespeicherter, übermittelter oder anderweitig verarbeiteter Daten, Befehle, Programme und Konfigurationen **vor** einer vom Nutzer **nicht genehmigten Manipulation oder Veränderung** und meldet deren Beschädigung
- Z. 2 lit. g: Verarbeitung personenbezogener oder sonstiger **Daten** ist **auf** das für die **Zweckbestimmung** des Produkts mit digitalen Elementen **erforderliche Maß** zu **beschränken**
- Z. 2 lit. h: Produkt stellt die **Verfügbarkeit** wesentlicher und grundlegender **Funktionen** (auch nach einem Sicherheitsvorfall) sicher, inkl. Abwehr- und Eindämmungsmaßnahmen gegen Überlastungsangriffe auf Server

Z. 2 lit. i: Produkt **minimiert negative Auswirkungen** von den Produkten selbst oder von vernetzten Geräten **auf** die **Verfügbarkeit** der **von anderen Geräten oder** Netzen bereitgestellten **Dienste**

Z. 2 lit. j: Produkt ist so konzipiert, entwickelt und hergestellt worden, dass sie auch **bei externen Schnittstellen möglichst geringe Angriffsflächen** bietet

Z. 2 lit. l: Produkt bietet sicherheitsbezogene Information durch **Aufzeichnung** und/oder Überwachung einschlägiger **interner Vorgänge** wie Zugang zu Daten, Diensten oder Funktionen sowie Änderungen an Daten, Diensten oder Funktionen

Z. 2 lit. m: Produkt bietet den Nutzern die Möglichkeit, alle **Daten und Einstellungen** dauerhaft, sicher und einfach **zu löschen**

Hersteller-Pflichten für Produkte mit digitalen Elementen (4)

Grundlegende Anforderungen Anhang I Teil II

Z. 3: Hersteller von Produkten mit digitalen Elementen müssen die **Sicherheit des Produkts** mit digitalen Elementen **regelmäßig und wirksam testen** und überprüfen

Z. 4: Sobald eine Sicherheitsaktualisierung bereitgestellt worden ist, sind **Informationen über beseitigte Schwachstellen zu teilen** und eindeutige und verständliche Informationen zu veröffentlichen, wie Nutzer die Schwachstelle beheben können

Z. 7: Hersteller stellen Mechanismen für die **sichere Verbreitung von Aktualisierungen** für Produkte mit digitalen Elementen bereit, damit Schwachstellen rechtzeitig (ggf. automatisch) behoben oder eingedämmt werden können

Z. 8: Hersteller stellen **Sicherheitsaktualisierungen kostenlos** zur Verfügung

Für wichtige [nach Anhang III] **und kritische** [nach Anhang IV] **Produkte mit digitalen Elementen bestehen** darüber hinaus **weitere Verpflichtungen (z.B. zur Sicherung der Authentifizierung, zur Prävention und Erkennung von Eindringen sowie zum Netzschutz)**

Haftung IT-Verantwortlicher (1)

- **Schlechterfüllung** arbeitsvertraglicher Pflichten berechtigt zum Schadensersatz (§ 280 I BGB i.V.m. § 611 I BGB)
- Nachweis für Schlechterfüllung obliegt Arbeitgeber (§ 619a BGB)
- Haftung nach **Verschuldensgrad** gestaffelt (§ 276 BGB i.V.m. § 254 BGB):
  ° Vorsatz → voll
  ° grobe Fahrlässigkeit → voll, sofern verhältnismäßig
  ° „mittlere“ Fahrlässigkeit → anteilig
  ° (leichte) Fahrlässigkeit → nicht
  (Grundlage: diverse BAG-Urteile)
- Schadensersatz bei betrieblich veranlassten Tätigkeiten auch abhängig vom Betriebsrisiko („**gefahrgeneigte Arbeit**“)

Haftung IT-Verantwortlicher (2)

- Verletzung des Fernmeldegeheimnisses strafbewährt (§ 206 StGB)
- Urkundenunterdrückung durch Vernichtung, Beschädigung oder Zurückhaltung von (elektronischen) Buchführungsunterlagen strafbar (§ 274 StGB)
- Dritter hat Recht auf Schadensersatz (§ 823 BGB) und Unterlassung (§ 1004 BGB)
- Betroffener kann bei Datenschutzverstoß wider der Sorgfaltspflicht Recht auf Schadensersatz geltend machen (Art. 82 EU-DSGVO)
  → Beweislast trägt der Verantwortliche!
- Verletzung des Datengeheimnisses bzw. Fernmeldegeheimnisses berechtigt (je nach Schwere des Vergehens) zur „fristlosen“ Kündigung (ArbG-Urteile)
- Unbefugte Offenbarung personenbezogener Daten kann (wegen Verstoß gegen Art. 5 Abs. 1 lit. f EU-DSGVO) bis zu 20 Mio. € kosten (Art. 83 Abs. 5 EU-DSGVO)
- Nichteinhaltung EU-NIS2-Richtlinie kann bis zu 10 Mio. € kosten

Einflussfaktor Technik (1)

Informationen als besonderer „Rohstoff“:

- Information ist immateriell
- Wert von Informationen mal exponentiell, mal subtrahierend
- Informationen sind manipulierbar
- Informationen auch unbewusst oder ungewünscht übertragbar
- Zugang zu und Bewertung von Informationen entscheidend

→ neue Maßstäbe! (auch für rechtliche Regelungen!)

Einflussfaktor Technik (2)

Fortentwicklung der Informationstechnik:

- schnelle Fortentwicklung von IT-Systemen (Verdoppelung der Datenspeicherkapazitäten & Arbeitsgeschwindigkeit alle 2 Jahre)
- hohe Komplexität vernetzter IT-Systeme
- stark anwachsender Sektor Informationswirtschaft
- hohe Abhängigkeit von IT-Systemen & Informationen
- Allgegenwart der Datenverarbeitung (Notebooks, Smartphones, IT in vielen technischen Systemen, …)
- Ambivalenz technischer Entwicklungen („dual use“)

→ technisches Grundverständnis nötig

Einflussfaktor Unternehmensspezifika (1)

Branchenzugehörigkeit & Marktstellung

- branchenspezifische Anforderungen (insb. für Banken, Versicherungen, Pharmaunternehmen, Automobilindustrie → Stichwort: „Nachweis guter Praxis“)
- marktbeherrschende Stellung
- internationale Ausrichtung (vor allem hinsichtlich SOX)
- Vorteile durch bzw. Forderung nach Zertifizierungen
- Abwehr von Wirtschaftsspionage (lt. KPMG-Studie 2020:)
  - Datendiebstahl / Datenmissbrauch 31 %
  - Verletzung von Schutz- und Urheberrechten 19 %
  - Verrat von Betriebs- und Geschäftsgeheimnis 16 %

Einflussfaktor Unternehmensspezifika (2)

Innerbetriebliche Organisation

- Stellenwert der IT-Administration
- Bestellung eines Datenschutzbeauftragten
- Einsetzung eines IT-Sicherheitsbeauftragten (CIO, CISO etc.)
- Aktivität der internen Revision (in Kenntnis von IT-Spezifika)
- Bewusstsein (Awareness) hinsichtlich IT-Sicherheit
- Erfahrung aus zurückliegenden Sicherheitsvorfällen / Datenpannen
- Zufriedenheit der Mitarbeiter