IT-Management

11. Informationssicherheit

Prof. Dr. Thomas Allweyer

Informationssicherheit

1. Bedrohungen
2. Sicherheitsziele
3. Informationssicherheits-Managementsystem
4. Informationssicherheitsleitlinie
5. Schutzbedarfsanalyse
6. Zusammenarbeit mit externen Partnern
7. Notfallmanagement
8. Gesetze und Normen
   - ISO 27 001
   - IT-Grundschutz

Informationssicherheit

- **Wachsende Bedeutung der Informationssicherheit**
  - Immer größere Abhängigkeit von IT-Systemen
  - Zunehmende Vernetzung führt zu höherer Verwundbarkeit.
  - Zahlreiche Angriffe
- **Risiko sicherheitsrelevanter Vorfälle reduzieren**
  - Es genügt nicht, einzelne technische Maßnahmen zu ergreifen.
  - Abgestimmtes Konzept erforderlich inkl. Hardware, Software, Organisation, Mitarbeiter
  - Ständige Weiterentwicklung
- **Informationssicherheit umfasst:**
  - IT-Sicherheit – Schutz der IT-Systeme und gespeicherten Daten
  - Schutz von Informationen allgemein, auch in Papierform
  - Meist zudem auch Datenschutz betrachtet
    - Z. B. Schutz personenbezogener Daten vor Missbrauch

Informationssicherheit

1. Bedrohungen
2. Sicherheitsziele
3. Informationssicherheits-Managementsystem
4. Informationssicherheitsleitlinie
5. Schutzbedarfsanalyse
6. Zusammenarbeit mit externen Partnern
7. Notfallmanagement
8. Gesetze und Normen
   - ISO 27 001
   - IT-Grundschutz

Schäden

- **Beispiel**
  - Ransomware-Angriff auf einen norwegischen Aluminiumkonzern im März 2019
  - Trotz guter Backup- und Notfallmanagement-Strategie musste die Produktion wochenlang auf manuellen Betrieb umgestellt werden.
  - Schaden ca. 40 Millionen Euro
- **9 von 10 deutschen Großunternehmen waren 2018 Ziel von DDoS-Angriffen**
  - Gesamtschaden ca. 4 Milliarden Euro

Bedrohungen und Versäumnisse

- **Bedrohungen treffen auf Versäumnisse der Unternehmen.**
- **Beispiele**
  - Mangelhaft konfigurierte Systeme
  - Zu großzügig vergebene Berechtigungen
  - Nicht installierte Sicherheitsupdates
  - Fehlende Backups
  - Unsichere oder für jeden sichtbar notierte Passwörter
- **Behebung eklatanter Versäumnisse und grundlegende Sicherheitsmaßnahmen erhöhen das Sicherheitsniveau deutlich**
  - Wichtig: Bewusstsein für Bedrohungen und Bedeutung der Informationssicherheit

Informationssicherheit

1. Bedrohungen
2. Sicherheitsziele
3. Informationssicherheits-Managementsystem
4. Informationssicherheitsleitlinie
5. Schutzbedarfsanalyse
6. Zusammenarbeit mit externen Partnern
7. Notfallmanagement
8. Gesetze und Normen
   - ISO 27 001
   - IT-Grundschutz

Sicherheitsziele

- **Verfügbarkeit**
  - Systeme und Informationen sind vorhanden und nutzbar.
- **Vertraulichkeit**
  - Informationen sind nur den berechtigten Personen zugänglich.
- **Integrität/Ursprünglichkeit**
  - Informationen und Funktionen wurden nicht in unzulässiger Weise verändert.
- **Authentizität**
  - Die Information stammt tatsächlich von dem angegebenen Urheber.
- **Nachvollziehbarkeit**
  - Es lässt sich nachvollziehen, wer was geändert und gemacht hat.
- **Konformität**
  - Übereinstimmung mit Gesetzen, Standards und Richtlinien (z. B. zum Datenschutz)
- **Verbindlichkeit/Nichtabstreitbarkeit**
  - Es lässt sich eindeutig feststellen, dass eine Information von einem bestimmten Urheber stammt und der Inhalt nicht verändert wurde (Kombination aus Authentizität und Integrität).

Informationssicherheit

1. Bedrohungen
2. Sicherheitsziele
3. Informationssicherheits-Managementsystem
4. Informationssicherheitsleitlinie
5. Schutzbedarfsanalyse
6. Zusammenarbeit mit externen Partnern
7. Notfallmanagement
8. Gesetze und Normen
   - ISO 27 001
   - IT-Grundschutz

Informationssicherheits-Managementsystem (ISMS)

- **Maßnahmen müssen aufeinander abgestimmt werden**
  - Nicht nur technische Maßnahmen, sondern auch Prozesse, Organisation und Mitarbeiter
- **Integration mit existierenden Managementsystemen**
  - U. a. Qualitäts- oder Risikomanagementsystem
  - Erweiterung bestehender Systeme um Aspekte der Informationssicherheit
  - Die Themen sind eng verknüpft
    - Z. B. gibt es viele Risiken, die mit Informationssicherheit in Zusammenhang stehen. Diese müssen im Risikomanagement behandelt werden.

Ebenen eines Informationssicherheits-Managementsystems

Nach: Hanschke, I.: Informationssicherheit und Datenschutz – einfach und effektiv. München 2020.

Ebenen eines Informationssicherheits-Managementsystems

- **Strategie**
  - Ziele und grundsätzliche Festlegungen
  - Beschrieben in Informationssicherheitsleitlinie
- **Anforderungen**
  - U. a. relevante Gesetze und Normen
  - Werden im Rahmen einer Schutzbedarfsanalyse für verschiedene Bereiche und IT-Assets konkretisiert
- **3. und 4. Ebene: Umsetzung der Anforderungen**
  - Siehe nächste Folien
- **Überprüfungen und Nachweise**
  - Audits überprüfen Einhaltung von Standards, z. B. ISO 27001
  - Assessments bewerten Wirksamkeit des Managementsystems
  - Aufzeichnungen: Manuell (z. B. Protokolle von Überprüfungen) oder automatisch (z. B. elektronische Protokolle)

Umsetzung der Anforderungen zur Informationssicherheit – Ebene 3

- **Richtlinien**
  - Verbindliche Anweisungen, z. B. Umgang mit Passwörtern.
  - Werden in Form von Handlungsanweisungen oder technischen Maßnahmen umgesetzt.
- **Konzepte**
  - Bereichsübergreifend angewandte Grundsätze und Vorgehensweisen.
  - Z. B. Konzepte zum Einsatz von Verschlüsselung oder zur Auswahl und zum Einsatz von Standardsoftware
- **Organisation**
  - Rollen, Gremien und Verantwortlichkeiten
  - U. a. Informationssicherheitsbeauftragter und Datenschutzbeauftragter
- **Prozesse**
  - Z. B. Prozesse zur Schutzbedarfsfeststellung oder zum Management von Sicherheitsvorfällen
  - Integration mit Prozessen anderer Bereiche
    - Beispiel: Im Prozess zur Einstellung neuer Mitarbeiter müssen Benutzerkonten und Berechtigungen gemäß den Richtlinien zur Informationssicherheit vergeben werden, und die Mitarbeiter müssen zu dem Thema geschult werden.

Umsetzung der Anforderungen zur Informationssicherheit – Ebene 4

- **Handlungsanweisungen**
  - Verfahrensanweisungen, z. B. Anwendung eines Schemas zur Informationsklassifikation oder des Eigentümerprinzips (jedes IT-Asset hat einen verantwortlichen Eigentümer)
  - Detailliertere Arbeitsanweisungen, z. B. Anleitung zur sicheren Konfiguration eines bestimmten Systems
- **Technische Maßnahmen**
  - Z. B. Zugangsschleusen, Firewalls, Verschlüsselungssoftware
  - Einhaltung von Richtlinien möglichst durch technische Maßnahmen sicherstellen – Handlungsanweisungen können leicht missachtet oder vergessen werden.

Weiteres zu ISMS

- **Ein ISMS ist ständig weiterzuentwickeln**
  - Neue Technologien und neuartige Bedrohungen
  - Hierfür sollte ein ständiger Verbesserungsprozess implementiert werden
- **Ein ISMS benötigt ausreichende Ressourcen**
- **Mitarbeiter haben eine zentrale Bedeutung**
  - Müssen für das Thema sensibilisiert werden
  - Schulungen
  - Konsequentes Handeln der Führungskräfte
    - Keine stillschweigende Duldung von Sicherheitsverstößen

Informationssicherheit

1. Bedrohungen
2. Sicherheitsziele
3. Informationssicherheits-Managementsystem
4. **Informationssicherheitsleitlinie**
5. Schutzbedarfsanalyse
6. Zusammenarbeit mit externen Partnern
7. Notfallmanagement
8. Gesetze und Normen
   - ISO 27 001
   - IT-Grundschutz

Aufbau einer Informationssicherheitsleitlinie

Definition
• Nennung der Organisation • Aufbau • Geschäftszweck • Geltungsbereich der Leitlinie
Analyse
• Regulatorische Anforderungen • Sicherheitsziele • Gefährdungen • Bedeutung der Sicherheit für die Organisation • Angestrebtes Sicherheitsniveau
Regeln
• Sicherheitsorganisation und -prozesse • Wichtige Richtlinien und Konzepte • Verpflichtung der Mitarbeiter • Bekenntnis der Leitungsebene • Inkraftsetzen

In Anlehnung an: Kersten, H.; Klett, G.; Reuter, J.; Schröder, K.: IT-Sicherheitsmanagement nach der neuen ISO 27 001. ISMS, Risiken, Kennziffern, Controls. 2., aktualisierte Auflage. Wiesbaden 2020.

Informationssicherheitsleitlinie

- **Zentrales Dokument des ISMS**
  - Betrifft vor allem die Ebenen Strategie und Anforderungen sowie grundlegende Festlegung zu den Inhalten der anderen Ebenen
- **„Bedeutung der Sicherheit für die Organisation“ und „Angestrebtes Sicherheitsniveau“:**
  - Angemessenes Verhältnis von Aufwand und Nutzen
  - Z. B. benötigt eine Großbank ein höheres Sicherheitsniveau als ein Handwerksbetrieb.

Informationssicherheit

1. Bedrohungen
2. Sicherheitsziele
3. Informationssicherheits-Managementsystem
4. Informationssicherheitsleitlinie
5. Schutzbedarfsanalyse
6. Zusammenarbeit mit externen Partnern
7. Notfallmanagement
8. Gesetze und Normen
   - ISO 27 001
   - IT-Grundschutz

Schutzbedarfsanalyse

- **Auf Grundlage der allgemeinen Sicherheitsanforderungen konkreten Schutzbedarf für die IT-Assets festlegen**
  - U. a. für Geschäftsprozesse, Informationen, Anwendungen, Infrastruktur-Elemente
- **Daraus werden geeignete Maßnahmen erarbeitet und umgesetzt**
  - Organisatorisch und technisch
- **Einschätzung, wie viel Schutz ein IT-Asset benötigt:**
  - Wie wichtig ist es für das Unternehmen?
  - Welcher Schaden droht gegebenenfalls?
    - Für verschiedene Schadenskategorien, z. B. finanzieller Schaden, Imageverlust, Beeinträchtigung der Aufgabenerfüllung
- **Überblick über die vorhandenen Assets benötigt**
  - Informationen aus Service-Configuration-Management und Enterprise-Architecture-Management nützlich
  - Zusammenhänge betrachten: Z. B. hat ein hoher Schutzbedarf eines Geschäftsprozesses auch Auswirkungen auf die in diesem Prozess verwendeten Anwendungssysteme.

Aufgabe

- **Aufgabe: Es wird der Schutzbedarf eines zentralen E-Mail-Servers hinsichtlich Verfügbarkeit betrachtet**
- **Könnte bei Nicht-Verfügbarkeit z. B. Folgendes drohen:**
  - Gefahr für Leib und Leben?
  - Verstoß gegen Gesetze?
  - Finanzielle Schäden?
  - Beeinträchtigte Aufgabenerfüllung?
  - Image-Schaden?

Höhe des Schutzbedarfs

- **Normaler Schutzbedarf**
  - Es drohen gewisse, aber nicht kritische Beeinträchtigungen.
  - Standardsicherheitsmaßnahmen, z. B. aus IT-Grundschutz (siehe weiter hinten)
- **Hoher Schutzbedarf**
  - Es droht gravierender Schaden
  - Erweiterte Sicherheitsmaßnahmen auf Basis individueller Risikoanalyse
- **Sehr hoher Schutzbedarf**
  - Es droht existenzbedrohender Schaden
  - Erweiterte Sicherheitsmaßnahmen auf Basis individueller Risikoanalyse

Informationssicherheit

1. Bedrohungen
2. Sicherheitsziele
3. Informationssicherheits-Managementsystem
4. Informationssicherheitsleitlinie
5. Schutzbedarfsanalyse
6. Zusammenarbeit mit externen Partnern
7. Notfallmanagement
8. Gesetze und Normen
   - ISO 27 001
   - IT-Grundschutz

Beispiele für Risiken durch externe Partnern

- **Verfügbarkeitsrisiken**
  - Die eigenen Dienste funktionieren nur, wenn die Systeme der Partner verfügbar sind
- **Vertraulichkeitsrisiken**
  - Partner haben Zugriff auf einen Teil der Unternehmensdaten
- **Know-how-Risiken**
  - Es kann Wissen zum Partner abfließen und von diesem genutzt werden
- **Risiken in Bezug auf Schutzrechte**
  - Bei gemeinsamen Entwicklungen ist es wichtig, alle benötigten Rechte zu erhalten, auch an den von Partnern entwickelten Teilen.

Nach: Schmidt, K.: Information Security Management. In: Tiemeyer, E. (Hrsg.): Handbuch IT-Management. Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis. 7. Auflage. München 2020, S. 797-840.

Zusammenarbeit mit externen Partnern

- **Alle Sicherheitsziele können durch Geschäftspartner gefährdet werden.**
  - Z. B. können Sicherheitslücken in extern bezogenen Hard- und Softwarekomponenten Angriffe ermöglichen.
- **Zusammenarbeit mit Partnern muss im ISMS berücksichtigt werden**
  - Auswahl geeigneter Partner und Produkte
  - Partner sollten ebenfalls über ein ISMS verfügen und Sicherheitsmaßnahmen belegen können.
  - Verfügbarkeitsrisiken werden reduziert, wenn unternehmenskritische Leistungen von mehreren Partnern bezogen werden.
  - Sicherheitsaspekte sollten vertraglich garantiert werden.
    - U. a. Vertraulichkeitserklärungen und Service-Level-Agreements (SLA)
    - Speziell auf die Sicherheit bezogene Security-Service-Level-Agreements (SSLA)

Informationssicherheit

1. Bedrohungen
2. Sicherheitsziele
3. Informationssicherheits-Managementsystem
4. Informationssicherheitsleitlinie
5. Schutzbedarfsanalyse
6. Zusammenarbeit mit externen Partnern
7. Notfallmanagement
8. Gesetze und Normen
   - ISO 27 001
   - IT-Grundschutz

Informationssicherheit

1. Bedrohungen
2. Sicherheitsziele
3. Informationssicherheits-Managementsystem
4. Informationssicherheitsleitlinie
5. Schutzbedarfsanalyse
6. Zusammenarbeit mit externen Partnern
7. Notfallmanagement
8. **Gesetze und Normen**
   - ISO 27 001
   - IT-Grundschutz

Gesetze und Normen

- **Viele Regelwerke aus dem Kapitel „Compliance“ haben Auswirkungen auf die Informationssicherheit.**
  - Z. B. erfordert die Einhaltung von Regelungen zur elektronischen Buchhaltung und zum Datenschutz den Schutz der Daten vor Verlust und Manipulation.
  - Risikomanagement muss die Risiken aus mangelnder Informationssicherheit berücksichtigen.
  - Auch COBIT und ITIL adressieren das Thema Informationssicherheit.
- **IT-Sicherheitsgesetz (IT-SiG)**
  - Verpflichtung für Betreiber kritischer Infrastrukturen (z. B. Energieversorgung, Telekommunikation, …)
  - Behördliche Aufsichtsbefugnisse
  - Meldepflicht für sicherheitsrelevante Vorfälle

Internationale Norm ISO/IEC 27 001

- Spezifiziert Anforderungen an ein Informationssicherheits-Managementsystem (ISMS)
- Zentrale Norm einer Normenreihe zu ISMS
- Beispiele für Inhalte weiterer Normen (beginnen alle mit 27 0)
  - Grundlegende Begriffe, Leitfäden, Messung, Auditierung, …
- Organisationen können ihr ISMS nach ISO 27 001 zertifizieren lassen

Anforderungen der ISO 27 001 an ein Informationssicherheits-Managementsystem (ISMS)

Kontext der Organisation	**Führung und Verpflichtung**	**Planung**	**Unterstützung**
• Rahmenbedingungen und Anforderungen ermitteln • Informationssicherheits-Managementsystem (ISMS) aufbauen und anwenden	• Übernahme der Verantwortung durch die oberste Führung • Leitlinie erstellen • Rollen, Verantwortlichkeiten, Befugnisse festlegen	• Informationssicherheitsziele festlegen • Risiken managen	• Ressourcen bereitstellen • Kompetenz aufbauen • Bewusstsein schaffen • Für angemessene Kommunikation sorgen • Dokumentieren und mit Dokumenten geeignet umgehen
Betrieb	**Bewertung der Leistung**	**Verbesserung**	
• Umsetzung der ISMS-Aktivitäten planen und steuern (auch für ausgelagerte Prozesse) • Risiken beurteilen und behandeln	• Überwachen und messen • Analysieren und bewerten • ISMS auditieren • Bewertung durch das Management	• Nichtkonformitäten feststellen • Korrekturmaßnahmen durchführen • ISMS ständig verbessern	

ISO 27 001 – Anhang

- **Der Anhang enthält 114 Controls (Sicherheitsmaßnahmen).**
  - Relativ allgemein formuliert – eher weiter aufgeschlüsselte Anforderungen als konkrete Maßnahmen
  - Der Anhang ist ebenfalls verbindlich für eine Zertifizierung.
- **Einordnung der Controls in Sicherheitsthemen**
  - Z. B. Organisation der Informationssicherheit, Zugangssteuerung, Betriebssicherheit, Handhabung von Informationssicherheitsvorfällen
  - Sicherheitsthemen sind wiederum in Maßnahmenziele unterteilt

ISO 27 001 – Anhang: Maßnahmenziele

- **Beispiel: Maßnahmenziele für das Thema „Zugangssteuerung“**
  1. Geschäftsanforderungen an die Zugangssteuerung:
     - Der Zugang zu Information und informationsverarbeitenden Einrichtungen ist eingeschränkt.
  2. Benutzerzugangsverwaltung:
     - Es ist sichergestellt, dass befugte Benutzer Zugang zu Systemen und Diensten haben und unbefugter Zugang unterbunden wird.
  3. Benutzerverantwortlichkeiten:
     - Benutzer sind für den Schutz ihrer Authentisierungsinformation verantwortlich gemacht.
  4. Zugangssteuerung für Systeme und Anwendungen:
     - Unbefugter Zugang zu Systemen und Anwendungen ist unterbunden.

Zitiert nach: Kersten, H.; Klett, G.; Reuter, J.; Schröder, K.: IT-Sicherheitsmanagement nach der neuen ISO 27 001. ISMS, Risiken, Kennziffern, Controls. 2., aktualisierte Auflage. Wiesbaden 2020.

ISO 27 001 – Anhang: Controls

- **Beispiel: Controls für das Ziel „ Benutzerzugangsverwaltung“**
  1. Registrierung und Deregistrierung von Benutzern:
     - Ein formaler Prozess für die Registrierung und Deregistrierung von Benutzern ist umgesetzt, um die Zuordnung von Zugangsrechten zu ermöglichen.
  2. Zuteilung von Benutzerzugängen:
     - Ein formaler Prozess zur Zuteilung von Benutzerzugängen ist umgesetzt, um die Zugangsrechte für alle Benutzerarten zu allen Systemen und Diensten zuzuweisen oder zu entziehen.
  3. Verwaltung privilegierter Zugangsrechte:
     - Zuteilung und Gebrauch von privilegierten Zugangsrechten ist eingeschränkt und wird gesteuert.
  4. Verwaltung geheimer Authentisierungsinformation von Benutzern:
     - Die Zuordnung geheimer Authentisierungsinformation wird über einen formalen Verwaltungsprozess gesteuert.
  5. Überprüfung von Benutzerzugangsrechten:
     - Die für Werte Zuständigen überprüfen in regelmäßigen Abständen die Benutzerzugangsrechte.
  6. Entzug oder Anpassung von Zugangsrechten:
     - Die Zugangsrechte aller Beschäftigten und Benutzer, die zu externen Parteien gehören, auf Information und informationsverarbeitende Einrichtungen werden bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung entzogen oder bei einer Änderung angepasst.

Zitiert nach: Kersten, H.; Klett, G.; Reuter, J.; Schröder, K.: IT-Sicherheitsmanagement nach der neuen ISO 27 001. ISMS, Risiken, Kennziffern, Controls. 2., aktualisierte Auflage. Wiesbaden 2020.

ISO 27 001 - Zertifizierung

- **Für eine Zertifizierung muss dargelegt werden, wie die Anforderungen und Controls (soweit relevant) umgesetzt wurden.**
  - Hierfür muss es eine Dokumentation geben.
- **Die Anforderungen der ISO sind recht allgemein formuliert**
  - Anwendbar für alle Arten von Organisationen und alle Länder
  - Ggf. müssen länderspezifische Gesetze als Ergänzung herangezogen werden.
  - Beispiel: Ein Control legt fest, dass der Schutz personenbezogener Daten den zutreffenden Gesetzen entsprechen muss.
    - Bei einem außereuropäischen Geschäftspartner ist durch eine ISO 27 001-Zertifizierung nicht sichergestellt, dass er die DSGVO einhält.

IT-Grundschutz

- Herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Enthält nicht nur Anforderungen und Vorgehensweisen, sondern auch einen umfassenden Katalog von „Bausteinen“ mit konkreten Sicherheitsmaßnahmen
- Für typische Fragestellungen kann man auf eigenen Bedrohungsanalysen verzichten und stattdessen den Istzustand mit den Bausteinen des IT-Grundschutzes vergleichen
  - Voraussetzung: typische Rahmenbedingungen und normaler Schutzbedarf
- Zum Grundschutz gehören drei BSI-Standards und ein jährlich herausgegebenes IT-Grundschutz-Kompendium
  - Neuester Stand der Technik berücksichtigt

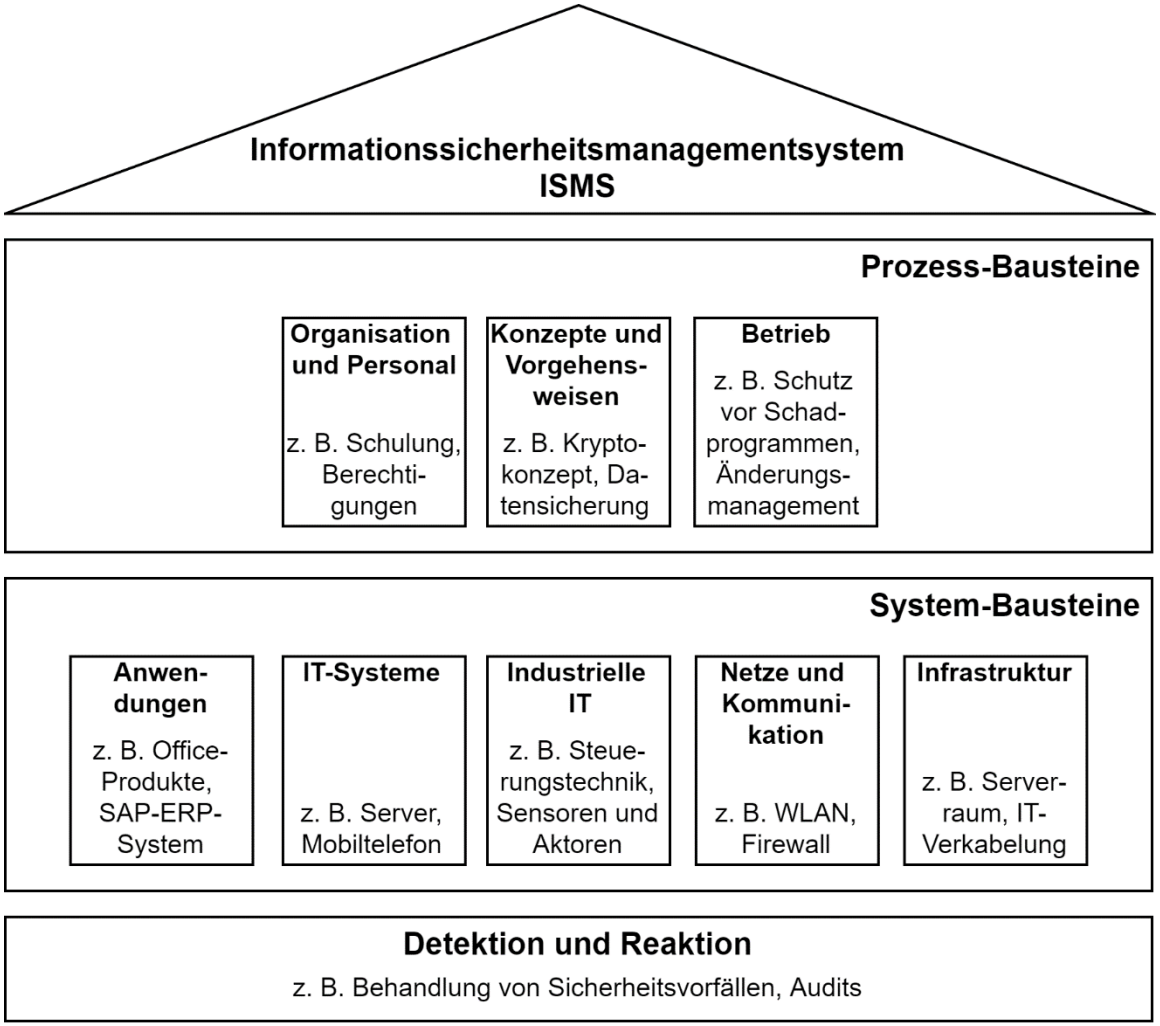
BSI-Standards

- **BSI-Standards**
  - BSI-Standard 200-1: Managementsysteme für Informationssicherheit
  - BSI-Standard 200-2: IT-Grundschutz-Methodik
  - BSI-Standard 200-3: Risikomanagement
- **BSI-Standards sind konform zur ISO 27 001**
  - Ein ISMS auf Basis des IT-Grundschutzes kann nach ISO 27 001 zertifiziert werden.

IT-Grundschutz: Anforderungen und Gefährdungen

- **Anforderungen**
  - Basis-Anforderungen
    - Stellen einen Minimalschutz sicher
    - Diese sollten als Erstes erfüllt werden.
  - Standard-Anforderungen
    - Stellen ein angemessenes Schutzniveau sicher
    - Für eine ISO 27 001-Zertifizierung müssen Basis- und Standardanforderungen erfüllt sein.
  - Anforderungen für erhöhten Schutzbedarf
    - Hierfür werden nur einige beispielhafte Anforderungen aufgeführt.
- **Gefährdungen**
  - Insgesamt 47 elementare Gefährdungen
    - Z. B. Feuer, Netzwerkausfall, Softwarefehler, Ausspähen, Sabotage
  - Die Anforderungen an die einzelnen Bausteine ergeben sich aus elementaren und zusätzlich bausteinspezifischen Gefährdungen.

Gliederung des IT-Grundschutz-Katalogs



Nach: Bundesamt für Sicherheit in der Informationstechnik (Hrsg): ITGrundschutz-Kompendium. Edition 2020. Köln 2020.

Inhalte des Prozessbausteins „Identitäts- und Berechtigungsmanagement“ (1)

Beschreibung	Zielsetzung ist, dass die Benutzer Zugang zu den IT-Ressourcen und Informationen erhalten, die sie benötigen. Unautorisierten Benutzern soll der Zugang verwehrt werden.
Gefährdungs-lage	Als spezifische Bedrohungen und Schwachstellen werden beschrieben: • Fehlende oder unzureichende Prozesse für das Identitäts- und Berechtigungsmanagement • Fehlende zentrale Deaktivierungsmöglichkeiten von Benutzerzugängen • Ungeeignete Verwaltung von Rechten
Anforderungen	Für diesen Baustein sind 21 Anforderungen beschrieben. Zu den Basisanforderungen zählen unter anderem • Regelungen für die Einrichtung von Benutzern, Benutzergruppen und die Vergabe von Berechtigungen • Regelungen des Passwortgebrauchs • Identifikation und Authentisierung

Inhalte des Prozessbausteins „Identitäts- und Berechtigungsmanagement“ (2)

	Beispiele für Standardanforderungen: • Verfahren für das Zurücksetzen von Passwörtern • Geeignete Auswahl von Authentisierungsmechanismen • Festgelegte Prozesse beim Identitäts- und Berechtigungsmanagement • Zentraler Authentifizierungsdienst Beispiele für Anforderungen bei erhöhtem Schutzbedarf: • Berechtigungskonzept für Notfälle • Mehr-Faktor-Authentisierung
Bezug zu elementaren Gefährdungen	Für den Baustein sind 15 der elementaren Gefährdungen relevant. So adressiert die oben genannte Anforderung „Regelung des Passwortgebrauchs“ unter anderem die folgenden Gefährdungen: • Unbefugtes Eindringen in IT-Systeme • Verstoß gegen Gesetze oder Regelungen

- **Vergleiche mit den weiter vorne aufgeführten Controls der ISO 27 001 zum selben Thema**
  - Beschreibungen im Grundschutzbaustein sind umfangreicher und konkreter.
  - Eignen sich als Grundlage für die Umsetzung der ISO-Anforderungen

Inhalte des Systembausteins „Allgemeine Smartphones und Tablets“ (1)

Beschreibung	Ziel des Bausteins ist es, Informationen über typische Gefährdungen für Smartphones und Tablets zu geben sowie Ansätze zu ihrer sicheren Konfiguration aufzuzeigen.
Gefährdungs-lage	Zu den spezifischen Bedrohungen und Schwachstellen gehören unter anderem der Verlust des Geräts, fehlende Betriebssystem-Updates und Schwachstellen in Apps. Geräte können manipuliert, mit Schadsoftware versehen oder webbasierten Angriffen ausgesetzt sein. Fitness- und Ortungsdaten können ebenso wie sensitive Daten auf dem Sperrbild-schirm missbraucht werden. Schließlich drohen Gefahren durch die private Nutzung dienstlicher Geräte oder durch Bring-Your-Own-Device (BYOD), d. h. die dienstliche Nutzung privater Geräte.
Anforderungen	Für diesen Baustein sind 30 Anforderungen beschrieben. Zu den Basisanforderungen zählen unter anderem • Festlegung einer Strategie für Smartphones, Tablets und Cloud-Einsatz • Sichere Grundkonfiguration, Verwendung eines Zugriffsschutzes, restriktive Datenschutzeinstellungen • Updates von Betriebssystem und Apps • Keine Installation von Apps aus unsicheren Quellen

Inhalte des Systembausteins „Allgemeine Smartphones und Tablets“ (2)

	Beispiele für Standardanforderungen: • Richtlinie für Mitarbeiter zur Nutzung mobiler Geräte • Verschlüsselung des Speichers • Schutz vor Phishing und Schadprogrammen • Deaktivierung nicht genutzter Kommunikationsschnittstellen • Auswahl und Freigabe von Apps Beispiele für Anforderungen bei erhöhtem Schutzbedarf: • Zusätzliche Authentisierung vertraulicher Anwendungen • Getrennte Arbeitsumgebungen für private und dienstliche Nutzung • Besonders abgesicherte Endgeräte
Bezug zu elementaren Gefährdungen	Für den Baustein sind 26 der elementaren Gefährdungen relevant. So adressiert die Anforderung „Verschlüsselung des Speichers“ unter anderem die folgenden Gefährdungen: • Ausspähen von Informationen, Abhören • Manipulation von Hard- oder Software • Verstoß gegen Gesetze oder Regelungen • Integritätsverlust schützenswerter Nachrichten

- Daneben gibt es noch Bausteine mit spezifischen Anforderungen für die Betriebssysteme iOS und Android.