IT Sicherheit: IT-Sicherheitsmanagement

Dr. Christian Rathgeb

Hochschule Darmstadt, ATHENE, da/sec Security Group

01.07.2020

IT-Sicherheitsmanagementsystem I

- Technologie allein kann NICHT alle IT-Sicherheitsprobleme einer Institution lösen!
- Es müssen auch (1) organisatorische, (2) personelle, und (3) infrastrukturelle Maßnahmen getroffen/ berücksichtigt werden
  - Beispiele:
    (1) Festlegung von Verantwortlichkeiten, Schlüsselmanagement,
    (2) Schulung, Einweisung, Sensibilisierung von Mitarbeitern,
    (3) Gebäudesicherung

Ein IT-Sicherheitsmanagementsystem (engl. Information Security Management System (ISMS)) ist eine Sammlung von Vorgehensweisen und Vorschriften, um einen IT-Sicherheitsprozess zu etablieren und im laufenden Betrieb aufrechtzuerhalten

IT-Sicherheitsmanagementsystem II

Dimensionen des IT-Sicherheitsmanagements:

- Technologie, z.B.
  - Kryptographische Verfahren
  - Schlüsselverteilung
  - Zugriffskontrolle
- Prozesse, z.B.
  - Festlegung von Verantwortlichkeiten
  - Etablierung des IT-Sicherheitsmanagements
  - Aufrechterhaltung im laufenden Betrieb
- Menschen, z.B.
  - Schulung und Qualifikation
  - Sensibilisierung

IT-Sicherheitskonzept

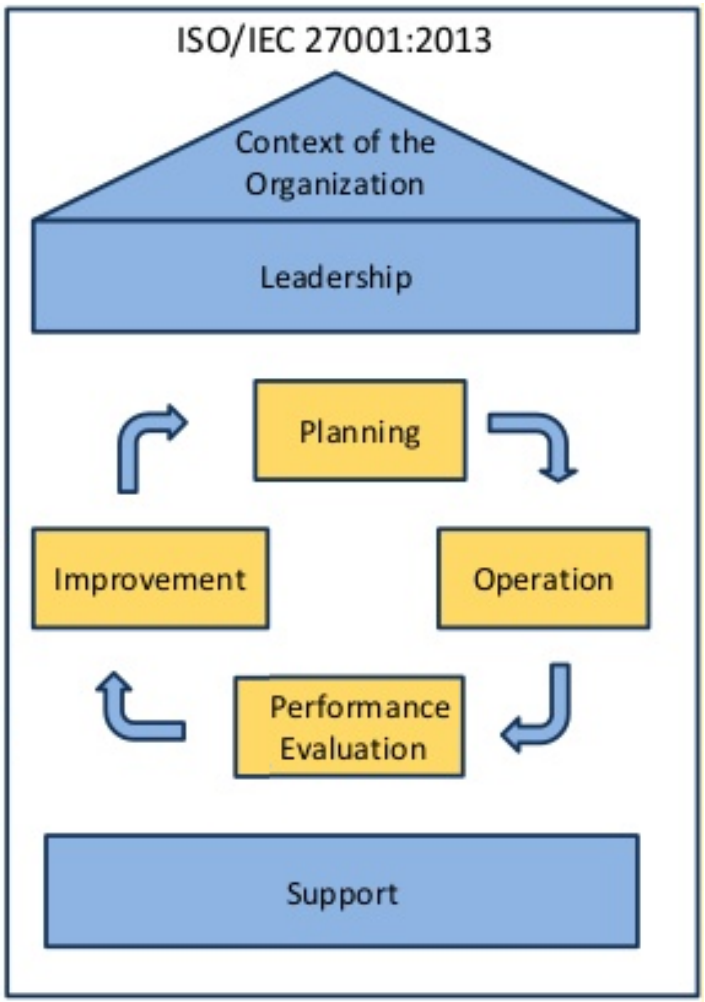
- Schutzmaßnahmen hängen von der konkreten Einsatzumgebung und vom Schutzbedarf der zu verarbeitenden Daten ab
- Alle Sicherheitsmaßnahmen müssen so aufeinander abgestimmt werden, dass sich in der Gesamtheit ein für die Institution angemessenes Sicherheitsniveau ergibt
- Für die Etablierung und Umsetzung der IT-Sicherheitsmaßnahmen gibt es standardisierte Vorgehensmodelle, zB: ISO-Standards 27001 und 27002, IT-Grundschutz des BSI
- Vorgehensmodelle beschreiben den Aufbau eines *IT-Sicherheitskonzeptes*

ISO/IEC 27001

- Der Standard ISO/IEC 27001 enhält sieben wesentliche Kapitel:

1. Context of the organization
2. Leadership
3. Planning
4. Support
5. Operation
6. Performance evaluation
7. Improvement

ISO/IEC 27001: Überblick



ISO/IEC 27001: Context of the organization

- Die Aufgabe der Organisation ist es eine Umgebungsanalyse durchzuführen
- Welche internen/ externen Faktoren sind relevant für das IT-Sicherheitsmanagement?
- Das Ziel bzw. die Abgrenzung des IT-Sicherheitsmanagement muss ermittelt werden
- Für die gegebene Zielsetzung müssen entsprechende Anforderungen definiert werden

ISO/IEC 27001: Leadership

- Diese Teil des Standards betrifft die Führung (Management) der Organisation
- IT-Sicherheits-Richtlinien müssen durch die Führung entwickelt und festgehalten werden
- Eine detailierte Dokumentation von IT-Sicherheits-Richtlinien muss erstellt werden
- Das Vorhandensein der benötigten Ressourcen muss sichergestellt werden
- Unterstützung von Angestellten zur Umsetzung der Richtlinien
- Zuständigkeiten müssen definiert werden

ISO/IEC 27001: Planning

- In der Planung wird ein Umsetzungsplan für das benötigte IT-Sicherheitsmanagement entwickelt (Zeitplan, Arbeitsschritte, Zuständigkeiten etc.)
- Ein wichtiger Teil der Planung ist das Identifizieren von Möglichen Risiken
- Eine Risikoanlyse wird durchgeführt (Information security risk assessment) in welcher identifizierte Risiken bewertet werden
- Weiters müssen entsprechende Maßnahmen definiert werden (Information security risk treatment) welche beim Eintritt entsprechender Risiken durchgefüht werden

ISO/IEC 27001: Support

- In diesem Punkt müssen benötigte unterstützende Faktoren definiert werden
- Dies beinhaltet benötigte Ressourcen sowie entsprechende Kompetenzen
- Weiters muss dokumentierte Information welche für das IT-Sicherheitsmanagement benötigt wird definiert werden
- Auch die Definition der benötigten internen/ externen Kommunikation für das IT-Sicherheitsmanagement fällt unter diesen Punkt

ISO/IEC 27001: Operation

- Unter diesen Punkt fällt die operative Planung und Kontrolle
- Der im Punkt Planning definierte Umsetzungsplan für das benötigte IT-Sicherheitsmanagement wird implementiert und kontrolliert
- Dies beinhaltet eine wiederholte Durchführung einer Risikobewertung und entsprechender Maßnahmen
- Risikobewertung und entsprechender Maßnahmen sollten in entsprechenden Berichten dokumentiert werden

ISO/IEC 27001: Performance evaluation

- Die Organisation muss die Effektivität des eingeführten IT-Sicherheitsmanagement analysieren und evaluieren
- Dazu muss definiert werden wann eine solche Evaluierung durchgeführt wird und von wem
- Weiters muss definiert werden welche Aspekte/ Prozesse/ Personen analysiert werden müssen
- Die Methoden der Messung müssen eine Wiederholung der Messung mit gleichen Ergebnissen erlauben (Reproducibility)

ISO/IEC 27001: Improvement

- Die sich aus der Evaluierung ergebenden (potentiellen) Fehler müssen identifiziert und korregiert werden
- Das korrigierte System muss im nächsten Schritt erneut evaluiert werden
- Das Ergebnis der Verbesserung muss dokumentiert werden
- Ensprechende Verbesserungen sollten bei Bedarf wiederholt durchgeführt werden

Die in ISO/IEC 27001 definierten Schritte sowie geeigente Mechanismen zur Umsetzung werden in ISO/IEC 27002 detailierter beschrieben.

Der IT-Grundschutz des BSI I

- Die Methode des IT-Grundschutzes basiert auf zwei Werken:
  1. Dem BSI-Standard 100-2, der die IT-Grundschutz-Vorgehensweise beschreibt,
  2. und den IT-Grundschutz-Katalogen, welche die Baustein-, Gefährdungs- und Maßnahmenkataloge enthalten.
- Der IT-Grundschutz nutzt die Tatsache, dass ein Großteil der in der Praxis vorhandenen IT-Systeme und Anwendungen von den Anwendern ähnlich und in vergleichbaren Einsatzumgebungen betrieben wird.
- Beispiele: Server unter Unix, Client-PCs unter Windows oder Datenbankanwendungen.

Der IT-Grundschutz des BSI II

- Durch den Einsatz dieser typischen Komponenten ergeben sich immer wieder ähnliche Gefährdungen für den IT-Betrieb. Wenn nicht besondere Sicherheitsanforderungen vorliegen, sind diese Gefährdungen weitgehend unabhängig vom Nutzungsszenario.
- Hieraus ergeben sich zwei Ideen für die Herangehensweise:

  1. Eine umfassende Risikoanalyse ist nicht immer notwendig: Die Gefährdungen für den IT-Betrieb und die Wahrscheinlichkeit für Schäden, die sich aus diesen Gefährdungen ergeben, lassen sich unter bestimmten Voraussetzungen pauschalisieren.
  2. Es ist nicht immer notwendig, Sicherheitsmaßnahmen für jeden Anwendungsfall neu zu entwickeln: Es lassen sich Bündel von Standard- Sicherheitsmaßnahmen ableiten, die bei normalen Sicherheitsanforderungen einen angemessenen und ausreichenden Schutz vor diesen Gefährdungen bieten.

Der IT-Grundschutz des BSI III

- Auf Basis dieser Annahmen schlägt IT-Grundschutz eine Vorgehensweise zur Erstellung und Prüfung von Sicherheitskonzepten vor.
- Im BSI-Standard 1002 zur IT-Grundschutz-Vorgehensweise ist Schritt für Schritt beschrieben, wie ein Informationssicherheitsmanagement in der Praxis aufgebaut und betrieben werden kann.
- IT-Grundschutz interpretiert damit die sehr allgemein gehaltenen Anforderungen der ISO-Standards 27001 und 27002 und hilft Anwendern in der Praxis bei der Umsetzung mit vielen Hinweisen, Hintergrundwissen und Beispielen.

Der IT-Grundschutz des BSI V

- Erst bei einem signifikant höheren Schutzbedarf oder für IT-Systeme, die nicht in den IT-Grundschutz-Katalogen behandelt werden, muss eine ergänzende Sicherheitsanalyse durchgeführt werden.
- Zusammenfassend ergeben sich folgende Vorteile durch eine Orientierung am IT-Grundschutz:
  - Standard-Sicherheitsmaßnahmen werden konkret und detailliert beschrieben
  - Die resultierenden Sicherheitskonzepte sind erweiterbar, aktualisierbar und kompakt, da sie auf eine existierende Referenzquelle verweisen
  - Die umzusetzenden Sicherheitsmaßnahmen sind praxiserprobt und so ausgewählt, dass ihre Umsetzung möglichst kostengünstig möglich ist

IT-Sicherheitskonzept (BSI) I

- Erarbeitung eines IT-Sicherheitskonzeptes erfolgt in mehreren Schritten:

1. **IT-Strukturanalyse** in der alle Bestandteile des IT-Verbund der Institution beschrieben werden
2. **Schutzbedarfsanalyse** ermittelt an Hand von möglichen Schadensszenarien den Schutzbedarf der Daten, IT-Systeme und Räumlichkeiten
3. **Gefährdungsanalyse** in der mögliche Gefährdungen, die Schäden verursachen können, ermittelt werden

IT-Sicherheitskonzept (BSI) II

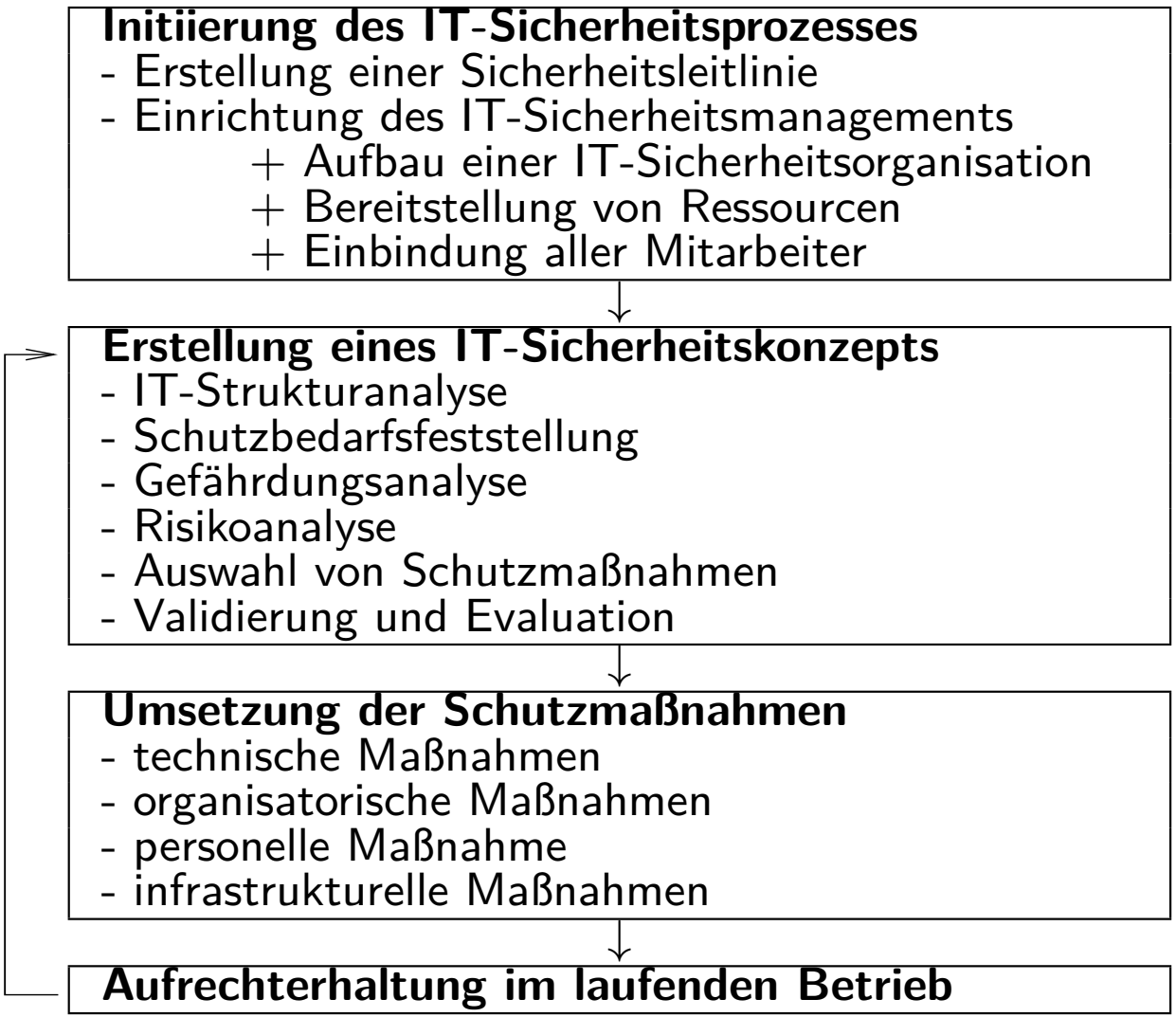
4. **Risikoanalyse** bewertet die Gefährdungen an Hand der Eintrittswahrscheinlichkeit und den möglichen Schäden (ermittelt in der Schutzbedarfsanalyse), die durch die ermittelten Gefährdungen entstehen können.
5. **Schutzmaßnahmen** werden an Hand der Risikoanalyse für jede Gefährdung ausgewählt
6. **Evaluierung** geschieht extern oder intern und überprüft, ob die ausgewählten Schutzmaßnahmen wirksam und ausreichend sind, um den IT-Verbund in seiner Gesamtheit zu schützen

- Die einzelnen Umsetzungspunkte, insbesondere Bedrohungs- und Risikoanalyse erfordern fundierte Kenntnisse über Sicherheitsprobleme und Schwachstellen!

IT-Sicherheit als Querschnittsaufgabe

- Im Anschluss müssen die Schutzmaßnahmen umgesetzt und im laufenden Betrieb aufrechterhalten werden
- Dies erfordert die Überwachung der Einhaltung der Schutzmaßnahmen und Anpassungen am Sicherheitskonzept
- Beispiel: bei Sicherheitsvorfällen oder Änderungen der Bewertung eingesetzter kryptographischer Verfahren
- Ressourcen müssen bereitgestellt werden und klare Verantwortlichkeiten müssen benannt werden
- *IT-Sicherheit ist eine Querschnittsaufgabe, die alle Bereiche einer Institution betreffen und muss daher im Verantwortungsbereich der Führung liegen!*

Ebenen eines IT-Sicherheitsmanagementsystem (BSI)



strategische Ebene (Leitungsaufgabe)

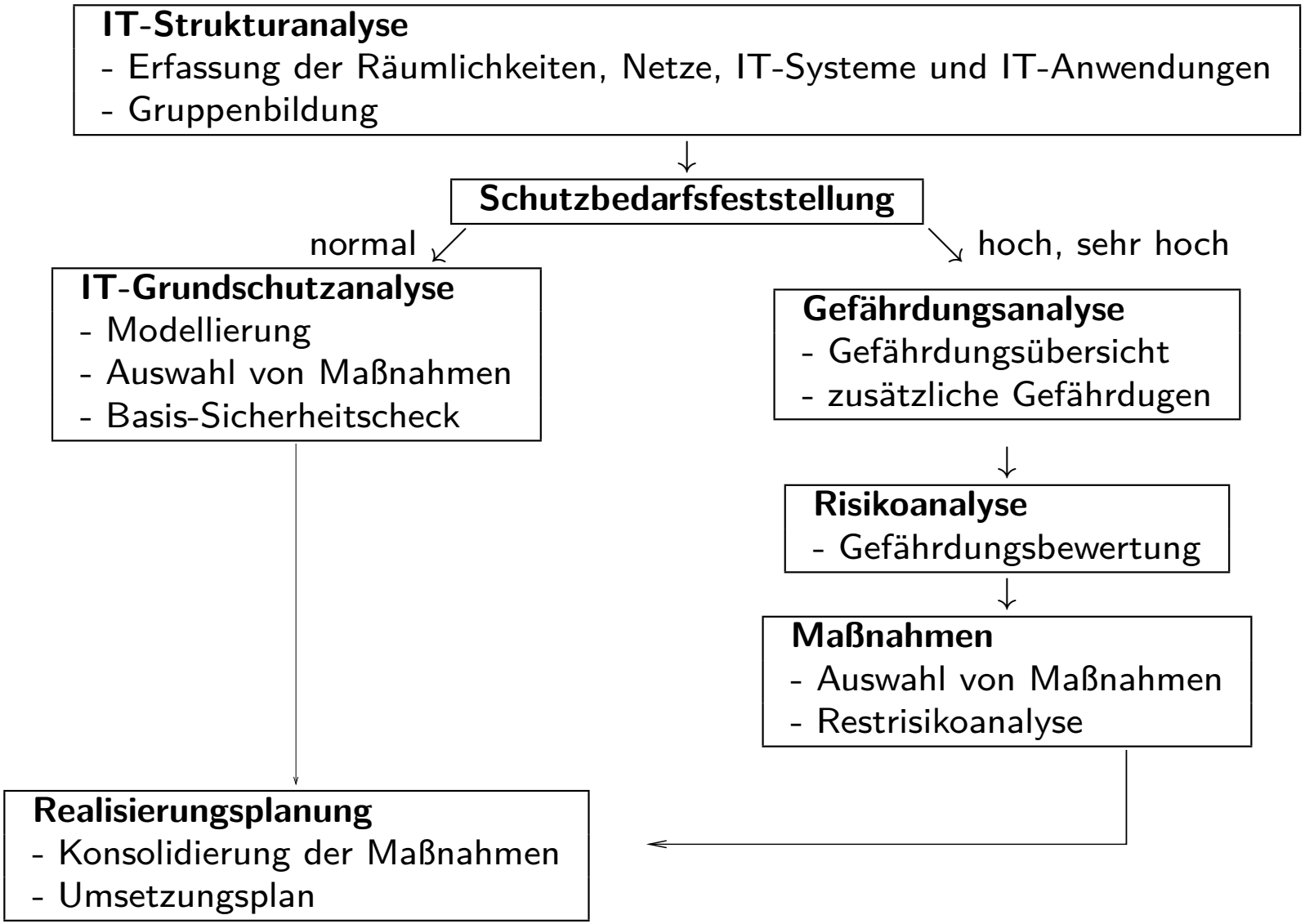
taktische Ebene

operative Ebene

IT-Sicherheitskonzept nach IT-Grundgesetz

- Für Standardkomponenten eines IT-Verbundes, für die sich ein normaler Schutzbedarf ergibt, wurden vom BSI bereits Gefährdungs- und Risikoanalysen durchgeführt und Schutzmaßnahmen vorgeschlagen (beschrieben in den IT-Grundschutzkatalogen)
- Vorgehen umfasst: Strukturanalyse, Schutzbedarfsfestellung, Modellierung des IT-Verbundes (Formulierung der Bestandteile des IT-Verbundes), Auswahl von Maßnahmen und Basis-Sicherheitscheck, bei normalem Schutzbedarf
- Für IT-Systeme, mit hohem bis sehr hohem Schutzbedarf (bzw. die im Grundschutz nicht vorgesehen sind), müssen zusätzlich Gefährdungs- und Risikoanalysen durchgeführt werden

IT-Sicherheitskonzept



IT-Strukturanalyse I

- Ziel der Strukturanalyse ist die Darstellung aller Bestandteile des IT-Verbundes und ihrer Beziehungen untereinander:

1. Geschäftsprozesse (z.B. Personalverwaltung, Entgegennahme von Bestellungen),
2. Daten/Informationen (z.B. Personaldaten, Verträge, aber auch technische Informationen wie Konfigurationsdateien),
3. Anwendungen (z.B. Betriebssysteme, Office-, E-Mail-, Backup-Programme),
4. IT-Systeme (z.B. Computer, Server, Router, USB-Sticks),
5. Kommunikationsnetze (z.B. Intranet, Internet),
6. Räumlichkeiten (z.B. Büros, Standorte).

IT-Strukturanalyse II

- Die Erhebung muss strukturiert erfolgen
- Ausgehend von den Geschäftsprozessen werden zunächst alle relevanten Daten/Informationen erhoben, die für die Geschäftsprozesse benötigt werden
- Im nächsten Schritt werden dann alle Anwendungen, die die erhobenen Daten/Informationen verarbeiten und darauf folgend die IT-Systeme, auf denen die Anwendungen laufen, ermittelt
- Zum Abschluss werden die Räumlichkeiten ermittelt, in denen ermittelte IT-Systeme stehen und die Kommunikationsnetze, an denen die IT-Systeme angeschlossen sind

IT-Strukturanalyse III

- Um die Komplexität zu verringern, sollten ähnliche Objekte zu Gruppen zusammengefasst werden, z.B., wenn sie
- vom gleichen Typ sind,
- ähnlich konfiguriert sind,
- ähnlich in das Netz eingebunden sind,
- ähnlichen Rahmenbedingungen unterliegen,
- ähnliche Anwendungen bedienen.
- Typischerweise können Arbeitsplatzrechner von Mitarbeitern, die ähnliche Aufgaben erledigen, zu einer Gruppe zusammengefasst werden. Gleiches gilt für Büroräume.

Schutzbedarfsfeststellung

Schutzbedarfsanalyse gliedert sich in mehrere Schritte.

- Zunächst wird der Schutzbedarf der Informationen bestimmt.
- Der Schutzbedarf der IT-Systeme und Kommunikationsnetze richtet sich dann im Wesentlichen nach dem Schutzbedarf der in diesen Systemen zu verarbeitenden Informationen.
- Ähnlich wird der Schutzbedarf der Räume, in denen die IT-Systeme untergebracht sind, bestimmt.

Ergebnis ist eine Auflistung

- des Schutzbedarfs aller in der IT-Strukturanalyse aufgeführten Teile hinsichtlich der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit

Modellierung

Idee des IT-Grundschutz: Beschreibung der Bestandteile (Prozesse, Anwendungen, IT-Systeme, Kommunikationsnetze, Räumlichkeiten) einer Institution als Bausteine

- nicht jeder Rechner wird einzeln betrachtet, sondern ähnliche Rechner mit ähnlichen Aufgaben zusammengefasst (Reduktion der Komplexität)
- Zu jedem Baustein finden sich in den IT-Grundschutzkatalogen Gefährdungen und entsprechende Maßnahmen gegen diese Gefährdungen

Auswahl von Maßnahmen I

- Im Schritt Modellierung wurden alle Komponenten als Bausteine formuliert
- In den IT-Grundschutzkatalogen finden sich für jeden Baustein:
  - Gefährdungen
  - Schutzmaßnahmen

Gilt nur für Bausteine mit Schutzbedarf normal
Die Gefährdungen werden im IT-Grundschutz wie folgt kategorisiert:

- Höhere Gewalt
- Organisatorische Mängel
- Menschliche Fehlhandlungen
- Technisches Versagen
- Vorsätzliche Handlungen

Auswahl von Maßnahmen II

Entsprechende Schutzmaßnahmen finden sich in folgenden Kategorien:

- Planung und Konzeption
- Umsetzung
- Betrieb
- Aussonderung
- Notfallvorsorge

Auswahl von Maßnahmen III

Bei der Auswahl und Anpassung der Schutzmaßnahmen sollten die folgende Aspekte berücksichtigt werden:

- Wirksamkeit: Sie müssen vor den möglichen Gefährdungen wirksam schützen
- Eignung: Sie müssen in der Praxis einsetzbar sein, d.h. keine Organisationsabläufe behindern oder andere Schutzmaßnahmen aushebeln
- Praktikabilität: Sie sollten leicht verständlich, einfach anwendbar und wenig fehleranfällig sein
- Akzeptanz: Sie sollten barrierefrei sein und niemanden diskriminieren
- Wirtschaftlichkeit: Sie sollten das Risiko bestmöglich minimieren aber auch in einem geeigneten Verhältnis zu den zu schützenden Werten stehen

Basis-Sicherheitscheck

- Falls die IT-Grundschutz-Vorgehensweise auf einen existierenden Informationsverbund angewandt wird, muss geprüft werden, welche Standard- Sicherheitsmaßnahmen, die in der Modellierung als
  - erforderlich identifiziert wurden,
  - bereits umgesetzt sind
  - und wo noch Defizite bestehen
- Hierzu werden Interviews mit den Verantwortlichen und stichprobenartige Kontrollen durchgeführt
- Dieser Arbeitsschritt wird als Basis-Sicherheitscheck bezeichnet

Schadensszenarien I

Stärke der eingesetzten Schutzmaßnahmen hängt ab vom Schutzbedarf der

- Geschäftsprozesse,
- Informationen,
- IT-Systeme,
- Kommunikationsnetze,
- Räumlichkeiten

hinsichtlich der Schutzziele

- Vertraulichkeit,
- Integrität,
- Authentizität,
- Nichtabstreitbarkeit,
- Verfügbarkeit

Schadensszenarien II

Typische Schadensszenarien

- Verstoß gegen Gesetze, Vorschriften, Verträge
- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung
- Negative Innen- oder Außenwirkung
- Finanzielle Auswirkungen

Schadensszenarien III

Verstoß gegen Gesetze/Vorschriften/Verträge:

Die Schwere des Schadens ist abhängig von den rechtlichen Konsequenzen, die sich aus dem Nichterreichen der oben aufgeführten Ziele ergeben können.

Beispiele für in Deutschland relevante Gesetze, Vorschriften und Verträge sind:

- Gesetze: Grundgesetz, Bürgerliches Gesetzbuch, Bundesdatenschutzgesetz und Datenschutzgesetze der Länder, Informations- und Kommunikationsdienstgesetz, Gesetz zur Kontrolle und Transparenz im Unternehmen
- Vorschriften: Verschlusssachenanweisung. Verwaltungsvorschriften, Verordnungen und Dienstvorschriften
- Verträge zur Wahrung von Betriebsgeheimnissen, Dienstleistungsverträge im Bereich Datenverarbeitung

Schadensszenarien IV

Beeinträchtigung des informationellen Selbstbestimmungsrechts:, z.B.

- Unzulässige Erhebung personenbezogener Daten ohne Rechtsgrundlage oder Einwilligung,
- unbefugte Kenntnisnahme bei der Datenverarbeitung bzw. der Übermittlung von personen- bezogenen Daten,
- unbefugte Weitergabe personenbezogener Daten,
- Nutzung von personenbezogenen Daten zu einem anderen, als dem bei der Erhebung zulässigen Zweck,
- Verfälschung von personenbezogenen Daten in IT-Systemen oder bei der Übertragung

Schadensszenarien V

Beeinträchtigung der persönlichen Unversehrtheit:
Fehlfunktionen von IT-Systemem können unmittelbar zu gesundheitlichen Schäden (Verletzungen, Invalidität oder Tod von Personen) führen.
Beispiele hierfür sind

- medizinische Überwachungsrechner,
- medizinische Diagnosesysteme,
- Flugkontrollrechner,
- Verkehrsleitsysteme

Schadensszenarien VI

Beeinträchtigung der Aufgabenerfüllung: Der Verlust der Ziele Verfügbarkeit oder Integrität von Daten kann die Aufgabenerfüllung in einer Institution erheblich beeinträchtigen.
Beispiele hierfür sind

- Fristversäumnisse durch verzögerte Bearbeitung von Verwaltungsvorgängen,
- verspätete Lieferung aufgrund verzögerter Bearbeitung von Bestellungen,
- fehlerhafte Produktion aufgrund falscher Steuerungsdaten,
- unzureichende Qualitätssicherung durch Ausfall eines Testsystems

Schadensszenarien VII

Negative Innen- oder Außenwirkung: Durch den Verlust einer der Ziele Vertraulichkeit, Integrität oder Verfügbarkeit einer IT-Anwendung können verschiedenartige negative Innen- oder Außenwirkungen entstehen.
Beispiele hierfür sind

- Ansehensverlust einer Institution,
- Vertrauensverlust gegenüber einer Institution,
- Demoralisierung der Mitarbeiter,
- Beeinträchtigung der wirtschaftlichen Beziehungen zusammenarbeitender Institutionen,
- verlorenes Vertrauen in die Arbeitsqualität einer Institution,
- Einbuße der Konkurrenzfähigkeit

Schadensszenarien VIII

Finanzielle Auswirkungen: Finanzielle Schäden können durch den Verlust der Vertraulichkeit schutzbedürftiger Daten, die Veränderung von Daten oder den Ausfall von IT-Anwendungen entstehen. Beispiele hierfür sind

- unerlaubte Weitergabe von Forschungs- und Entwicklungsergebnissen,
- Ausfall eines IT-gesteuerten Produktionssystems und dadurch bedingte Umsatzverluste,
- Einsichtnahme in Marketingstrategiepapiere oder Umsatzzahlen,
- Ausfall eines Buchungssystems einer Reisegesellschaft,
- Zusammenbruch des Zahlungsverkehrs einer Bank,
- Diebstahl oder Zerstörung von Hardware

Schadensszenarien IX

Üblich ist die Einteilung in die folgenden drei Kategorien:

mittel	Die Schadensauswirkungen sind begrenzt und überschaubar
hoch	Die Schadensauswirkungen können beträchtlich sein
sehr hoch	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle: Schutzbedarfskategorien

Berücksichtigung der individuellen Gegebenheiten einer Institution:

- Ein Verlust von 200.000 Euro ist für einen großen Konzern nicht bedrohlich,
- kann bei ein kleines Unternehmen aber zur Insolvenz führen