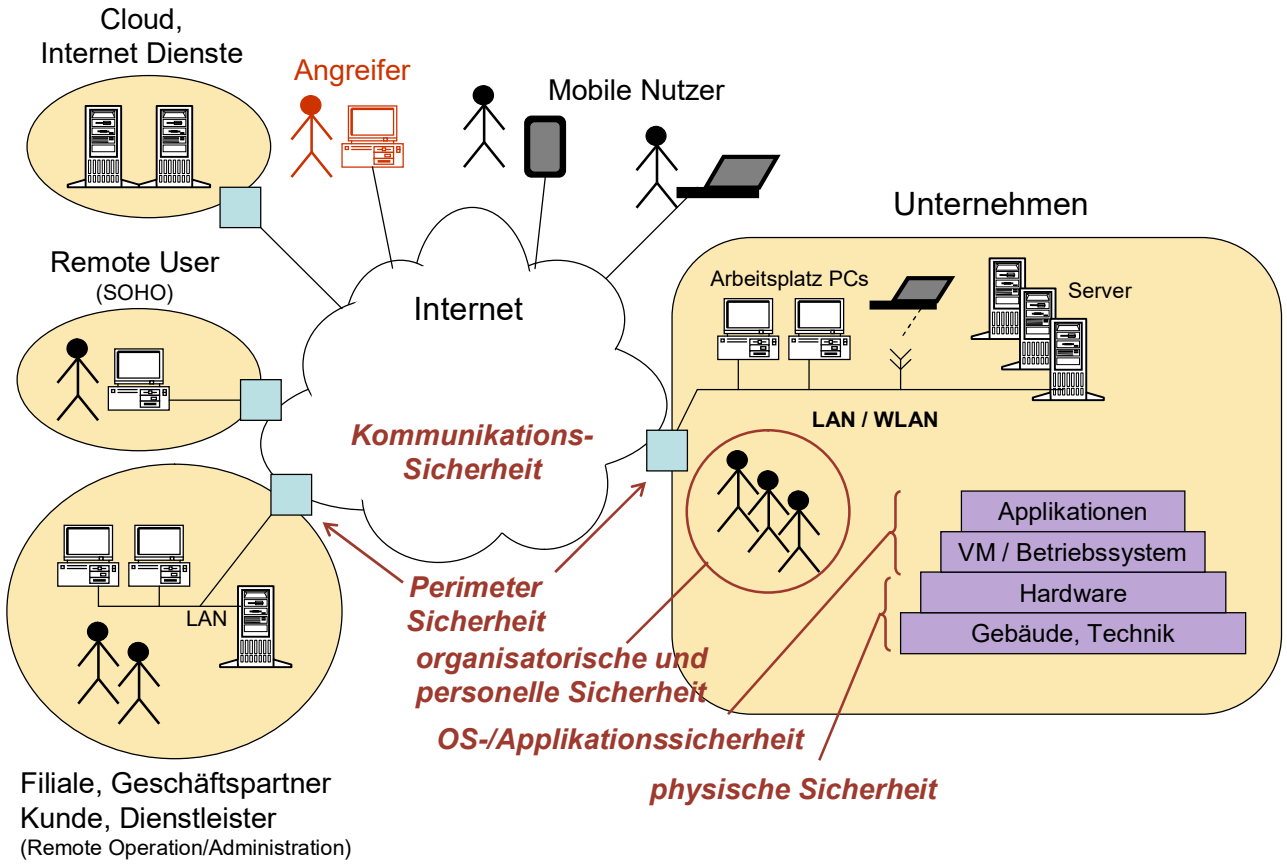
Grundbegriffe und Zusammenhänge

Inhalt

- Bereiche der IT-Sicherheit
- Grundwerte der IT-Sicherheit
- Safety und Security
- Sicherheit und Vertrauen
- Schutzbedarf, Schwachstellen, Bedrohungen
- Risikoanalyse, Sicherheitsmaßnahmen, Restrisiko
- Dreiecksbeziehung: IT-Sicherheit, Kosten, Funktionalität
- Kettenregel

Bereiche der IT-Sicherheit



Physische Sicherheit

- Gebäudesicherheit, Strom, Klima, Zutrittsschutz
- Hardwaresicherheit, Racks, Netzverteiler

Operating System (OS) Sicherheit

- Zugangschutz, Zugriffsschutz, Berechtigungskonzepte
- Hardwaresicherheit, Racks, Netzverteile

Applikationssicherheit

- Sicherheit in der Software-Entwicklung: Secure Coding
- Sicherheit von Web-Applikationen

Kommunikationssicherheit

- Verschlüsselung, Authentisierung, Integritätsschutz
- VPNs, IPSec, SSL/TLS

Perimetersicherheit, Netzsicherheit

- Sicherheit am Übergang zwischen verschiedenen Netzen
- Firewalls, Firewallsysteme, Intrusion Detection

Endpoint-Security, Network Access Control

- Prüfung der Sicherheitsausstattung von (mobilen) Clients
- Prüfung der Aktualität der Software, Policy-Konformität, etc.

Organisatorische und personelle Sicherheit

- Konzepte, Richtlinien, Betriebshandbücher
- Personalauswahl und –weiterbildung, Vertreterregelungen
- Service Level Agreements

IoT- und ICS-Security

- ICS-Security (Industrial Control Systems), IT Einsatz in der Industrie, Industrie 4.0
- IoT Internet of things: Am Internet angebundene Geräte wie Smart TV, SmartHome Geräte, ggf. Herzschrittmacher, Insulinpumpen,…

Was soll geschützt werden: Werte (assets)

Beispiele zu schützender Werte

- Vertrauliche Unternehmensdaten
- Rechner, Rechnergesteuerte Anlagen
- Image und Reputation des Unternehmens
- Kundendaten
- Auf oberster Ebene: Geschäftsprozesse

Asset-Management im Unternehmen:

- Identifikation und Bewertung/Einordnung von Assets

Begriffe und Abkürzungen:

- IT-Sicherheit (IT = Informationstechnik): Oberbegriff für Rechenanlagen, Endgeräte, Server und zugehörige Kommunikationstechnik (Netze, Router, Switches, etc.)
- Cyber-Security: Sicherheit im „Cyberraum", der „Internet-Welt"
- Teils noch genutzt: IuK- / IKT- Sicherheit: Sicherheit in der Informations- und Kommunikationstechnik (engl. ICT = Info.+Communication Technology)
- Informationssicherheit: Umfasst auch Sicherheit von Informationen, die NICHT IT-basiert vorliegen (z.B. gedruckte Dokumente)
- Datensicherheit: Von Juristen häufig verwendetes Synonym für Informationssicherheit. (Daten repräsentieren Informationen)
- Datenschutz (engl. *Privacy*): Schutz personenbezogener Daten, gesetzliche Regelungen

Warum IT-Sicherheit? => PPT

IT ist für die meisten Organisationen eine kritische Infrastruktur geworden.

- Ohne IT ist es i.d.R. nicht mehr möglich, die Geschäftsabläufe aufrecht zu erhalten

Beispiele anderer kritischer Infrastrukturen

- Gesellschaft / Wirtschaft: Infrastruktur der Energie- und Stromversorgung
- Gesellschaft: Infrastruktur im Gesundheitswesen: Krankenhäuser, Ärzte, etc.
- Wirtschaft (Gesellschaft): Infrastruktur der Telekommunikation
- Wirtschaft: Internet
- Staat: Infrastrukturen für Ordnung (Legislative und Exekutive, z.B. Polizei)
- Staat: Infrastruktur zum Schutz des Staates: Diplomatie, Militärwesen, Geheimdienst

1. Definition IT-Sicherheit

- IT-Sicherheit ist der Zustand, bei dem
  - Verfügbarkeit
  - Integrität und
  - Vertraulichkeit

  beim Einsatz von IT in angemessener Weise geschützt sind.

- Verfügbarkeit, Integrität, Vertraulichkeit sind die *Grundwerte* der IT-Sicherheit
- engl: CIA = Confidentiality, Integrity and Availability
- Häufig werden zusätzlich auch
  - Authentizität und/oder
  - Verbindlichkeit

  mit zu den Grundwerten gezählt.

Definitionen der Grundwerte der IT-Sicherheit

Definition Verfügbarkeit (availibility)

Verfügbarkeit ist der Zustand, in dem die Nutzbarkeit von Informationen und IuK-Systemen gegeben ist.

Definition Vertraulichkeit (confidentiality)

Vertraulichkeit ist der Zustand, bei dem Daten gegen unzulässige Kenntnisnahme und unbefugten Zugriff geschützt sind.

Authentizität = „Echtheit“, „Ungefälschtheit“

- Authentizität bezieht sich in der IT-Sicherheit typischerweise auf
  - auf den Zugang zu IT-Systemen,
  - auf das Senden/Empfangen von Daten oder
  - auf das Erstellen oder Verarbeiten von Daten.
- Authentizität des Zugreifenden
- Sender-/Empfängerauthentizität, Authentizität der Kommunikationspartner
- Authentizität von Daten und Systemen wird als Integrität bezeichnet

Definition Authentizität (authenticity):

Authentizität ist der Zustand, bei der der Ursprung von Informationen oder der Ursprung bei Zugängen zu IT-Systemen oder Zugriffen auf Daten sichergestellt ist.

Definition Integrität (integrity):

Integrität ist der Zustand, der unbefugte oder unzulässige Veränderungen an IT-Systemen oder an Daten/Informationen ausschließt.

Der Schutz der Integrität reduziert sich häufig in der IT auf die Möglichkeit zur Erkennung unzulässiger oder unbefugter Veränderungen.

Definition Verbindlichkeit (Nicht-Abstreitbarkeit, nonrepudiation)

Verbindlichkeit ist der Zustand, in den Aktionen einer Instanz eindeutig zugeordnet und nicht geleugnet werden können. (Beweisbarkeit gegenüber Dritten)

Voraussetzung für Verbindlichkeit:

- Merkmal der Verbindlichkeit ist durch Dritte nicht oder nur sehr schwer fälschbar.

Verbindung kann hergestellt werden z. B. durch:

- Vertrag
  - Verbindung zwischen Personen und der getroffenen Absprache, Nachweis durch Unterschrift oder Zeugen
- Unterschrift
  - Verbindung zwischen Willenserklärung und dem Unterzeichner
- Geld
  - Verbindlicher Nachweis eines abstrakten „Geldwerts“ (Subjekt der Verbindung ist anonym)

Weitere Beispiele

- Verbindlichkeit eines Wildunfalls: Blutspuren, Fellrückstände am Auto
- Bei Straftaten: Herstellen von Verbindung zwischen Tat und Täter durch Suche von Beweisen: Bsp. DNA-Spuren

Im Rahmen der IT betrifft die Verbindlichkeit insbesondere

- Nachweis der Urheberschaft von Daten
  - Bsp.: Transaktionen im Homebanking
- Nachvollziehbarkeit des Verarbeitens/Änderns von Daten
  - Administrationszugriffe auf kritische Server

Safety und Security

- Für den Begriff Sicherheit wird im Englischen unterschieden zwischen Safety und Security
- Safety
  - Sicherheit hinsichtlich passiver, fahrlässiger Bedrohungen,
  - häufig auch als „Betriebssicherheit“ übersetzt
- Security
  - Sicherheit insbesondere hinsichtlich aktiver, vorsätzlicher Bedrohungen
- Bsp. Safety: Not-Aus Schalter an Maschinen, Sicherheitsgurt im Auto
- Bsp. Security: Firewalls, Passwortschutz
- Mechanismen zur Safety dienen häufig auch der Security
- Safe aber nicht secure: CRC, fehlerkorrigierende Codes

Sicherheit und Vertrauen

Sicherheit im täglichen Leben:

- Sicherheit bei Geldgeschäften / im Haushalt
- Sicherheit bei Kunden – Lieferanten - Beziehungen
- Sicherheit im Krankheitsfall: Ärzte
  - gegensätzliche Interessen: Geld verdienen, Patient heilen, Eid des Hypokrates
  - Win-Win-Situation erzeugen. Wie?

Jeweils: Schäden / Gefährdungen / Risiken, Maßnahmen (technisch, organisatorisch)
Sanktionierung, Reaktion bei Vorfällen (Incident Handling / Incident Response)

Nachbaraufgabe: Wie wird *Sicherheit im Straßenverkehr* erreicht?

- Was ist das übergeordnete Ziel?
- Nennen Sie mögliche Gefährdungen und Schäden:

- Suchen Sie Sicherheitsmaßnahmen unterschiedlicher Art.
  - Technische Maßnahmen
  - Organisatorische Maßnahmen
  - Personelle Maßnahmen

- Wie erfolgt das Incident Handling (Reaktion auf Eintritt von Gefährdungen)?
- Wieso ist eine Sanktionierung wichtig?
- Gibt es ein Notfall-Management?

Subjektive Einschätzung von Risiken ist häufig falsch

- Flugverkehr: Risiko gering, Eintrittswahrscheinlichkeit minimal, Schadenshöhe immens
- Autoverkehr: Risiko hoch, Eintrittswahrscheinlichkeit hoch, mittlere Schadenshöhe gering (Anteil tödlicher Verkehrsunfälle gering)

Gründe: Flugverkehr: Hohes Vertrauen gegenüber Dritten erforderlich,
mittlere Schadenshöhe immens

Vertrauen ist ein wesentlicher Bestandteil der Sicherheit

- „Sicherheit ist Manifestation des Vertrauens“ durch
  - Erfahrungen (persönliches Vertrauen)
  - Kennzeichen (z. B. Polizeiuniform, Enkeltrick)
  - Regeln (z. B. Gesetze)

Schutzbedarf

Der Schutzbedarf ist ein Maß für den *Schaden*, der aus der Verletzung von Grundwerten resultiert.

- Insbesondere ist der Schutzbedarf unabhängig von Bedrohungen!

Schutzbedarf von Geschäftsprozessen

- vererbt sich auf die IT, welche die Geschäftsprozesse unterstützt
- vererbt sich auf die verarbeiteten/gespeicherten Informationen

innerhalb der IT zunächst auf die Applikationen, dann auf die Betriebssysteme, Kommunikationssysteme, etc.

Typische Skalierung des Schadens:

- vernachlässigbar, gering, mittel, hoch, sehr hoch, katastrophal
- oftmals Hinterlegung mit Geldwerten (exponentiell)

<100 €, 100-1000€, 1000-10.000€, 10.000-100.000€, 100.000€ -1Mio €, > 1Mio €

Beispiele möglicher Schäden

- Beeinträchtigung von Produkten / Dienstleistungen
  - Ausfall von Produktionsanlagen, von IT-Funktionen und/oder Diensten
  - Datenverlust
- Beeinträchtigung der Marktstellung
  - Ausspähung von Preisinformationen / Angeboten durch die Konkurrenz
  - Ausspähung von Entwicklungsinformationen durch die Konkurrenz

- Verstoß gegen gesetzliche oder sonstige Auflagen (Compliance)
  - Datenschutz
- Imagebeeinträchtigung des Unternehmens
  - Negative Schlagzeilen durch bekannt werdende Vorfälle
  - „Shitstorm“
  - Vertrauensverlust von Kunden

Schäden und Folgeschäden

- Beispiel: Hacker legt E-Business Angebot einer Firma lahm, z. B. durch DoS-Angriff.
- Direkte Schäden
  - Umsatzverlust durch Downtime
  - Kosten für sicheren Wiederanlauf (Experten, Software, etc.)
- Folgeschäden:
  - Image-/Rufschädigung
  - Reduzierung des Kundenvertrauens
  - Abwanderung von Kunden
- Folgeschäden sind häufig erheblicher als die direkten Schäden

Wodurch werden Grundwerte der IT-Sicherheit verletzt?

- Bedrohungen (threats) und Gefährdungen (Begriffe werden synonym verwendet)

Beispiele:

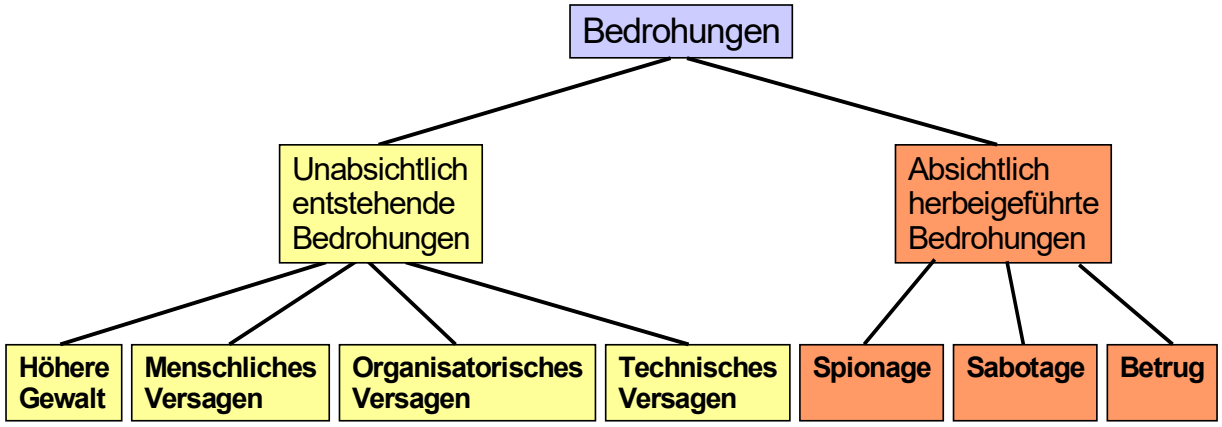
- Integrität: Eindringen von Hackern in interne Systeme
- Verfügbarkeit: Systemausfall durch Sprinkleranlage infolge eines Brands
- Vertraulichkeit/Authentizität: Ermittlung von Zugangsinformationen durch Phishing

Dass Bedrohungen wirksam werden können, wird häufig erst dadurch ermöglicht, dass die bedrohten Ziele Schwachstellen (weakness, vulnerabilities) aufweisen.

- Typisch: Fehlerbehaftete Software, mangelhafte Konfiguration

Anmerkung: Nicht jede Schwachstelle ist direkt eine Verletzlichkeit. Im Rahmen der IT-Sicherheit interessieren jedoch nur Schwachstellen, die Verletzlichkeiten darstellen. Daher werden die Begriffe hier synonym verwendet.

Beispielklassifizierung von Bedrohungen



Begriff des Risikos

- Beim Eintreten von Bedrohungen entstehen Schäden (-> Schutzbedarf).
- Die mittlere Schadenshöhe hängt dabei davon ab, wie wahrscheinlich es ist, ob eine Bedrohung eintritt.
- Das Risiko ist definiert als diese mittlere Schadenshöhe.
- Das Risiko einer Bedrohung ergibt sich als Produkt der Eintrittswahrscheinlichkeit und der Schadenswirkung der Bedrohung.

Risikomanagement

Das Risikomanagement beschäftigt sich umfassend mit Geschäftsrisiken

- Vertragsrisiken
- Finanzrisiken
- Projektrisiken
- IT-Risiken

Die IT-Sicherheit beschränkt sich auf IT-Risiken

Risikoanalyse

Zweck und Ziele:

- Identifizierung der Unternehmenswerte (assets) und ihrer finanziellen Werte (value)
- Identifizierung der Bedrohungen (threats)
- Beurteilung der Auswirkungen der Bedrohungen (impact) und der sich ergebenden Risiken
- (Festlegung von Gegenmaßnahmen (countermeasures, controls) abhängig von Risiken)

Vorgehensweisen: Qualitative Analyse und Quantitative Analyse

Qualitative Analyse

- Entwicklung von Risikoszenarien
- Durcharbeiten der Szenarien und qualitative Bewertung der Risiken im Rahmen eines internen Expertenworkshops („Bauchgefühl“)
- Ordnen der Risikoszenarien in eine Rangfolge nach Ausmaß und Eintrittswahrscheinlichkeit
- (Festlegung von Gegenmaßnahmen priorisiert nach Risiken)

Quantitative Analyse

- Schutzbedarfsanalyse:
  - Welche Unternehmenswerte sind zu schützen und welcher Schaden kann entstehen?
- Identifizierung von Bedrohungen im Bezug auf den Ist-Zustand
- Abschätzung der Schäden und Eintrittswahrscheinlichkeiten für die Bedrohungen
- (Festlegung von Gegenmaßnahmen in Abhängigkeit der ermittelten Risiken)

Typische Situation:

- Aufbau eines neuen Systems im Unternehmen (z. B. E-Commerce)
- Viele Maßnahmen bereits gegeben
  - Rechenzentrum, Firewall, etc.
- Ermittlung, welche neuen Risiken entstehen bzw. welche bisherigen Risiken sich ändern
  - Eintrittswahrscheinlichkeit kann steigen (z. B. Attraktives Angriffsziel, persönliche Vorteile bei erfolgreichem Angriff, Internet-Zugang)
  - Schadensmaß kann steigen (z. B. wegen enger Kopplung an interne Datenbanken)
- In größeren Unternehmen ist ein Vorgehen zur Risikoanalyse i.d.R. auf Basis eines Bedrohungskatalogs bereits vorgegeben.

Relevante Kenngrößen

SLE = Single Loss Expectancy = Erwartungswert eines Einzelschadens

= (Bedrohungsfaktor) * (Wert) = exposure Factor * asset

ALE = Annual Loss Expectancy = Erwartungswert des jährlichen Schadens

= SLE * jährliche Häufigkeit (annualized rate of occurrence (ARO))

Eintrittswahrscheinlichkeiten und Schadenshöhen sind häufig nur schwer festzulegen. Wichtig sind sinnvolle Abschätzungen.

Möglichkeiten des Umgangs mit Risiken

- Risikoreduzierung: Implementierung von Gegenmaßnahmen
- Risikotransfer: Abschluss einer Versicherung
- Risikoakzeptanz: Hinnahme des Risikos
- Ignoranz: Ignorieren des Risikos

Sicherheitsmaßnahmen (präventiv / reaktiv)

Sicherheitsmaßnahmen wirken Risiken entgegen. Sie reduzieren entweder die Eintrittswahrscheinlichkeit (präventive Maßnahmen) der Bedrohung oder ihr Schadenspotenzial (reaktive Maßnahmen).

Das Risiko wird durch Sicherheitsmaßnahmen i.d.R. nicht auf Null reduziert.

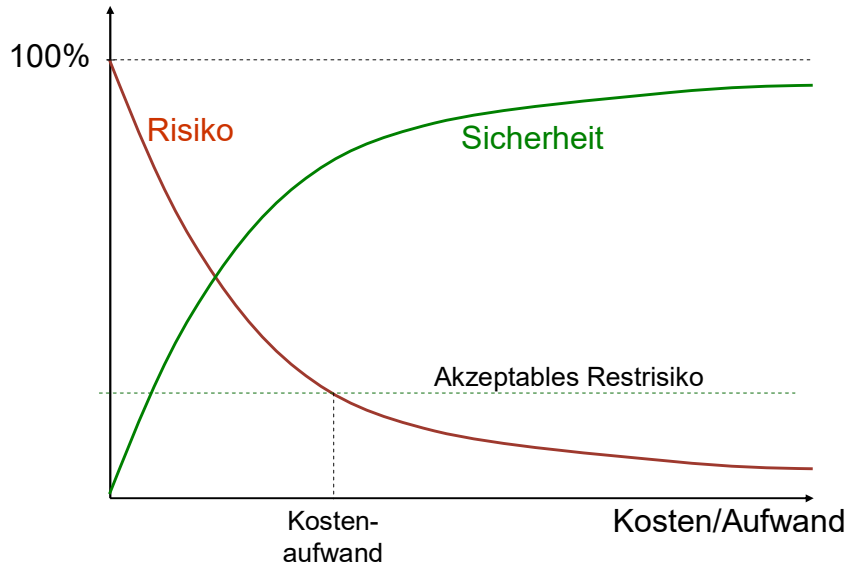
Ziel des Einsatzes von Sicherheitsmaßnahmen ist es, dass Risiko auf ein tragbares Restrisiko zu reduzieren.

Definition Restrisiko:

Das Restrisiko ist das nach der Umsetzung von Sicherheitsmaßnahmen verbleibenden Risiko.

Es gibt niemals 100% Sicherheit!

- Ausnahme: Reduzierung der Funktionalität auf Null



2. Definition der IT-Sicherheit:

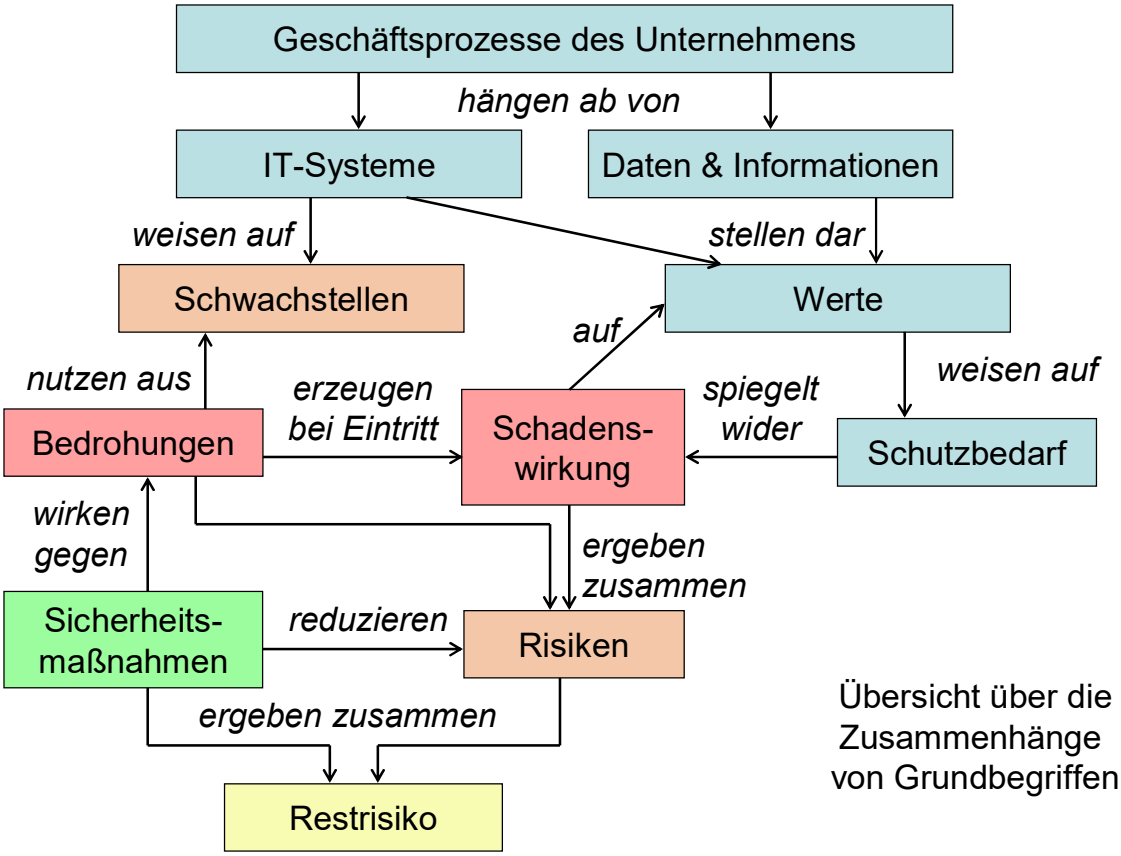
IT-Sicherheit ist der Zustand der IT, in dem die Risiken, die beim IT-Einsatz aufgrund von Bedrohungen vorhanden sind, durch angemessene Maßnahmen auf ein tolerierbares Maß reduziert sind.

Beispielzusammenhänge zwischen Bedrohungen, Maßnahmen und Risiken

- Bsp.: Erdbeben
  - Reduzierung der Eintrittswahrscheinlichkeit: Standortverlagerung
  - Reduzierung des erwarteten Schadens: Erdbebensicherer Bau des Gebäudes
- Bsp. Blitzeinschlag
  - Eintrittswahrscheinlichkeit läßt sich nicht reduzieren
  - Auswirkungen lassen sich reduzieren durch Blitzableiter und Überspannungsschutz
- Bsp. Zugriffsschutz
  - Durch Maßnahmen zum Zugriffsschutz wird die Eintrittswahrscheinlichkeit unbefugter Zugriffe reduziert.
  - Die Auswirkungen eines unbefugten Zugriffs bleiben unverändert.
- Bsp. Verschlüsselung:
  - Risiko Abhören: Verschlüsselung reduziert die Auswirkung
  - Risiko Offenlegung von Informationen: Verschlüsselung reduziert Eintrittswahrscheinlichkeit
- Bsp. Backup:
  ob Maßnahme präventiv/reaktiv, hängt von der betrachteten Gefährdung ab!
  - Festplatten-Chrash: Backup reduziert die Auswirkung eines Chrashs
  - Datenverlust: Backup reduziert die Eintrittswahrscheinlichkeit eines Datenverlusts

Unterschieden werden in der Regel

- Organisatorische Maßnahmen
- Technische Maßnahmen
- Personelle Maßnahmen
- Physische/Infrastrukturelle Maßnahmen



Übersicht über die Zusammenhänge von Grundbegriffen

Exkurs IT-Grundschutz

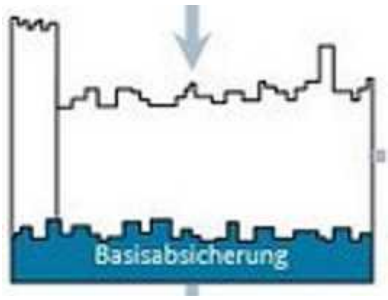
Vorgehensweise des Bundesamts für Informationssicherheit (BSI)

- neu überarbeitet Oktober 2017
- alte Versionen Grundschutzstandards 100-1, 100-2, 100-3 ersetzt durch 200-1/2/3
- Grundschutzkataloge zu Gefährdungen, Bausteinen und Maßnahmen waren ausgeufert (sehr viel, sehr groß)
- Handhabbarkeit dadurch eingeschränkt

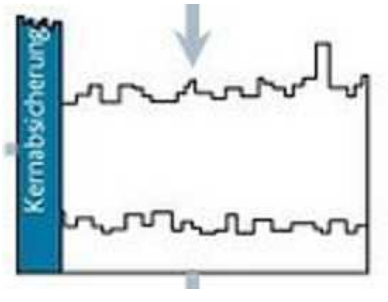
BSI-Standards:

- BSI-Standard 200-1:
  - allgemeine Anforderungen an ein Managementsystem für Informationssicherheit (ISMS)
  - kompatibel zum internationalen Standard ISO 27001
- BSI-Standard 200-2: IT-Grundschutz-Methodik
- BSI-Standard 200-3: Risikomanagement auf Basis von IT-Grundschutz
- BSI-Standard 100-4: Notfallmanagement (alt)

Grundschutz-Kompendium unterscheidet 3 Arten von Absicherung:

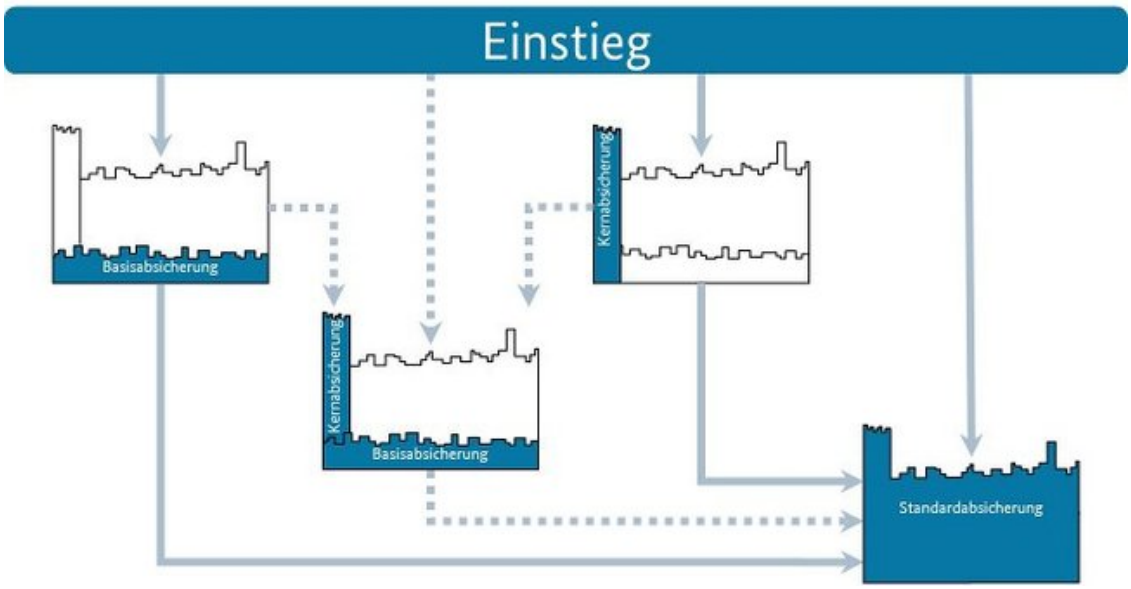


Basis-Absicherung
- Einstieg zum Aufbau ISMS,
- elementare Schritte, auch für KMU gut realisierbar
- begrenztes Sicherheitsniveau (nur das Wichtigste)
- über das ganze Unternehmen



Kern-Absicherung:
- nur spezielle, besonders wichtige Prozesse/IT
- Basis- und Standardanforderungen,
- evtl. Anforderungen für erhöhten Schutzbedarf

Standard-Absicherung:
- Basis- und Standardanforderungen
- über das ganze Unternehmen



Basis-Absicherung Anwendbarkeitskriterien:

- Die Umsetzung von Informationssicherheit steht noch am Anfang, sie hat ein eher niedriges Niveau.
- Die Geschäftsprozesse haben kein deutlich erhöhtes Gefährdungspotential
- Das angestrebte Sicherheitsniveau ist normal.
- Es gibt keine Assets, deren Diebstahl, Zerstörung oder Kompromittierung einen existenzbedrohenden Schaden für die Institution bedeutet.
- Kleinere Sicherheitsvorfälle werden toleriert.

Kern-Absicherung Kriterien:

» Die Anzahl der Geschäftsprozesse mit deutlich erhöhtem Schutzbedarf ist überschaubar bzw. umfasst nur einen kleinen Anteil aller Geschäftsprozesse.

» Diese Geschäftsprozesse sind leicht identifizierbar und abgrenzbar.

» Die Kronjuwelen (Assets, deren Diebstahl, Zerstörung oder Kompromittierung existenzbedrohend für die Institution wäre) sollen vorrangig geschützt werden.

» Kleinere Sicherheitsvorfälle, die Geld kosten oder anderweitig Schaden verursachen, aber keinen existenzbedrohenden Schaden verursachen, sind hinnehmbar.

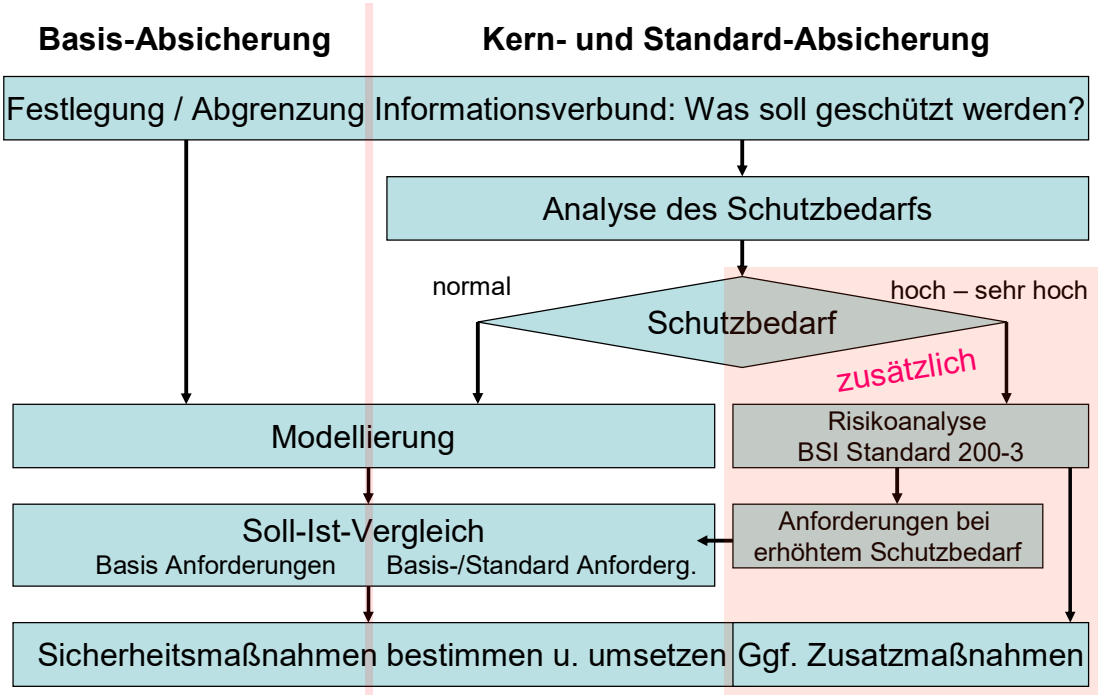
Standard-Absicherung = klassischen IT-Grundschutz-Vorgehensweise

» In vielen Bereichen gibt es bereits Sicherheitsmaßnahmen. Eine grundlegende Erst-Absicherung ist vorhanden.

» Es besteht kein Handlungsbedarf, einzelne Geschäftsprozesse vordringlich abzusichern. Es gibt keine Assets mit besonders hohem Schutzbedarf.

» Sicherheitsvorfälle, die wahrnehmbar die Aufgabenerfüllung beeinträchtigen, Geld kosten oder anderweitig erkennbaren Schaden verursachen, sind für die Institution nicht akzeptabel, auch wenn sie nicht existenzbedrohend sind.

Vorgehen gemäß Grundschutz-Kompendium



Bei normalem Schutzbedarf wird von pauschalisierter Gefährdungslage ausgegangen.

=> keine Risikoanalyse

Modellierung:

- Der betrachtete Informationsverbund wird mit Grundschutz-Bausteinen nachgebildet

Soll-Ist-Vergleich = IT-Grundschutz-Check = Basis Sicherheitscheck nach IT-Grundschutz

- Prüfung, in wie weit Anforderungen (Basis/Standard) aus den Bausteinen erfüllt sind

=> Anforderung entbehrlich / erfüllt / teilweise erfüllt / nicht erfüllt

Sicherheitsmaßnahmen bestimmen und umsetzen:

- für bisher nicht oder nur teilweise erfüllter Anforderungen
- geeignete Sicherheitsmaßnahmen festgelegen und umsetzen
  1. Maßnahmen identifizieren,
  2. Kosten abschätzen,
  3. Maßnahmen priorisieren, Umsetzungsreihenfolge festlegen,
  4. Verantwortung für Umsetzung zuweisen

Grundschutz-Kompendium wird jährlich überarbeitet und hat folg. Struktur

1. Elementare Gefährdungen (47): z.B. Datenverlust, Personalausfall, Social Engineering

2. Bausteine aufgeteilt in Gruppen

Abk.	Bausteingruppe (Anzahl Bausteine)	Beispiele für Bausteine
ISMS	Sicherheits-management (1)	Sicherheitsmanagement
ORP	Organisation und Personal (5)	Sensibilisierung/Schulung, ID-Management, Compliance Management
CON	Konzeption und Vorgehensweisen (7)	Datenschutz, Datensicherungskonzept, Auswahl und Einsatz von Standardsoftware, Löschen und Vernichten
OPS	Betrieb (11)	Patch-/Änderungsmanagement, SW-Test/Freigaben, Fernwartung, Telearbeit,
DER	Detektion und Reaktion (7)	Behandlung Si-Vorfälle, Audits/Revisionen, Notfallmangt.
APP	Anwendungen (12)	Office-Prod., Web-Browser, Fileserver, Samba
SYS	IT-Systeme (17)	Allg. Server/Client, Virtualisierung, Laptops, Android
IND	Industrielle IT (5)	Sensoren und Aktoren, SPS, allg. ICS-Komponente
NET	Netze und Kom-munikation (7)	VPN, Firewall, WLAN, Router/Switches
INF	Infrastruktur (8)	Mobiler Arbeitsplatz, IT Verkabelung

Standardisierter Aufbau jedes Bausteins:

1. Beschreibung
2. Gefährdungslage: Aufzählung relevanter Gefährdungen
3. Anforderungen: Basis-Anforderungen, Standard-Anforderungen, Anforderungen bei erhöhtem Schutzbedarf
4. Weiterführende Informationen / Literatur
5. Kreuzreferenztabelle Anforderungen/Gefährdungen

bsi.bund.de => Themen: Grundschutz => Grundschutz Kompendium

Typische Probleme bei der Einführung/Umsetzung von Sicherheitsmaßnahmen

1. Sicherheitsmaßnahmen kosten Geld!
2. Sicherheitsmaßnahmen sind häufig unbequem.
3. Um zu wirken muss Sicherheit umfassend sein.

1. Problem: Sicherheitsmaßnahmen kosten Geld!

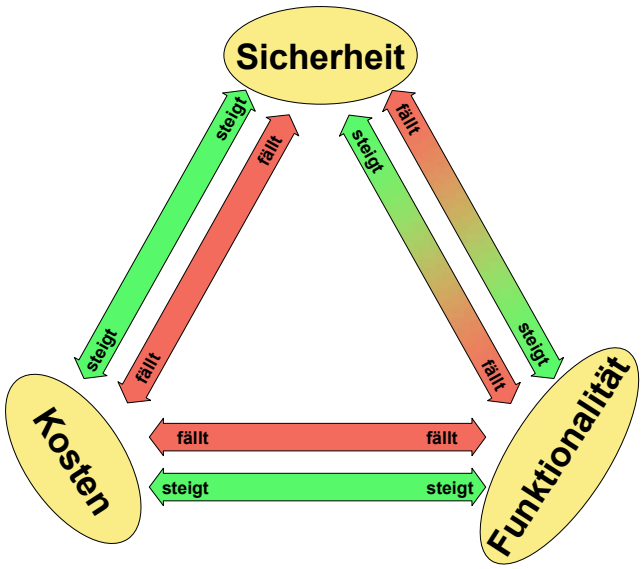
- Anschaffung:
  - Hardware und Software
  - ggf. SW-Entwicklung
  - Vorstudie zur Entscheidungsfindung
- Inbetriebnahme:
  - Installation und Konfiguration
  - Integrationsprojekt
- Betrieb:
  - Hardware/Software Wartung,
  - Releasewechsel, Patch- und Changemanagement
  - ggf. Vorhalten von Ersatzgeräten
  - Schulung von Mitarbeitern
  - interner User-Helpdesk

2. Problem: Sicherheitsmaßnahmen sind häufig „unbequem“.

- Beispiele:
  - Personenkontrollen auf Flughäfen,
  - gute Passwörter, 2 Faktor Authentisierung
  - Vorgehen gemäß Richtlinien: „Wieso darf ich eigentlich nicht ... ?“
  - Datensicherung

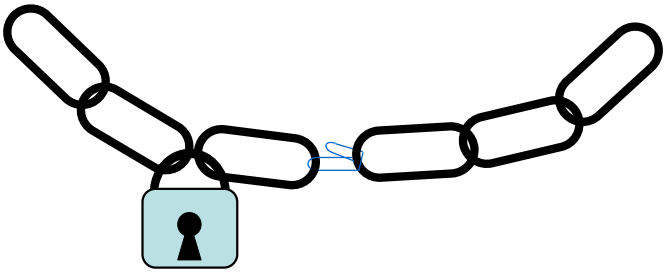
Dreiecksbeziehung: IT-Sicherheit, Kosten, Funktionalität

- Ein Mehr an IT-Sicherheit führt zu erhöhten Kosten (bei konstanter Funktionalität)
  - Sicherheitskonzept, Zusatzmaßnahmen, etc.
- Eine Erhöhung der Funktionalität führt zur Verminderung der IT-Sicherheit (bei konstanten Kosten)
  - Alle Benutzer einer speziellen Anwendung benötigen Administratorrechte
- Eine Erhöhung der Funktionalität führt zu erhöhten Kosten (bei konstanter IT-Sicherheit)
  - Alle Benutzer einer speziellen Anwendung benötigen Administratorrechte
  - Um die Sicherheit konstant zu halten, müssen alle betroffenen Benutzer geschult werden

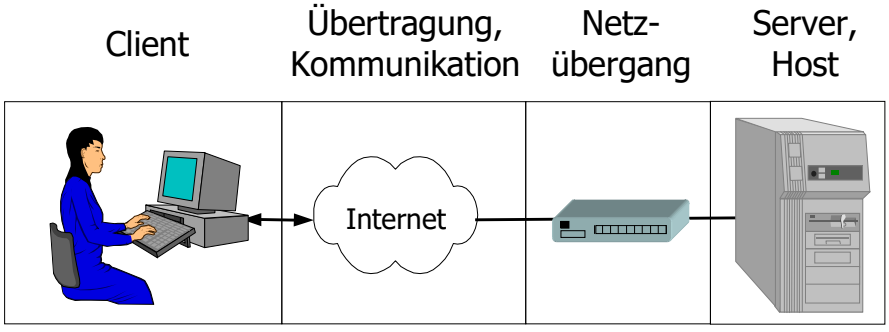


3. Problem: Sicherstellung umfassender Sicherheit

- Die Sicherheit wird durch das schwächste Kettenglied bestimmt.
- Häufig ist der Benutzer das schwächste Kettenglied
  - Bsp.: In einer Passwortdatei reicht ein schwaches Passwort aus, um den Systemzugang für einen Angreifer zu ermöglichen



Beispiel einer Sicherheitskette:



Beispiel einer Sicherheitskette

Gleichmäßige Sicherheit

- Unausgeglichene Sicherheitsmaßnahmen bedingen ein schlechtes Kosten-Nutzen Verhältnis!
- Bei der Skalierung von Sicherheitsmaßnahmen zu berücksichtigen.

Nachbarübung: Bitte zuordnen:

Hängt von der Eintrittswahrscheinlichkeit und Schadenshöhe ab		1. Schutzbedarf 2. Risikoanalyse 3. Safety 4. Security 5. IT-Grundschutz 6. Geschäftsprozesse 7. Risiko 8. Restrisiko
Ausgangspunkt für die Schutzbedarfsanalyse		
Hängt ausschließlich von der Schadenshöhe ab		
Verbleibt nach Umsetzung von Sicherheitsmaßnahmen		
Sicherheit gegenüber fahrlässig herbeigeführten Bedrohungen		
Gibt es in qualitativer und quantitativer Form		
Geht von einer pauschalisierten Gefährdungslage aus		
Sicherheit gegenüber vorsätzlich herbeigeführten Bedrohungen		