



Deggendorf Institute of Technology

Grundlagen der Informationssicherheit

amar.almaini@th-deg.de






Amar Almaini

innovativ & lebendig – Bildungsregion DonauWald

Organisatorisches (WS 2019/20)

- Pflichtmodul
- Vorlesung mittwochs, 9.45 – 13.00 Uhr, Pause 15 Min, E 006
- Kontaktmöglichkeiten:
 - persönlich nach Vorlesung oder zur Sprechstunde (nach Vereinbarung)
 - per Mail an amar.almaini@th-deg.de
dem Subjekt bitte „[InfoSec]“ voranstellen
- Prüfung
 - Klausur, 90'
- Übungen
 - Tbd. (Voraussichtlich 3 Übungsblätter)
- Einschreibeschlüssel (iLearn): CY-1-B-WS1920

Literatur

-  Address, Jason. *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress, 2014.
-  Weber, Kristin, Andreas E. Schütz, and Tobias Fertig. "Mitarbeiter zielgerichtet sensibilisieren." *Grundlagen und Anwendung von Information Security Awareness*. Springer Vieweg, Wiesbaden, 2019. 19-22.
-  Paar, Christof, and Jan Pelzl. *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.
-  Matt, Bishop. *Introduction to computer security*. Pearson Education India, 2006.
-  Ferguson, Niels, Bruce Schneier, and Tadayoshi Kohno. "Cryptography engineering." *Design Princi* (2010).

Inhalt der Lehrveranstaltung

- Einführung, Motivation, Grundlagen, Begriffe
- Risikoanalyse
- Kryptologie
- Klassische Verschlüsselungsverfahren
- Moderne Verschlüsselungsverfahren
- Hashfunktionen
- Programmsicherheit
- Security in Network
- Kryptografische Protokolle
- Schlüsselverwaltung

Motivation

Schlagzeilen der letzten Zeit

- 2.2 Milliarden Passwort-Credentials gestohlen und veröffentlicht ([Link](#), 25. 01. 2019)
- Cambridge Analytica hat 50 Millionen Facebook-Profile gescrapet und ggf. missbraucht ([Link](#), 21. 03. 2018)
- Gravierende Prozessor-Sicherheitslücken: Meltdown und Spectre ([Link](#), 04. 01. 2018)
- „Todesstoß: Forscher zerschmettern SHA-1“ ([Link](#), 23. 02. 2017)
- „Vault 7: Wikileaks präsentiert Liste der CIA-Hacker-Werkzeuge“ ([Link](#), 23. 02. 2017)
- „Kriminelle bieten Mirai-Botnetz mit 400.000 IoT-Geräten zur Miete an“ ([Link](#), 25. 11. 2016)

Motivation



Sicherheitssystem ist nur so stark wie sein schwächstes Glied.

Das BSI bietet einen „Leitfaden Informationssicherheit“

Der gibt einen kompakten Überblick über die wichtigsten organisatorischen, infrastrukturellen und technischen Informationssicherheitsmaßnahmen.

- Sicherheit ist ein Grundbedürfnis des Menschen – und damit unserer Gesellschaft.
- In Zeiten von Globalisierung, steigender Mobilität und wachsender Abhängigkeit der Industrienationen von Informations- und Kommunikationstechnik nimmt das Sicherheitsbedürfnis immer mehr zu.

„Leitfaden Informationssicherheit“

- Wachsende Verwundbarkeit und die Gefahr massiver wirtschaftlicher Schäden in Folge von Risiken bei der Informationsverarbeitung erhöhen den Handlungsdruck, durch aktives Informationssicherheitsmanagement, Schäden zu verhindern und das Restrisiko zu minimieren
- Die Verantwortung beschränkt sich keineswegs auf die jeweiligen IT-Fachabteilungen. Vielmehr gilt: Sicherheit ist Chefsache
- Verschiedene Gesetze und Regelungen belegen die persönliche Haftung von Geschäftsführern bzw. Vorständen im Falle von Versäumnissen

Einführung

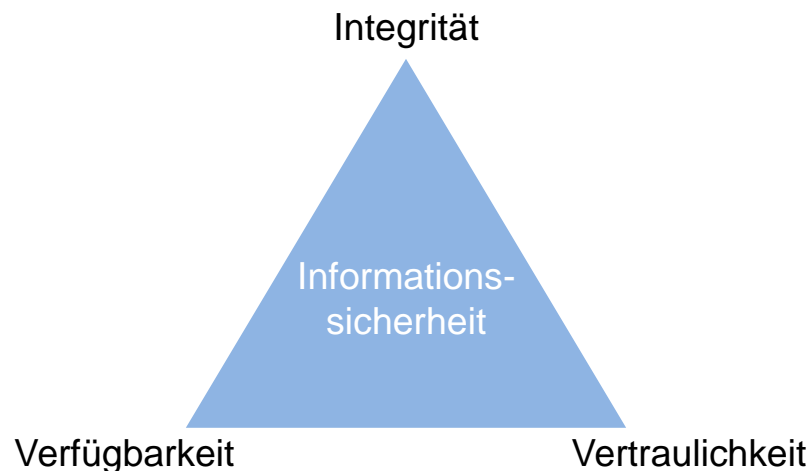
- Die Grundlage für Sicherheit sind Vermögenswerte, die geschützt werden müssen. Im Bereich der Informationssicherheit werden die Vermögenswerte oft als Informationsbestände gekennzeichnet
- Wir behaupten, dass es die Informationen sind, die der primäre Vermögenswert darstellen. Die IT und andere Ressourcen sind Werkzeuge zur Vereinfachung des Informationsmanagements.
- Der Begriff Informationssicherheit drückt daher aus eine ganzheitlichere Sichtweise als die IT-Sicherheit, die sich durch die Konzentration auf die technische Ressourcen in einer eher technischen Sichtweise äußert

Einführung

Informationstechnologie (IT) ist ein Konzept, das sich auf digitale Technologie bezieht, d. H. Hard- und Software zum Erstellen, Sammeln, Verarbeiten, Speichern, Übertragen, Präsentieren und Vervielfältigen von Informationen. Die Information kann in der Form von z.B. Ton, Text, Bild oder Video sein. IT bedeutet daher eine Verschmelzung der traditionellen Bereiche Computer, Telekommunikation und Medien.

Schutzziele: Vertraulichkeit, Integrität und Verfügbarkeit.

Die Sicherheit in Bezug auf IT und Informationen wird normalerweise durch drei Aspekte oder Ziele definiert. **Vertraulichkeit**, **Integrität** und **Verfügbarkeit**. Diese können als Sicherheitsziele angesehen werden und werden häufig als „CIA-Triade“ bezeichnet.



Schutzziel: Vertraulichkeit (Confidentiality)

Unter Vertraulichkeit versteht man, die Verhinderung der unbefugten Weitergabe oder Verwendung von Informationen.

Will man Informationen vertraulich behandeln, muss klar festgelegt sein, wer in welcher Art und Weise Zugriff auf diese Informationen hat.

- sensitive Daten, z. B.
 - Personenbezogen
 - Geschäftsgeheimnisse
 - Militärische Geheimnisse

Schutzziel: Vertraulichkeit (Confidentiality)

- wird durch Mechanismen bzw. Dienste gewährleistet, z.B.
 - Ver- und Entschlüsselung (Kryptografie)
 - Zugriffssteuerung (Access Control)
 - Verbergen in „unverdächtigen“ Daten (Steganographie)

- Beispiel aus der **Praxis**
 - E-Mail-Verkehr
 - Online-Banking

Schutzziel: Integrität (Integrity)

Unter Integrität versteht man, die Verhinderung der unbefugten Änderung von Informationen (**starke Integrität**) oder, dass es zumindest nicht möglich sein darf, Informationen **unerkannt** bzw. **unbemerkt** zu ändern (**schwache Integrität**).

- realisiert durch
 - Verhinderung unautorisierten Schreibzugriffs
 - Erkennung einer Integritätsverletzung (z.B. durch kryptografische Prüfsummen)

Schutzziel: Integrität (Integrity)

- Verletzung der Integrität möglich durch
 - unautorisierte Personen (Angriff von außen)
 - autorisierte Personen (Angriff von innen)

- Beispiel aus der **Praxis**

- Shared User Accounts

wenige Benutzerkonten mit Passwort vorhanden, die anschließend von mehreren Personen benutzt werden.



Quelle: <https://www.brandmauer.de/blog/it-security/das-sind-die-risiken-von-shared-user-accounts>

Schutzziel: Verfügbarkeit (Availability)

Unter Verfügbarkeit versteht man, die Gewährleistung des autorisierten Zugriffs auf Informationen bei Bedarf. Die **Verfügbarkeit** eines Systems beschreibt ganz einfach die Zeit, in der das System funktioniert.

➤ Ein Aspekt der Systemzuverlässigkeit

➤
$$\text{Verfügbarkeit} = \frac{\text{Gesamtzeit} - \text{Gesamtausfallzeit}}{\text{Gesamtzeit}} * 100$$

Verfügbarkeitsklasse	Verfügbarkeit
2	99 %
3	99,9 %
4	99,99 %
5	99,999%
6	99,9999 %

Schutzziel: Verfügbarkeit (Availability)

- Denial of Service Attack vermindert bzw. eliminiert die Verfügbarkeit von Ressourcen, Diensten etc. → wirtschaftlicher Schaden

Beispiel:

Für ein System, das 24 Stunden am Tag, an 365 Jahrestagen (24×365) zur Verfügung steht (8760 Stunden), bedeutet dies:

$$\frac{8760 - 3}{8760} * 100 \approx 99,9657 \text{ (fast **VK4**)}$$

Verfügbarkeitszeiten als Eigenschaft eines Systems werden in einem **Service-Level-Agreement** zwischen dem Systembetreiber und dem Kunden festgeschrieben.

Schutzziel: Verfügbarkeit (Availability)

Beispiel:

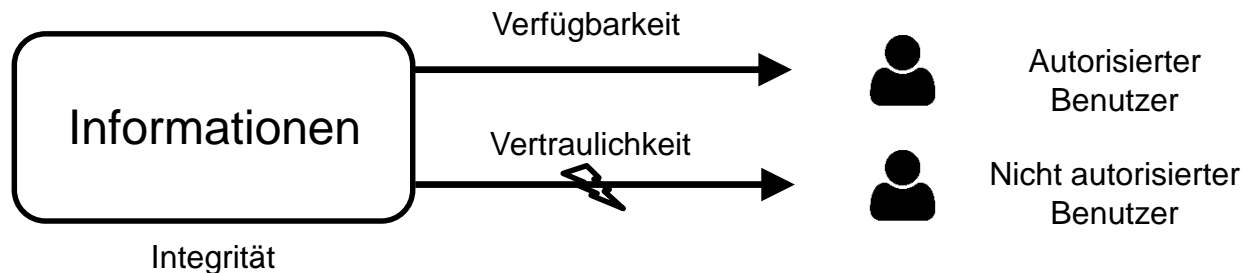
Für ein System, das 24 Stunden am Tag, an 365 Jahrestagen (24×365) zur Verfügung steht (8760 Stunden). Welche Verfügbarkeitsklasse hat das System, wenn die gesamte Ausfallzeit 20 Minuten war?

$$\frac{8760 * 60 - 20}{8760 * 60} * 100 \approx 99,99619$$

Verfügbarkeitsklasse: (fast **VK5**)

Vertraulichkeit, Integrität und Verfügbarkeit.

Integrität kann als Qualitätsmerkmal von Informationen angesehen werden, während Vertraulichkeit und Verfügbarkeit sind Merkmale der Beziehungen zwischen Informationen und einem autorisierten Benutzer (Verfügbarkeit) bzw. einem nicht autorisierten Benutzer (Vertraulichkeit).



Weitere Schutzziele

Authentizität: bezeichnet die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit eines Objekts.

- Die Sicherstellung, dass der Kommunikationspartner auch der ist, für den man ihn hält.
- Die Authentizität wird oft auch als übergeordnetes Schutzziel angesehen, da die anderen Schutzziele sonst wertlos sind, wenn man nicht sicher sein kann, ob man mit dem tatsächlichen gewünschten Kommunikationspartner kommuniziert oder mit einem unbekannten Dritten.

Weitere Schutzziele

Nichtabstreitbarkeit: es geht darum, dass eine Kommunikation im Nachhinein nicht von einer der beteiligten Instanzen gegenüber Dritten abgestritten werden kann.

- Wichtig ist dieses Ziel insbesondere für Dienstleister. Falls Verträge online abgeschlossen werden, ist die Nichtabstreitbarkeit sehr wichtig.

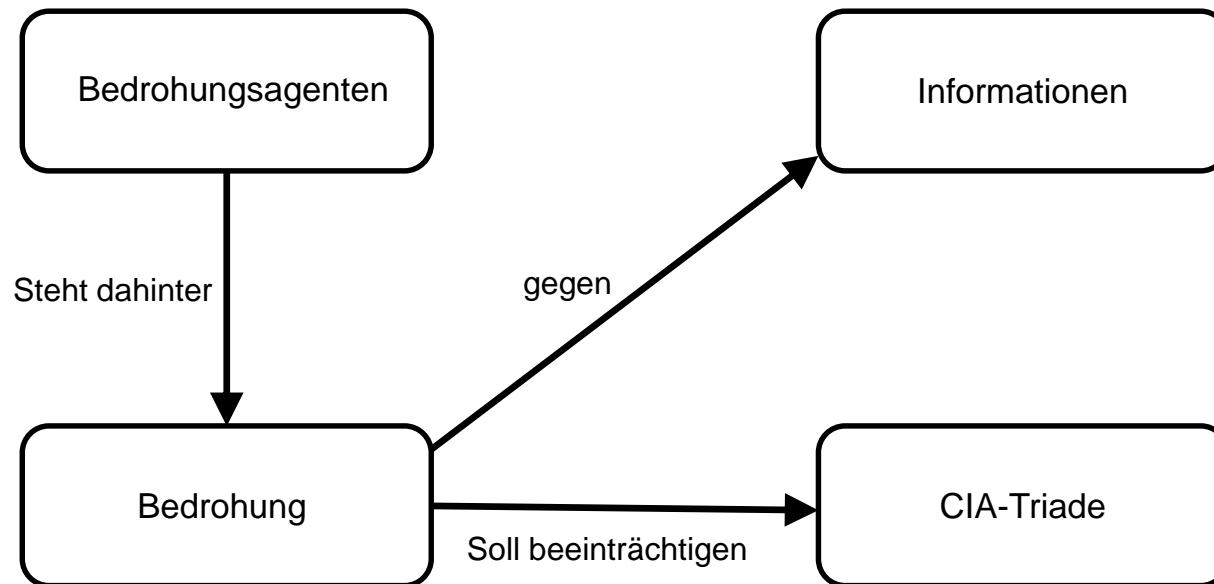
Zurechenbarkeit: eine durchgeführte Handlung kann einem Kommunikationspartner eindeutig zugeordnet werden.

- Ebenfalls für Dienstleister ist das Sicherheitsziel der Zurechenbarkeit sehr wichtig.

Bedrohungen (Threats)

- Eine Bedrohung ist eine potentielle Gefahr für Informationen oder Systeme.
- Wenn das Ziel der Informationssicherheit darin besteht, die CIA-Triade von Informationsressourcen auf einem erforderlichen Niveau zu erreichen und zu halten, ist die Bedrohung etwas, dass möglicherweise die CIA-Triade in der Zukunft beeinträchtigen kann.
- Eine Bedrohung besteht aus möglichen Handlungen oder Ereignisse, die sich negativ auf die CIA-Triade des Informationsressourcen auswirken können.
- Handlungen und Ereignisse geschehen nicht von selbst, es müssen Ursachen dahinter liegen.
- Zugrunde liegende Ursachen für Bedrohungen können als Bedrohungsagenten beschrieben werden.

Die Beziehungen zwischen dem Bedrohungsagenten, der Bedrohung, der CIA-Triade und dem Informationsvermögen



Einige Gesetzestexte

§202a StGB: „Ausspähen von Daten“

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

Einige Gesetzestexte

§202b StGB: „Abfangen von Daten“

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§202a Abs. 2) aus einer nicht öffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

Einige Gesetzestexte

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

(1) Wer eine Straftat nach §202a oder §202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§202a Abs.2) ermöglichen, oder
2. 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 Geldstrafe bestraft.

(2) §149 Abs.2 und 3 gilt entsprechend.

„Datenhehlerei“

§202d StGB, 2015

(1) Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.

(3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere

1. solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen, sowie
2. solche beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden.

Zusammenfassung §202

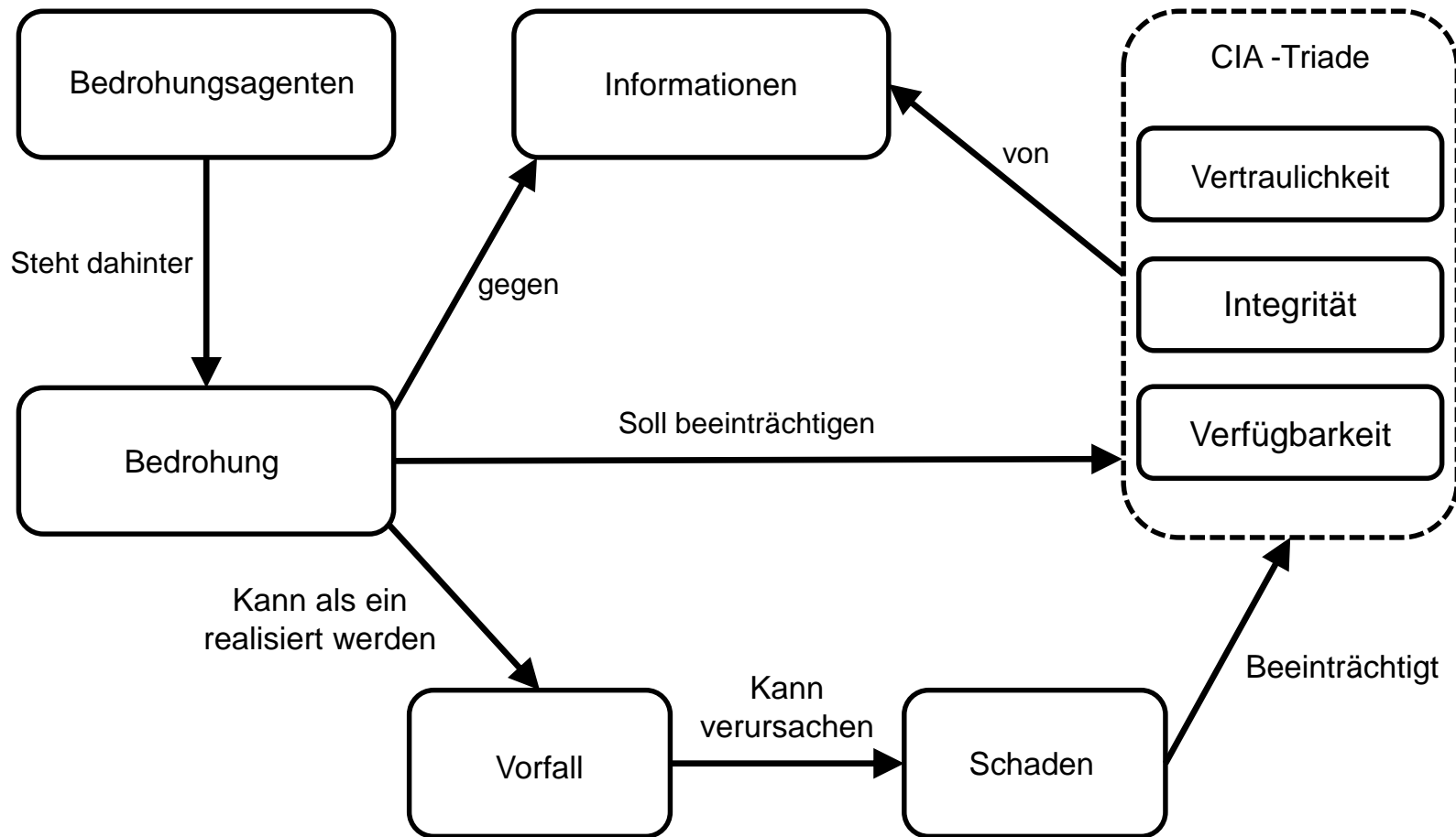
- Früher: Bloßes Eindringen in fremde Systeme nicht strafbar.
- Nun: Unbefugter Zugang unter Überwindung von Sicherheitsvorkehrungen ist strafbar!
- Hauptmangel: fehlende präzise Definition strafrechtlich relevanter Werkzeuge („Hackertools“)
- Werkzeuge nach § 202b sind offensichtlich auch viele Sicherheitstools, deren Einsatz zur Gewährleistung der Systemsicherheit unabdingbar ist?!
- „Gutartige“ Verwendung von Hackertools ist bislang nicht bestraft worden.

Referenz: Chaosradio CR 137 Der Hackerparagraph. Der §202c auf dem Prüfstand. (30.07.2008)

Vorfälle und Schäden

- Während eine Bedrohung die Annahme darstellt, dass ein unerwünschtes Ereignis in der Zukunft eintreten könnte, bezieht sich der Begriff **Vorfall** (incident) auf das tatsächliche Auftreten eines solchen Ereignisses.
- Vorfälle können zu Konsequenzen führen. Wenn eine Konsequenz die CIA-Triade unkontrolliert und negativ beeinflusst, wird sie als **Beschädigung** (damage) beschrieben.

Das gesamt Bild



Sicherheitsmechanismen

- Sicherheitsmechanismen verbessern die CIA-Triade der Informationsressourcen, d. H. Erhöhen die Informationssicherheit
- Die Begriffe Schutz, Gegenmaßnahmen, Kontrollen und Schutzmaßnahmen können als Synonyme für Sicherheitsmechanismen verwendet werden.
- Sicherheitsmechanismen können auf verschiedene Arten kategorisiert werden:
 - ihre Beziehung zur CIA-Triade
 - woraus sie bestehen - z.B. Hardware, Software und Richtlinien
 - Eine weitere Möglichkeit besteht darin, sie basierend auf ihrer Funktionalität in Bezug auf den Zeitpunkt eines Vorfalls

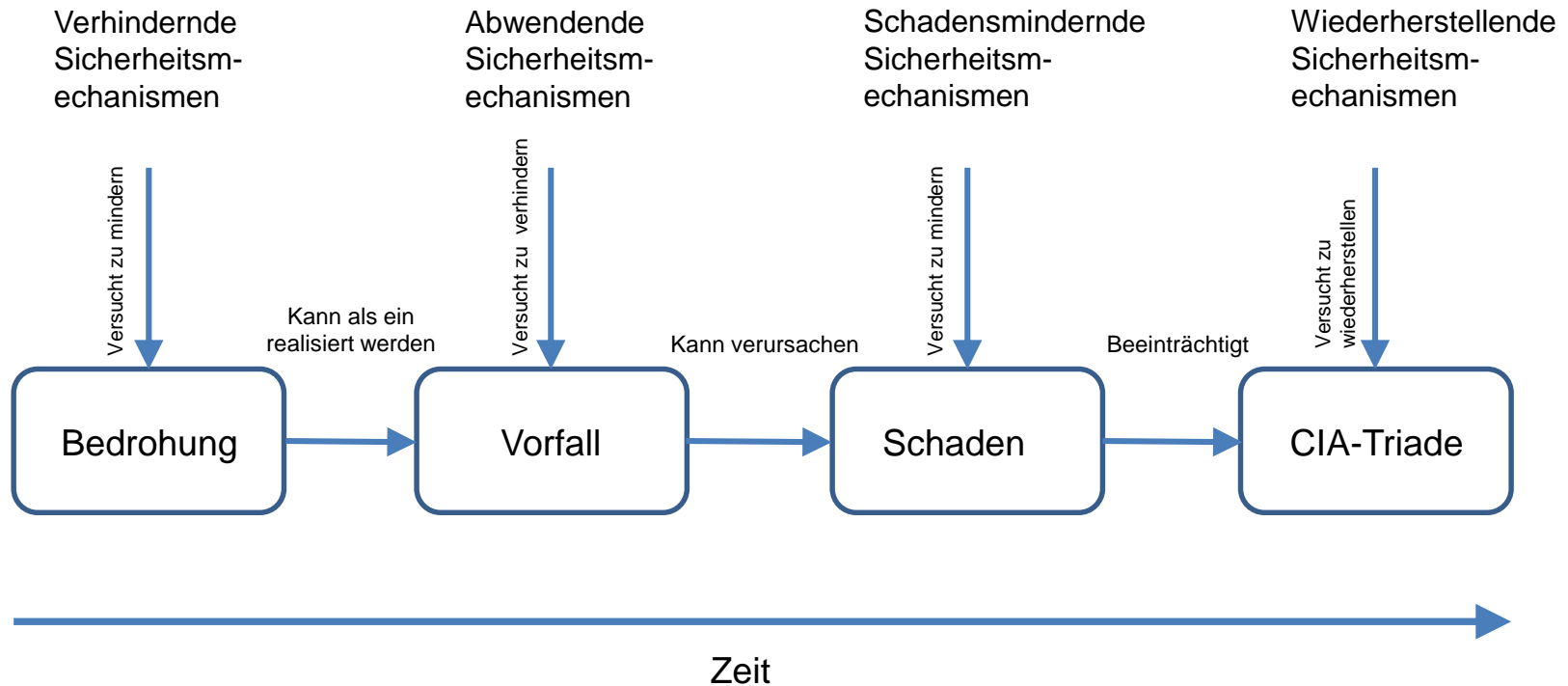
Sicherheitsmechanismen

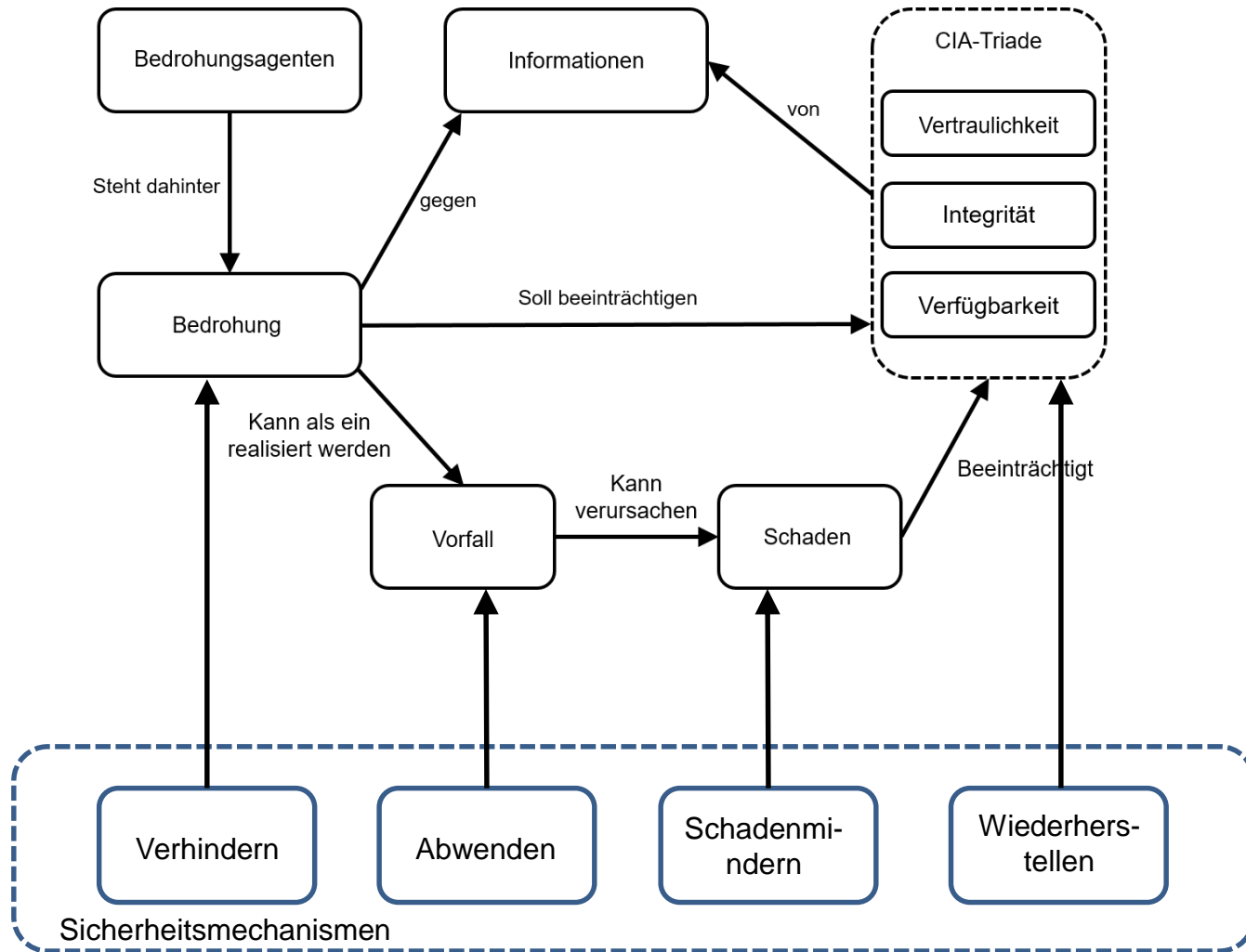
- Sicherheitsmechanismen können verhindern, abwenden oder wiederherstellen
- Verhindernde Sicherheitsmechanismen sind hoch auf die Bedrohung gerichtet. Sie beeinflussen gezielt die Bedrohungsagenten, um die Gefahr einer Bedrohung oder die Wahrscheinlichkeit, dass eine Bedrohung zum Vorfall wird zu verringern.
 - Bsp. Sicherheitsbewusstsein und Gesetze.

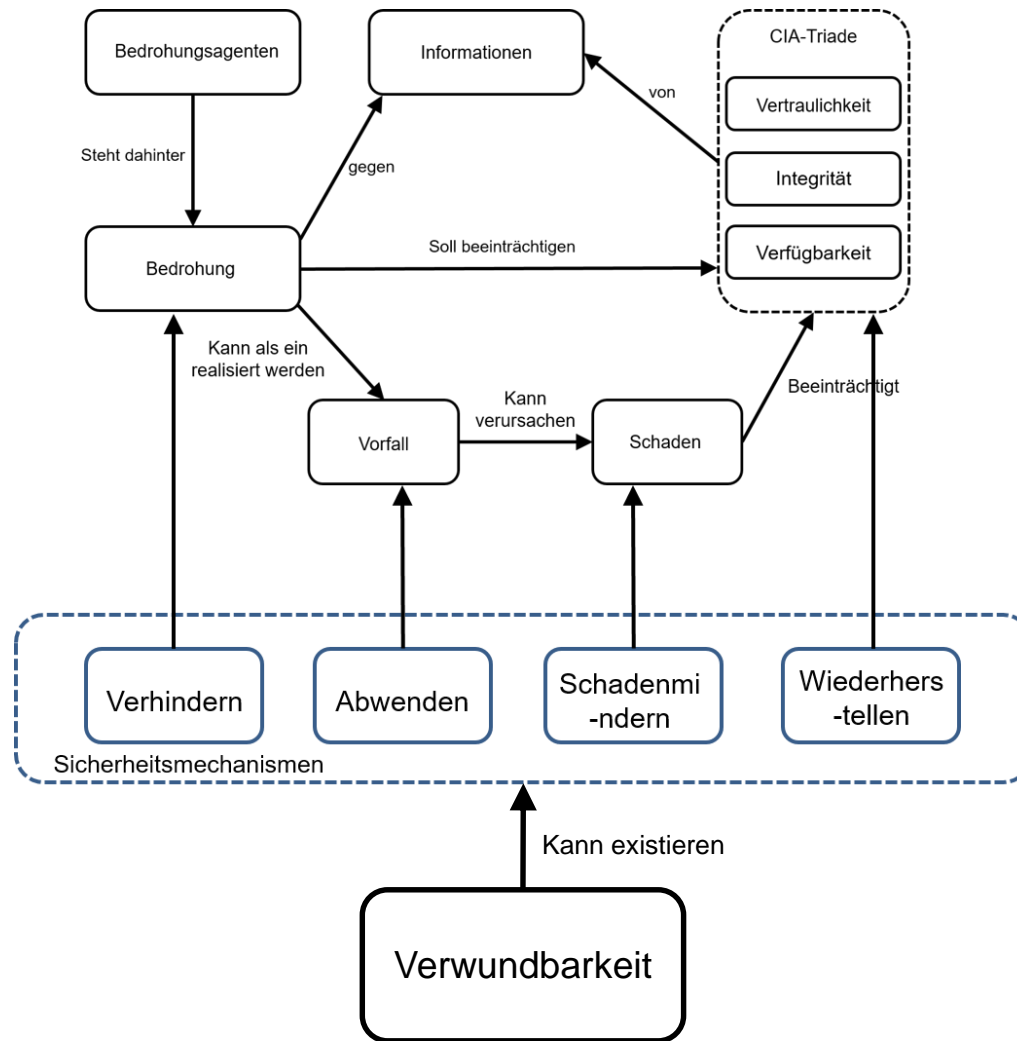
Sicherheitsmechanismen

- Abwendende Sicherheitsmechanismen sollen Vorfälle verhindern, Bsp. in Form von Firewalls oder Verschlüsselungsprogrammen
- Wiederherstellende Sicherheitsmechanismen stellen bereits beschädigte Informationen wieder her. Ein Beispiel für einen Sicherheitsmechanismus ist eine Antiviren Software, die infizierte Dateien repariert.
- In Übereinstimmung mit den vier Objekten Bedrohung, Vorfall, Schaden und der CIA-Triade fehlt ein Glied in der Kette. Es gibt Sicherheitsmechanismen, die Schäden nur reduzieren (Bsp. Feuerlöscher)

Sicherheitsmechanismen







Verwundbarkeit (Vulnerability)

- Sicherheitslücke (Verwundbarkeit) ist das Fehlen von Sicherheitsmechanismen oder Schwachstellen in bestehenden Sicherheitsmechanismen.
- In allen zuvor genannten Kategorien von Sicherheitsmechanismen kann eine Sicherheitslücke bestehen, die möglicherweise bekannt oder unbekannt ist.
- Sicherheitslücke ist eine Schwachstelle, die es einem Angreifer ermöglicht, die Informationssicherheit eines Systems zu verringern.

Risiko (Risk)

➤ Risiko ist die Einschätzung hinsichtlich des Auftretens von Vorfällen und des potenziellen Schadens, der durch Vorfälle verursacht wird.

➤ Folglich besteht der Risikobegriff aus zwei Teilen:

die **Wahrscheinlichkeit** oder die erwartete Häufigkeit, mit der ein Vorfall eintritt, und die **potenziellen Schäden**, die ein Vorfall verursachen kann. Dies kann in der folgenden Gleichung ausgedrückt werden:

$$R = L * P$$

R = Risiko

L = potenzielle Schäden

P = Wahrscheinlichkeit eines Schadens (0 → unmöglich, 1 → sicher)

Risiko (Risk)

- Auch wenn ein Vorfall zu einem schweren Schaden führt besteht kein Risiko, wenn die Wahrscheinlichkeit oder die erwartete Häufigkeit 0 ist, und umgekehrt.
- Dies bedeutet, dass $R = 0$ erfordert $L = 0$ und / oder $P = 0$.
- Wir müssen entscheiden, was wir tun können, um die Risikoauswirkung zu vermeiden oder zumindest zu verringern. Die Risikokontrolle umfasst eine Reihe von Maßnahmen zur Reduzierung oder Beseitigung des Risikos.

Risiko (Risk)

- Normalerweise möchten wir die Vor- und Nachteile verschiedener Maßnahmen abwägen, die wir ergreifen können, um die einzelnen Risiken zu bewältigen.
- Zu diesem Zweck können wir die Auswirkungen des Risikos quantifizieren, indem wir die Risikoauswirkung mit der Risikowahrscheinlichkeit multiplizieren und die Risikoexposition ermitteln.
- Beispiel
 - wenn die Wahrscheinlichkeit eines Virusangriffs 0,3 beträgt (P)
 - Die Kosten für die Bereinigung der betroffenen Dateien betragen 10.000 Euro (L)
 - Dann beträgt das Risiko (R) 3.000 Euro
 - $R = L * P$

Risiko (Risk)

- Mit einer solchen Berechnung können wir also feststellen, dass eine 100 Euro Investition in einen Virenschanner sich lohnt, da dies einen viel größeren potenziellen Verlust verhindert.
- Es ist klar, dass sich die Risikowahrscheinlichkeiten im Laufe der Zeit ändern können. Daher ist es wichtig, sie zu verfolgen und Ereignisse entsprechend zu planen.
- Viele der Systeme, die wir bauen und verwenden, können sich dramatisch auf Leben und Gesundheit auswirken, wenn sie ausfallen. Aus diesem Grund ist die **Risikoanalyse** ein wesentlicher Bestandteil der Sicherheitsplanung.

Risikoanalyse

- Ein Risiko zu analysieren bedeutet, sich mit einem möglichen Vorfall schon im Voraus auseinander zu setzen.
- Dieser Vorfall sollte realistisch (soweit uns das möglich ist) bewertet werden.
 - Was kann im schlimmsten Fall passieren?
 - Was würde das für uns oder für unser Unternehmen bedeuten?
- Eine Risikoanalyse muss einem systematischen Aufbau folgen. Die Ergebnisse müssen reproduzierbar sein. Das heißt, würde eine andere Person mit gleichem Know How dasselbe Risiko bewerten, sollte es anhand der objektiven Kriterien zum selben Ergebnis kommen.

Schadensklassen

- bezeichnet das Ausmaß eines Schadens.
- Schäden können neben direkten materiellen Auswirkungen (finanzieller Schaden, z. B. beim Kreditrisiko, Sachschaden) auch immaterielle Auswirkungen haben (z. B. Personenschäden, Zeitverluste).
- Anstatt mit Schadensklassen zu arbeiten können wir auch direkt mit finanziellen Werten arbeiten. Das heißt, Wir beziffern jeden potentiellen Schaden mit einer Summe **X** in Euro. Das macht es natürlich für unsere mathematische Formel einfach.

Schadensklassen

- In der Praxis ist dies aber schwierig (Bsp. Reputationsschaden)
- Deswegen bilden wir Schadensklassen (Bsp. gering, mittel, hoch, sehr hoch)
- Die Ergebnisse müssen reproduzierbar sein, deswegen zu den Schadensklassen noch eine Hilfestellung bzw. Beschreibung geben

Schadensklasse	Finanzieller Schaden
gering	< 5.000 €
mittel	> 5.000 € und < 20.000 €
hoch	> 20.000 € und < 50.000 €
sehr hoch	> 50.000 €

Eintrittswahrscheinlichkeit

- Bezeichnet den statistischen Erwartungswert oder die geschätzte Wahrscheinlichkeit für das Eintreten eines bestimmten Ereignisses in einem bestimmten Zeitraum in der Zukunft.
- Das gleiche wie Schadensklassen nur dieses Mal für die Eintrittswahrscheinlichkeit (Bsp. gering, mittel, hoch, sehr hoch)
- Die meisten Risiken können nur grob hinsichtlich ihrer Eintrittswahrscheinlichkeit und ihres möglichen Schadens geschätzt werden.

Risikomatrix

- Mit der Risikomatrix legen wir fest, welche Risiken für uns akzeptabel sind und für welche Risiken wir unbedingt Gegenmaßnahmen einplanen müssen
- Die Wahrscheinlichkeit des Auftretens eines Schadens wird gegenüber dessen Auswirkung tabellarisch ins Verhältnis gesetzt.
- Da wir den größten Schaden mit „sehr hoch“ und die größte Eintrittswahrscheinlichkeit mit „sehr hoch“ beziffert haben, ist unser maximales Risiko:

*Maximales Risiko = Sehr hoher Schaden * sehr hohe Eintrittswahrscheinlichkeit*

Risikomatrix

Klasse		Eintrittswahrscheinlichkeit	Schaden
	4 – sehr hoch	> 30 %	> 50.000 €
	3 - hoch	20 % - 30 %	> 20.000 € und < 50.000 €
	2 - mittel	10 % - 20 %	> 5.000 € und < 20.000 €
	1 - gering	0 % - 10 %	< 5.000 €

Risikomatrix (Beispiel)

Eintrittswahrscheinlichkeit	4 – sehr hoch	4	8	12	16
	3 - hoch	3	6	9	12
	2 - mittel	2	4	6	8
	1 - gering	1	2	3	4
		1 - gering	2 - mittel	3 - hoch	4 – sehr hoch
	Schaden				

Risikomatrix (Beispiel)

- Da wir ja das Risiko auch rechnerisch ermitteln möchten, ist es sinnvoll, den Klassen Werte zu hinterlegen
- In unserem Beispiel hat das maximale Risiko den Wert 16 und das minimale Risiko den Wert 1
- *Maximales Risiko = Sehr hoher Schaden * sehr hohe Eintrittswahrscheinlichkeit*
- *Maximales Risiko = 4 * 4*

Risikoakzeptanzniveau

- Risikomatrix definiert, welche Kombinationen aus Eintrittswahrscheinlichkeit und Schaden akzeptabel oder inakzeptabel sind oder aber näher untersucht werden müssen
- Anhand der oben dargestellten Risikomatrix kann das Unternehmen nun zum Beispiel festlegen, dass alle Risiken mit einem Ergebniswert von < 4 akzeptabel sind
- Geringe Risiken (in unserem Beispiel die mit einem Wert < 4) akzeptieren wir automatisch ohne nähere Untersuchung .

Risikomatrix (Beispiel)

Eintrittswahrscheinlichkeit	4 – sehr hoch	4	8	12	16
	3 - hoch	3	6	9	12
	2 - mittel	2	4	6	8
	1 - gering	1	2	3	4
		1 - gering	2 - mittel	3 - hoch	4 – sehr hoch
	Schaden				

Risikoakzeptanzniveau

- Mittlere Risiken (mit Werten zwischen 4 und 8 im Beispiel) müssen näher untersucht werden
- Mittlere Risiken werden individuell akzeptiert. Wer das Recht hat, diese Risiken zu akzeptieren, muss ebenfalls festgelegt werden (Projektleiter oder Geschäftsleitung)

Risikomatrix (Beispiel)

Eintrittswahrscheinlichkeit	4 – sehr hoch	4	8	12	16
	3 - hoch	3	6	9	12
	2 - mittel	2	4	6	8
	1 - gering	1	2	3	4
		1 - gering	2 - mittel	3 - hoch	4 – sehr hoch
	Schaden				

Risikomatrix (Beispiel)

Eintrittswahrscheinlichkeit	4 – sehr hoch	4	8	12	16
	3 - hoch	3	6	9	12
	2 - mittel	2	4	6	8
	1 - gering	1	2	3	4
		1 - gering	2 - mittel	3 - hoch	4 – sehr hoch
	Schaden				

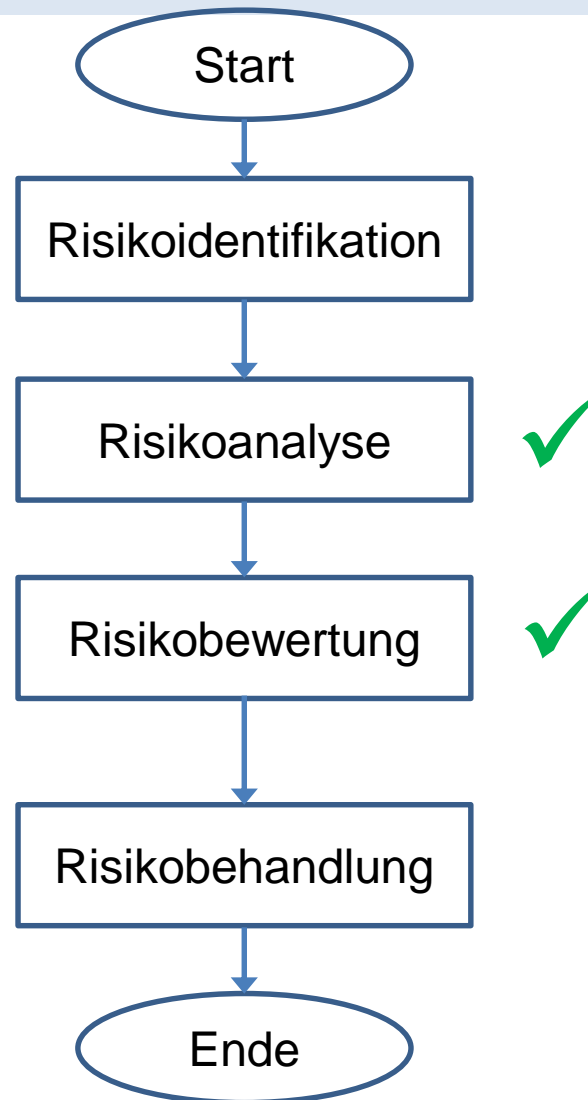
- Hohe Risiken (mit Werten größer als 8 im Beispiel) bedürfen grundsätzlich immer einer Risikobehandlung

Prozess Risikoanalyse

- Eine sinnvolle Risikoanalyse ist normalerweise in ein Risikomanagementsystem eingebunden
- Risikoanalyse ist nur ein Teilbereich aus dem kompletten Risikomanagement-Prozess, wie der Prozessablauf nach **ISO 31000** zeigt.

Risikomanagementsystem (RMS): Risikomanagement ist die Tätigkeit des Umgangs mit Risiken. Dies umfasst sämtliche Maßnahmen zur Erkennung, Analyse, Bewertung, Überwachung, Steuerung und Kontrolle von Risiken. *(Wikipedia)*

Prozessablauf



Risikoidentifikation

- Die Risikoidentifikation dient zur Ermittlung aller auf eine Organisation einwirkenden Risiken. Die Risiken werden systematisch identifiziert und mit ihren Ereignissen, Ursachen und Einflüssen auf das Projekt dokumentiert. Sie bildet die Basis für die anschließende Risikoanalyse im Prozess des Risikomanagements.
- Vorteile
 - Die systematische Vorgehensweise gewährleistet, dass möglichst wenige Risiken übersehen werden und somit frühzeitig Maßnahmen geplant werden können
 - Die vollständige Dokumentation der Risiken erleichtert die anschließende Risikoanalyse

Risikoidentifikation

➤ Nachteile

- Die Risikoliste ist ohne anschließende Risikoanalyse wenig aussagefähig und kann dadurch zu Missverständnissen in der Kommunikation führen
- Der Einsatz der Risikoidentifikation garantiert keine 100%ige Vollständigkeit, es können dennoch überraschende Risiken eintreten
- Die Durchführung der Risikoidentifikation und die Existenz der Risikoliste kann zu einer subjektiven "**Scheinsicherheit**" führen, aufgrund derer die ständige Überprüfung der Risikobelastung vernachlässigt wird

Risikoidentifikation

- Ergebnis
 - Liste mit Beschreibungen aller identifizierten Projektrisiken (Risikoereignis, Ursache(n), Einflüsse auf Projekt)
 - Dokumentation der Annahmen bzw. Szenarien, die erarbeitet wurden
- Der Risikoeigner sollte die Risiken für seinen Bereich kennen. Das kann der Abteilungsleiter sein, aber auch der Projektleiter
- Im Rahmen der Risikoanalyse geht es bei der Risikoidentifikation darum, potentielle Vorfälle zu benennen. Hier wird noch nichts bewertet → **Was könnte passieren?**

Beispiel

Szenario: Der für die Lohnabrechnung zuständige Mitarbeiter, fällt für mehrere Wochen (bis zu 6 Wochen), aus.

Ist das ein Risiko?

Nein!

- Wir haben hier lediglich einen Vorfall beschrieben
- Zum Risiko wird dieser erst, wenn sich daraus eine Konsequenz ergibt, die für das Unternehmen zu einem Schaden führt

Beispiel

Beschreibung des Schadens („führt zu“ oder „kann verursachen“):
Lohnabrechnung für das gesamte Unternehmen kann nicht mehr erstellt werden. Löhne können nicht mehr bezahlt werden

- Erst jetzt wird der Vorfall mit einem potentiellen Schadensszenario verknüpft

Ursache / Grund für das Eintreten des Szenarios (=Schwachstelle):

- Was ist denn nun die Ursache dafür, dass der Ausfall des Mitarbeiters zum Ausfall der Lohnabrechnung führt?
- Beim zuständigen Mitarbeiter handelt es sich um eine Single-Source, also um nur eine einzige Person, die das entsprechende Know How hat

Beispiel

Szenario: Der für die Lohnabrechnung zuständige Mitarbeiter, fällt für mehrere Wochen (bis zu 6 Wochen), aus.

Eintrittswahrscheinlichkeit = 3, Schaden = 3

Eintrittswahrscheinlichkeit	4 – sehr hoch	4	8	12	16
	3 - hoch	3	6	9	12
	2 - mittel	2	4	6	8
	1 - gering	1	2	3	4
		1 - gering	2 - mittel	3 - hoch	4 – sehr hoch
Schaden					

Prozessablauf



Risikobehandlung

Dieser Schritt ist nur nötig, wenn das Risiko nicht akzeptiert wird. Eine Risikobehandlung kann unterschiedlich ausfallen:

- **Minimieren** des Risikos, indem Maßnahmen umgesetzt werden, die entweder den Schaden oder die Eintrittswahrscheinlichkeit verringern
- **Eliminieren** des Risikos, indem man das Eintreten des Vorfalls komplett vermeidet
- **Übertragen** des Risikos an einen Dritten, zum Beispiel eine Versicherung
- **Akzeptieren** und **regelmäßige Überwachung** des Risikos

Risikobehandlung

Frage: Was ist eine mögliche **Zusatzmaßnahme** in unserem vorherigen Beispiel, um das Risiko zu behandeln?

- Eine weitere Person mit der Lohnbuchhaltung vertraut zu machen
- Damit minimiert sich der Schaden nach Umsetzung der Maßnahme und fällt nun in die Klasse „gering“
- Die Eintrittswahrscheinlichkeit, dass ein Mitarbeiter mehrere Wochen ausfällt, bleibt allerdings gleich
- Damit haben wir mit geringem Schaden und hoher Wahrscheinlichkeit ein akzeptiertes Risiko

Beispiel

Szenario: Der für die Lohnabrechnung zuständige Mitarbeiter, fällt für mehrere Wochen (bis zu 6 Wochen), aus.

Eintrittswahrscheinlichkeit = 3, Schaden = 1

Eintrittswahrscheinlichkeit	4 – sehr hoch	4	8	12	16
	3 - hoch	3	6	9	12
	2 - mittel	2	4	6	8
	1 - gering	1	2	3	4
		1 - gering	2 - mittel	3 - hoch	4 – sehr hoch
Schaden					

Beispiel

Szenario: Der für die Lohnabrechnung zuständige Mitarbeiter, fällt für mehrere Wochen (bis zu 6 Wochen), aus.

Eintrittswahrscheinlichkeit = 3, Schaden = 1

Eintrittswahrscheinlichkeit	4 – sehr hoch	4	8	12	16
	3 - hoch	3	6	9	12
	2 - mittel	2	4	6	8
	1 - gering	1	2	3	4
		1 - gering	2 - mittel	3 - hoch	4 – sehr hoch
Schaden					

Prozessablauf

