



Kostenfaktor IT-Sicherheit

Was muss/darf IT-Sicherheit kosten?
... oder wie beziffert man Imageschäden?

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)

<http://svs.informatik.uni-hamburg.de/>

Zu hohe oder zu niedrige Ausgaben?

»...mangelnde Investition in IT-Sicherheit...«
BSI Lagebericht 2007

vs.

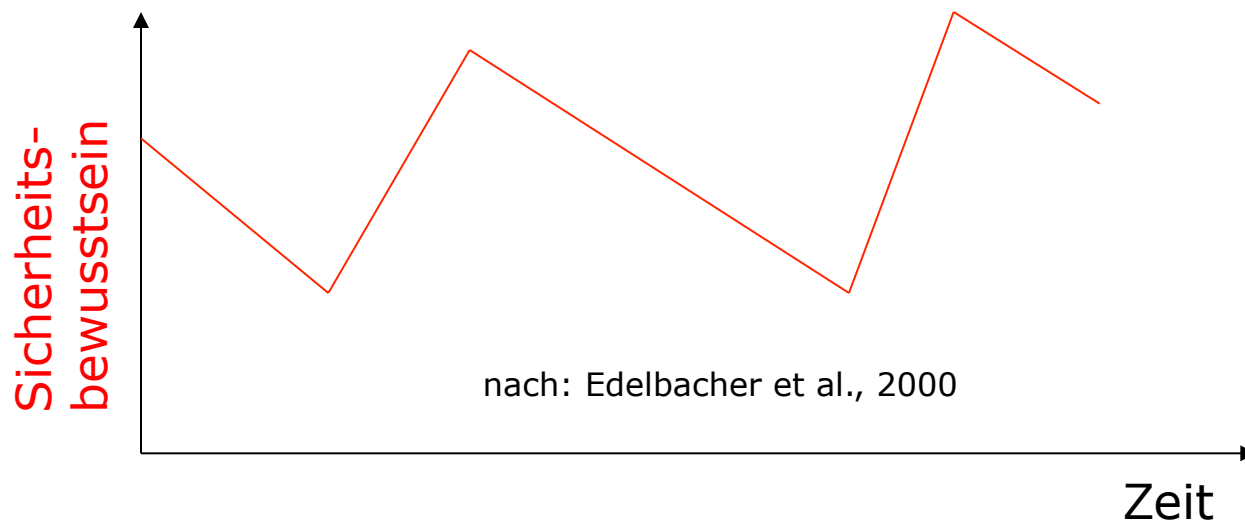
»The greatest IT risk facing most companies is more prosaic than a catastrophe. It is, simply, overspending.«
Nicholas G. Carr

- Ziele des Vortrags
 - Mögliche Antworten aus Wissenschaft und Praxis darstellen und kritisch hinterfragen
 - Aktuelle Forschungsansätze aufzeigen
 - Diskussion anregen

Erste einfache Antwort

Nichts (zusätzlich)

- Sicherheit ist eine Sekundärfunktion.
- »Kein System ist einfach nur sicher.«
- Sicherheit dient der Unterstützung und Erhaltung eines Primärziels.



Was ist IT-Sicherheit?

- Schutzziele gehen zurück auf Voydock, Kent 1983
- Klassische IT-Sicherheit berücksichtigt im Wesentlichen Risiken, die durch regelwidriges Verhalten in IT-Systemen entstehen.

Vertraulichkeit

unbefugter Informationsgewinn

Integrität

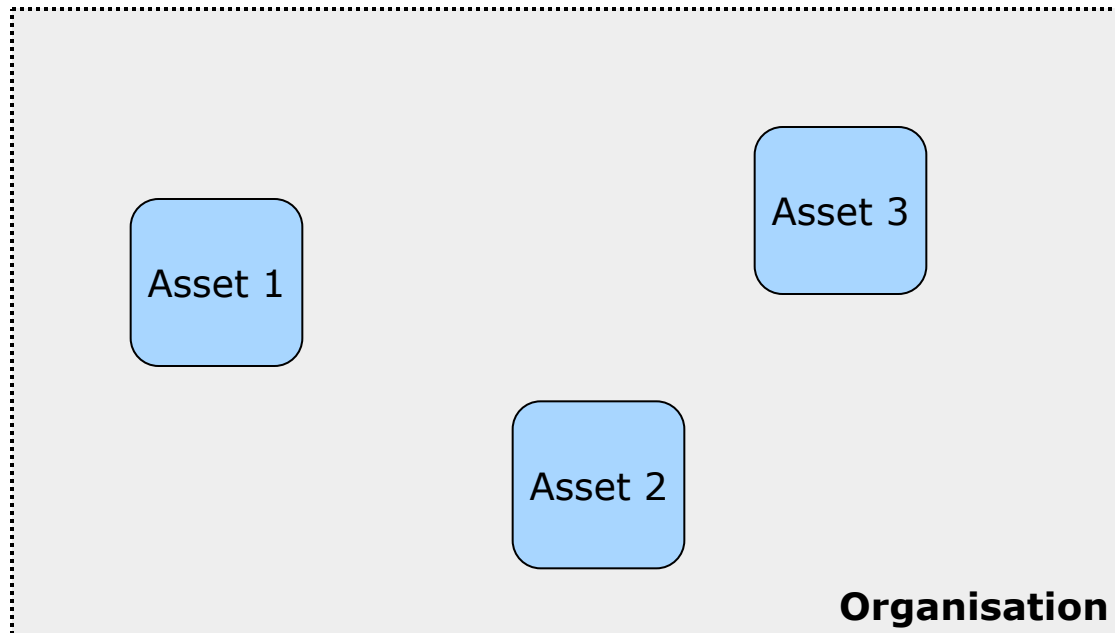
unbefugte Modifikation

Verfügbarkeit

unbefugte Beeinträchtigung der Funktionalität

Warum braucht man IT-Sicherheit?

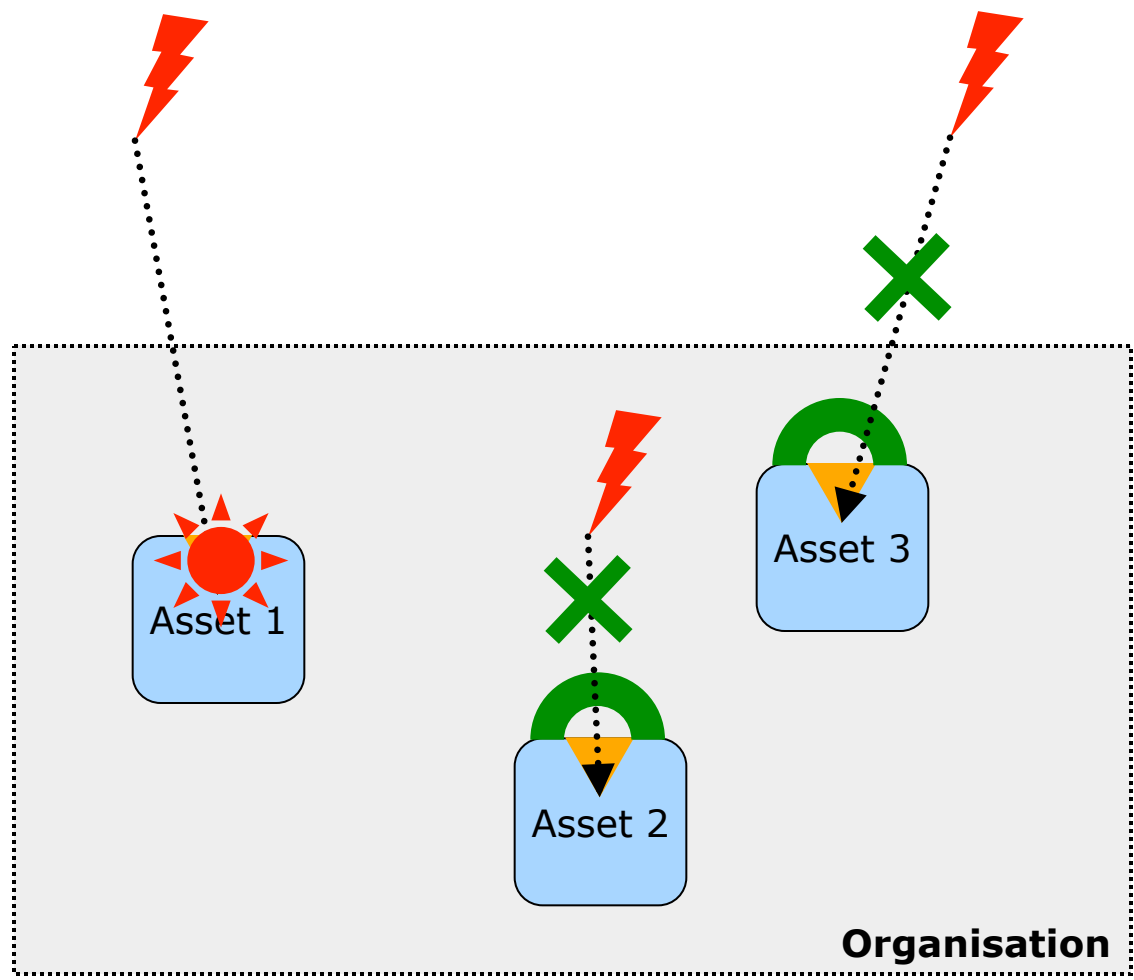
- Gründe, IT-Sicherheitsmanagement zu betreiben
 - Schutz von Unternehmenswerten (Assets)
 - Anforderung von Handelspartnern
 - IT-Compliance



Schutzziele

- Vertraulichkeit
- Verfügbarkeit
- Integrität

Von der Bedrohung zum Sicherheitsvorfall



- Bedrohungen, z.B.**
- Viren, Würmer
 - DoS
 - Hacking
 - Spionage
 - Social Engineering

- Verwundbarkeiten, z.B.**
- Konfigurationsfehler
 - Buffer Overflows

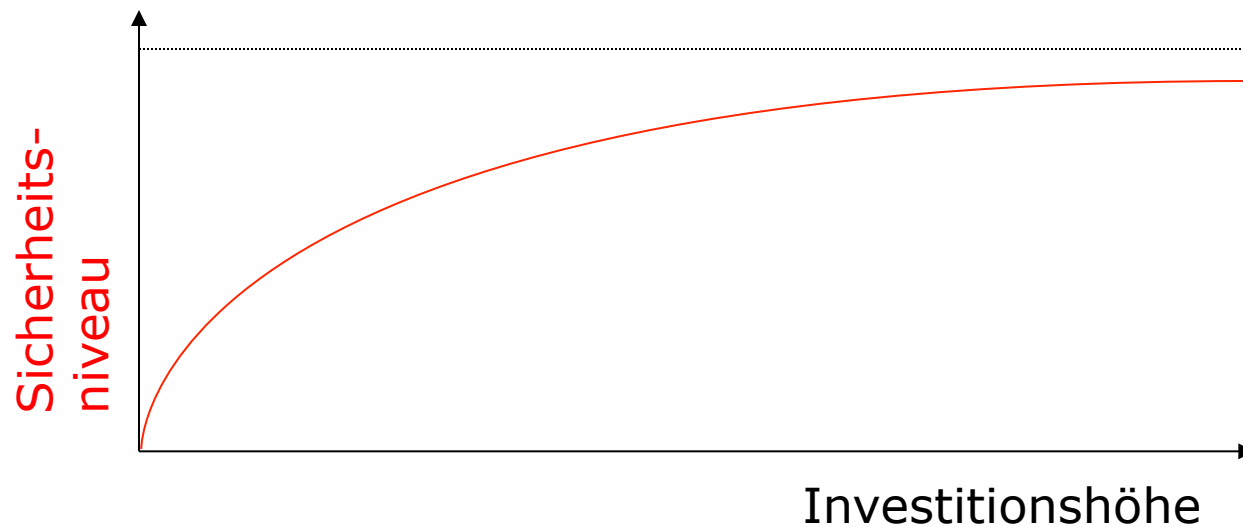
- Schutzziele**
- Vertraulichkeit
 - Verfügbarkeit
 - Integrität

- Maßnahmen**
- Präventiv
 - Detektiv
 - Reaktiv

Zweite einfache Antwort

So viel wie man braucht, um total sicher zu sein

- Kritik:
 - 100 %-ige Sicherheit ist nicht erreichbar



Dritte einfache Antwort

So viel wie das Budget hergibt

- Kritik
 - Budget nicht rational begründbar
- Anschlussfrage:
 - Wie groß muss das Budget gewählt werden?

Unterschiedliche Zielsetzungen

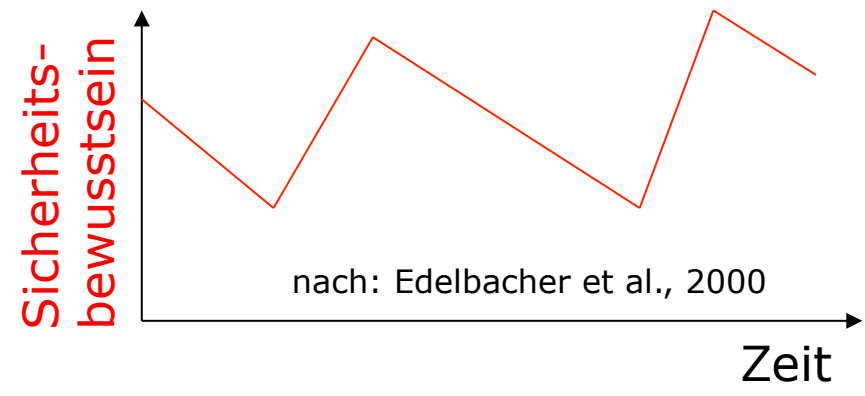
- Ziel Unternehmensleitung
 - Ausgaben gering halten
 - Kosten einsparen
 - Nur Projekte mit sichtbarem Nutzen realisieren
- Ziel Sicherheitsverantwortliche
 - Möglichst hohes Sicherheitsniveau schaffen
 - Budget erhöhen
- Was können Sie tun um Ihr Budget zu erhöhen?
 - Schüren Sie Angst!
 - Sammeln und drucken Sie Log-Files.
 - Verwenden Sie Abkürzungen und Fachbegriffe.
 - Zitieren Sie Studien von Sicherheitsfirmen und Beratungsunternehmen.

FUD-Strategie — Fear, Uncertainty, Doubt

Wieviel muss wirklich investiert werden?

vs.

Furcht, Ungewissheit, Zweifel



Computer Crime and Security Surveys

- Herausgegeben vom U.S. Computer Security Institute CSI
 - <http://www.gocsi.com/>
 - bekannteste Langzeit-Umfrage zu IT-Sicherheitsvorfällen
- Stichprobe
 - über 500 IT-Sicherheitsspezialisten aus verschiedenen Branchen



Computer Crime and Security Surveys

- Hauptergebnisse (2003)
 - Schäden in Unternehmen
 - Hauptschäden entstehen durch **Datendiebstahl**
 - Zweite Stelle: Schäden durch **Denial-of-Service-Angriffe**
 - Angriffsarten
 - 82 Prozent Virenangriffe
 - 80 Prozent Datenmissbrauch durch Insider
 - Reaktion auf Angriffe
 - 93 Prozent schließen Sicherheitslöcher
 - 50 Prozent verheimlichen Sicherheitslöcher
 - 30 Prozent verfolgen Angreifer (law enforcement)

Computer Crime and Security Surveys

- **Hauptergebnisse 2007**
 - Anstieg der Verluste durch Sicherheitsprobleme von 168.000 Dollar (2006) auf 350.000 Dollar (2007)
 - höchster Wert seit 2004
 - 18 Prozent der Befragten waren Opfer eines gezielten Angriffs
 - Hauptursache von Verlusten
 - in den vergangenen sieben Jahren: Viren (Schadsoftware)
 - nun an erster Stelle: »Financial fraud«
 - Insider-Angriffe
 - 59 Prozent der Fälle: unerlaubte Netznutzung
 - 52 Prozent der Fälle: Verseuchung mit Viren

Computer Crime and Security Surveys

- **Hauptergebnisse 2010/11**
 - **Malware** als verbreitetste Angriffsform
 - 67 Prozent der Teilnehmer berichten darüber
 - Anzahl der »Financial fraud« Vorfälle gegenüber der Vorjahre gesunken auf 8,7 Prozent
 - **Gezielte Angriffe** nehmen weiter zu
 - Bei etwa der Hälfte der Teilnehmer trat mindestens ein Informationssicherheitsvorfall auf
 - 46 Prozent dieser Teilnehmer berichten von mindestens einem gezielten Angriff
 - Erhöhte Sensibilität in Sicherheitsfragen
 - Immer weniger Teilnehmer sind bereit, genaue Daten über monetäre Verluste preiszugeben

Gründe für mangelnde Informationssicherheit

| | |
|--|------|
| Es fehlt an Geld | 55 % |
| Es fehlt an Bewusstsein bei den Mitarbeitern | 52 % |
| Es fehlt an Bewusstsein und Unterstützung im Topmanagement | 45 % |
| Es fehlt an Bewusstsein und Unterstützung beim mittleren Management | 37 % |
| Es fehlen verfügbare und kompetente Mitarbeiter | 32 % |
| Es fehlt an Möglichkeiten zur Durchsetzung sicherheitsrelevanter Maßnahmen | 31 % |
| Es fehlen die strategischen Grundlagen/Gesamtkonzepte | 29 % |
| Die Kontrolle und Einhaltung ist unzureichend | 27 % |
| Anwendungen sind nicht für Informationssicherheitsmaßnahmen vorbereitet | 25 % |
| Die vorhandenen Konzepte werden nicht umgesetzt | 22 % |
| Es fehlen realisierbare (Teil)-Konzepte | 19 % |

Basis: 158 Antworten

Quelle: <kes>/Microsoft-Sicherheitsstudie 2006
aus: ZIEL:SICHER 01/2007, Microsoft 2007, S. 6

Welchen Einfluss haben Sicherheitsvorfälle auf das Image?

- Garg, Curtis, Halper, 2003:
 - Messung des Börsenwerts eines Unternehmens
 - Beeinflussung durch einen Vorfall am Tag t ist an $t+1$ und $t+2$ in einigen Fällen (signifikant) nachweisbar

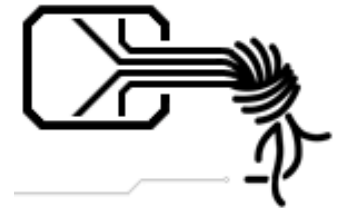
| Company | Announcement | Date of announcement | t (%) | $t+1$ (%) | $t+2$ (%) |
|---|---|----------------------|---------|-----------|-----------|
| Denial of service | | | | | |
| Yahoo | Denial of service attack beginning at 12:15 p.m. EST | 2/7/00 | -3.4 | -2.8 | -2.7 |
| eBay | Denial of service attack beginning at 6:00 p.m. EST | 2/8/00 | -3.7 | -4.8 | -10.1 |
| Microsoft | Denial of service attack beginning at 9:00 p.m. on 2/8/00 | 2/9/00 | -3.1 | -1.5 | -0.1 |
| Amazon | Denial of service attack beginning at 8:00 p.m. EST | 2/9/00 | -0.5 | -10.5 | -4.4 |
| Time Warner (CNN) | Denial of service attack beginning at 7:00 p.m. EST | 2/9/00 | 2.1 | 1.6 | 1.8 |
| E*Trade | Denial of service attack beginning at 4:00 a.m. EST | 2/9/00 | -2.0 | -5.1 | -4.7 |
| ZDNet | Denial of service attack beginning at 4:00 a.m. | 2/9/00 | 2.6 | -3.2 | -3.3 |
| Excite@Home | Denial of service attack | 2/10/00 | -3.3 | -3.2 | -5.9 |
| National discount brokers | denial of service attack | 2/24/00 | 4.1 | -1.8 | -9.4 |
| Microsoft | Denial of service attack over two days for MSN, MSNBC and Microsoft.com | 1/25/01 | -0.9 | 3.0 | 3.0 |
| | | | -0.8 | -2.9 | -3.6 |
| Theft of credit card information | | | | | |
| eUniverse (CD Universe) | On-line theft of credit card information for 300,500 customers | 1/10/00 | -18.0 | -20.7 | -24.6 |
| First data (Western Union) | On-line theft of credit card information for 15,000 customers | 9/8/00 | -5.7 | 0.2 | -0.8 |
| Egghead.com | On-line theft of credit card information for 3.3 million customers | 12/18/00 | -12.3 | -15.5 | -36.1 |
| Playboy | On-line theft of credit card information | 11/21/01 | -1.1 | -0.1 | 2.2 |
| | | | -9.3 | -9.0 | -14.9 |

| Company | Announcement | Date of announcement | t (%) | t+1 (%) | t+2 (%) |
|---|---|----------------------|-------|---------|---------|
| Denial of service | | | | | |
| Yahoo | Denial of service attack beginning at 12:15 p.m. EST | 2/7/00 | -3.4 | -2.8 | -2.7 |
| eBay | Denial of service attack beginning at 6:00 p.m. EST | 2/8/00 | -3.7 | -4.8 | -10.1 |
| Microsoft | Denial of service attack beginning at 9:00 p.m. on 2/8/00 | 2/9/00 | -3.1 | -1.5 | -0.1 |
| Amazon | Denial of service attack beginning at 8:00 p.m. EST | 2/9/00 | -0.5 | -10.5 | -4.4 |
| Time Warner (CNN) | Denial of service attack beginning at 7:00 p.m. EST | 2/9/00 | 2.1 | 1.6 | 1.8 |
| E*Trade | Denial of service attack beginning at 4:00 a.m. EST | 2/9/00 | -2.0 | -5.1 | -4.7 |
| ZDNet | Denial of service attack beginning at 4:00 a.m. | 2/9/00 | 2.6 | -3.2 | -3.3 |
| Excite@Home | Denial of service attack | 2/10/00 | -3.3 | -3.2 | -5.9 |
| National discount brokers | denial of service attack | 2/24/00 | 4.1 | -1.8 | -9.4 |
| Microsoft | Denial of service attack over two days for MSN, MSNBC and Microsoft.com | 1/25/01 | -0.9 | 3.0 | 3.0 |
| | | | -0.8 | -2.9 | -3.6 |
| Theft of credit card information | | | | | |
| eUniverse (CD Universe) | On-line theft of credit card information for 300,500 customers | 1/10/00 | -18.0 | -20.7 | -24.6 |
| First data (Western Union) | On-line theft of credit card information for 15,000 customers | 9/8/00 | -5.7 | 0.2 | -0.8 |
| Egghead.com | On-line theft of credit card information for 3.3 million customers | 12/18/00 | -12.3 | -15.5 | -36.1 |
| Playboy | On-line theft of credit card information | 11/21/01 | -1.1 | -0.1 | 2.2 |
| | | | -9.3 | -9.0 | -14.9 |
| Web-site defacement | | | | | |
| Staples | Web site defacement and diversion of on-line traffic | 10/11/99 | 0.3 | 4.6 | 0.9 |
| RSA Security | Web site defacement | 2/14/00 | -9.5 | -20.6 | -17.2 |
| Nike | Web site defacement and diversion of on-line traffic | 6/21/00 | -0.3 | 0.1 | 6.0 |
| Diageo (Burger King) | Web site defaced | 3/2/01 | 1.9 | 2.5 | -1.0 |
| British Telecom | Web site defaced | 4/2/01 | -2.3 | -1.5 | 5.4 |
| HSBC | Web site defaced | 9/21/00 | -1.6 | -1.2 | -0.6 |
| | | | -2.0 | -2.7 | -1.1 |
| Theft of customer information | | | | | |
| Microsoft | Hotmail defaced for two hours and hackers access accounts | 8/30/99 | 1.4 | 2.1 | 0.7 |
| Travelocity | On-line theft of personal information for 45,000 customers | 1/23/01 | -2.3 | -3.7 | 2.3 |
| Midwest Express | Hackers access customer information | 4/26/02 | 4.32 | | |
| Midwest Express | Hackers access customer information | 4/26/02 | | | |

Motivation hinter Angriffen im Wandel der Zeit

- **Hackerethik – Chaos Computer Club**

- Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
- Alle Informationen müssen frei sein.
- Misstrauen Autoritäten – fördere Dezentralisierung.
- Beurteile einen Hacker nach dem, was er tut und nicht nach üblichen Kriterien wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftlicher Stellung.
- Man kann mit einem Computer Kunst und Schönheit schaffen.
- Computer können dein Leben zum Besseren verändern.



- **Motto von Anonymous**

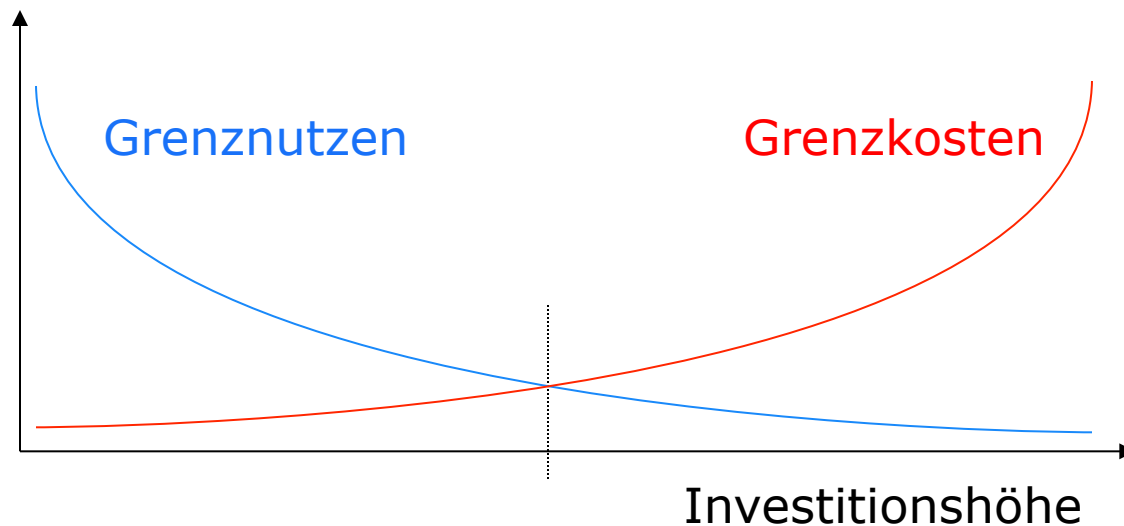
- We are Anonymous. We are Legion.
We do not forgive. We do not forget. Expect us.



Vierte einfache Antwort

So viel wie im Schnittpunkt von Grenzkosten und Grenznutzen an der Abszisse abzulesen ist.

- Kritik
 - Viel hilft nicht unbedingt viel, es kommt auch darauf an, wie das Geld ausgegeben wird



Vierte einfache Antwort

So viel wie im Schnittpunkt von Grenzkosten und Grenznutzen an der Abszisse abzulesen ist.

- Kritik
 - Viel hilft nicht unbedingt viel, es kommt auch darauf an, wie das Geld ausgegeben wird
- Effektivität
 - = die richtigen Maßnahmen ergreifen
 - Weniger ist manchmal mehr.
- Probleme
 - Funktionen sind schwierig zu ermitteln
 - Funktionen sind nicht stetig, häufig sind Sicherheitsmaßnahmen binäre Entscheidungen

Fünfte einfache Antwort (1)

Es sollten alle Maßnahmen realisiert werden,
die einen positiven Return on Security Investment aufweisen

- ROSI
 - basiert auf dem ALE-Konzept aus den 70er Jahren
 - soll Analogie zum klassischen Return on Investment herstellen
 - verschiedene Darstellungsformen und Weiterentwicklungen

$$ALE_i = SLE_i \cdot ARO_i$$

$$ROSI_k = ALE_0 - ALE_k - Cost_k$$

$$ROSI_k = \frac{(RiskExposure_k \cdot \%RiskMitigated_k) - Cost_k}{Cost_k}$$

nach: Soo Hoo, 2000; Sonnenreich, 2006

ROSI – Return on Security Investment

- R Recovery Costs – Kosten der wahrscheinlichen Schäden
- S Savings – Reduzierung der K. der wahrsch. Schäden
- T Total Costs – Kosten der Maßnahmen
- ALE Annual Loss Expenditure – verbl. Schadenskosten nach Vorfall

$$ALE = R - S + T$$

$$ROSI = R - ALE$$

$$ROSI = S - T$$

- ROSI – Return on Security Investment – »Ersparnis« durch Abwenden der wahrscheinlichen Schäden abzügl. der Kosten der Sicherheitsmaßnahmen

ROSI – Return on Security Investment

- Beispiel
 - Webservice
 - Savings – Reduzierung der K. der wahrsch. Schäden
S = 100.000 EUR p.a. (Kunden- und Imageverlust)
 - Total Costs – Kosten der Maßnahmen
T = 5.000 EUR p.a. (Zertifikat, Firewall, Updates etc.)

$$\text{ROSI} = S - T = 95.000 \text{ EUR p.a.}$$

- ROSI – Return on Security Investment – »Ersparnis« durch Abwenden der wahrscheinlichen Schäden abzügl. der Kosten der Sicherheitsmaßnahmen

Fünfte einfache Antwort (2)

- Kritik
 - Kosten und Nutzen schwer ermittelbar → Unterschiede zu klassischen Investitionsprojekten
 - Es geht nicht nur um operative Entscheidungen: Sicherheitsmanagement beginnt auf der strategischen Ebene
 - ROSI häufig kritisiert
 - Worin liegt der Nutzen?
 - Erfüllung gesetzlicher Anforderungen, Generierung zusätzlicher Einnahmen, Effizienzgewinne, Reduktion von Risiken
 - Wie setzen sich die Kosten zusammen?
 - Ausgaben für Anschaffung, Einführung, laufenden Betrieb, Kosten durch Änderung betriebl. Abläufe
- ➔ Risikomanagement-Ansatz auf operativer Ebene erforderlich

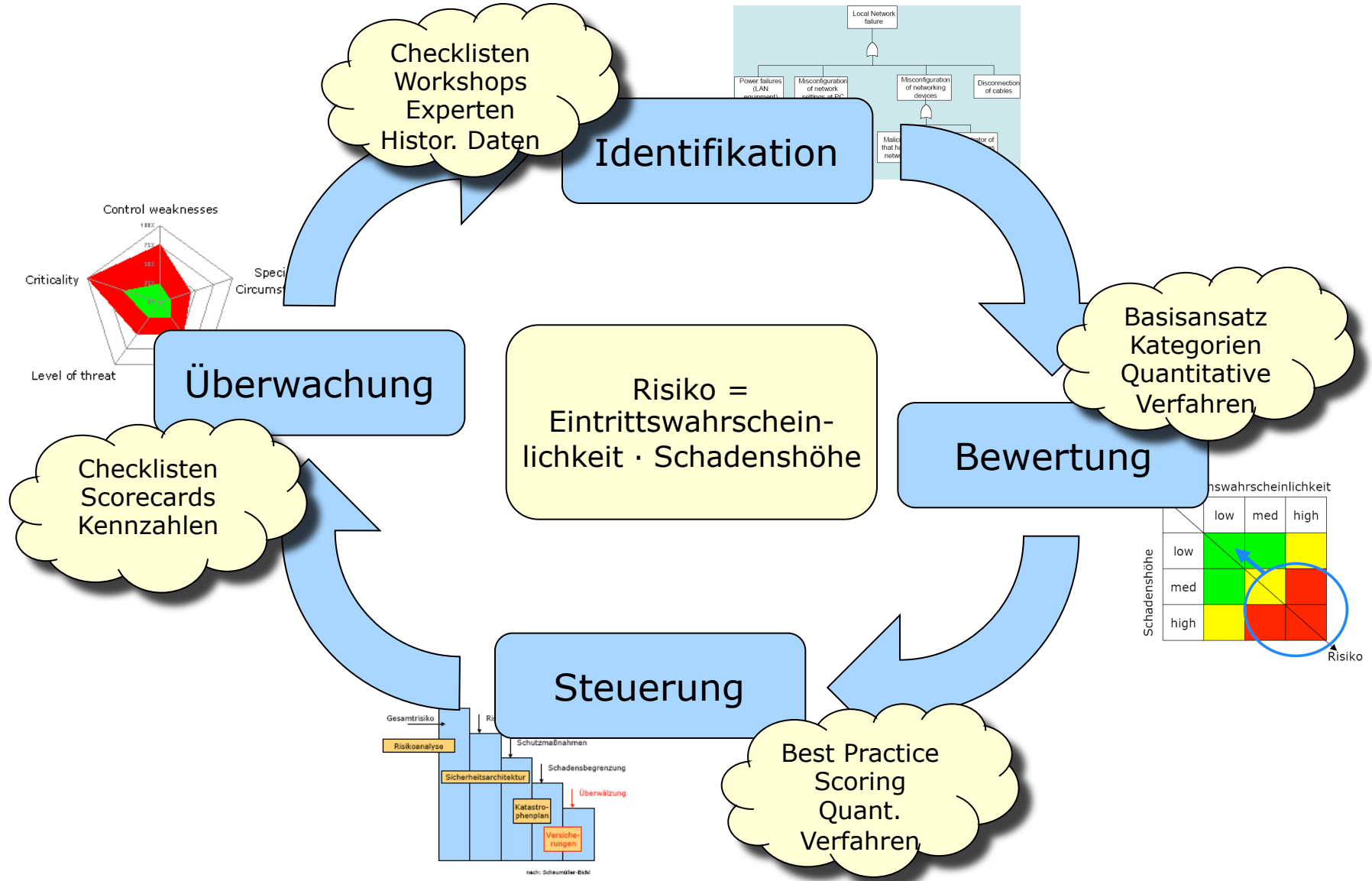
Sicherheitsmanagement beginnt auf der Strategiebene

| | Business Engineering | Sicherheitsmanagement |
|---|---|--|
| Strategieebene/ Sicherheitspolitik | Festlegung der Unternehmensaufgaben; Strategische Planung | Definition strategischer Ziele, Grundsätze und Richtlinien; Formulierung der Unternehmensziele aus Sicherheitssicht |
| Prozessebene/ Sicherheitskonzept | Gestaltung der Abläufe in Form von Prozessen | Übersetzung der Politik in Maßnahmen; Risikoanalyse |
| Systemebene/ Mechanismen | Unterstützung der Prozesse durch den Einsatz von Systemen; Analyse und Spezifikation der Anwendungssysteme | Detaillierung der Maßnahmen durch konkrete Mechanismen |

Sicherheitsmanagement beginnt auf der Strategiebene

- Aussagen für die strategische Ebene
 - Wer nur auf vorgefertigte Lösungen setzt, verliert auf lange Sicht wertvolles Know How.
 - Heterogene IT-Landschaften schützen vor Kumulrisiken.
 - IT-Sicherheit ist mehr als nur Technik.
 - Sicherheit sollte von Beginn an integraler Bestandteil der Prozesse werden und nicht hinterher hinzugebastelt werden.
 - Die Sicherheit sollte im Einklang mit anderen Disziplinen entwickelt werden, z.B. Synergien mit dem Business Engineering nutzen.

Operative Ebene – Betrachtung im Risikomanagement Kreislauf

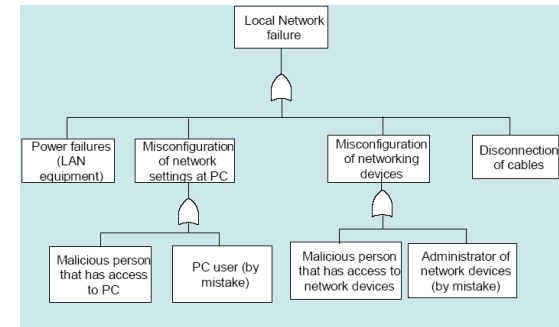
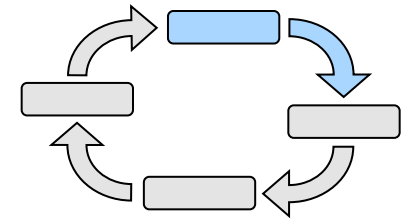


Identifikation von Bedrohungen

- Frage
 - »Welche Bedrohungen sind für das jeweilige Schutzobjekt relevant? «

- Methoden & Werkzeuge
 - OCTAVE-Methodik, CORAS-Framework
 - Checklisten
 - Workshops
 - Fehlerbäume, Attack-Trees
 - Szenarioanalysen

- Herausforderungen
 - Vollständige Erfassung aller Bedrohungen

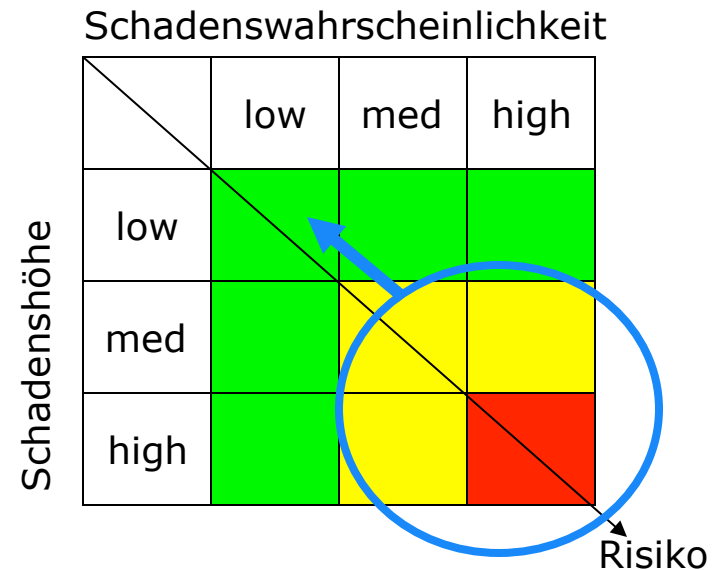
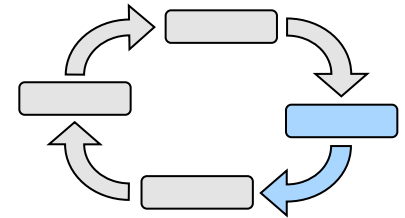


Bewertung von Risiken

- Frage
 - »Wie groß sind Eintrittswahrscheinlichkeit und Schadenshöhe eines potentiellen Schadensereignisses?«

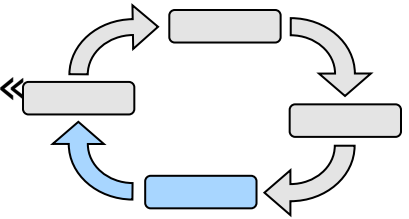
- Methoden & Werkzeuge
 - Qualitative Bewertung
 - Quantitative Bewertung
 - Spieltheorie
 - Maximalwirkungsanalyse

- Herausforderungen
 - Abhängigkeit von den Assets
 - Strategische Angreifer
 - Korrelationen
 - Quantifizierbarkeit



Steuerung der Risiken

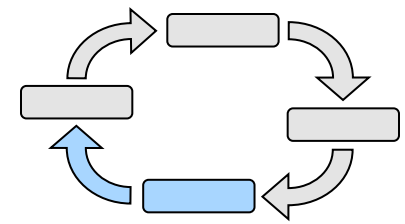
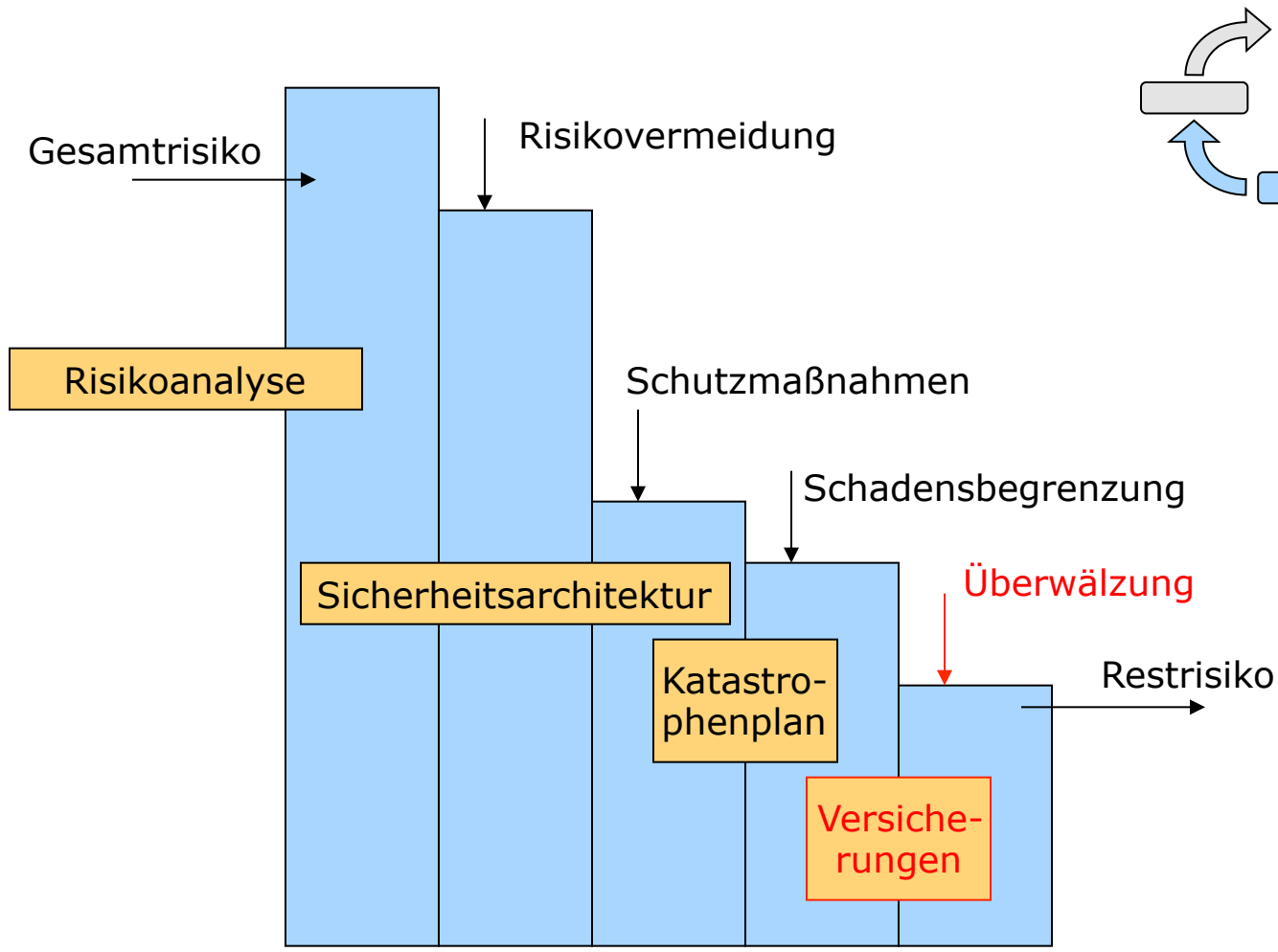
- Frage
 - »Welche Risiken sollen wie behandelt werden?«
- Methoden
 - Best Practice Ansätze / Grundschatz
 - Hilfsmittel aus der Investitionsrechnung und Entscheidungstheorie, z.B. NPV, IRR, AHP
- Herausforderungen
 - Qualität der Entscheidung hängt von zu Grunde liegenden Daten ab (baut auf dem Bewertungsschritt auf)



$$NPV_0 = -I_0 + \sum_{t=1}^T \frac{\Delta E(L_t) + \Delta OCC_t - C_t}{(1 + i_{calc})^t}$$

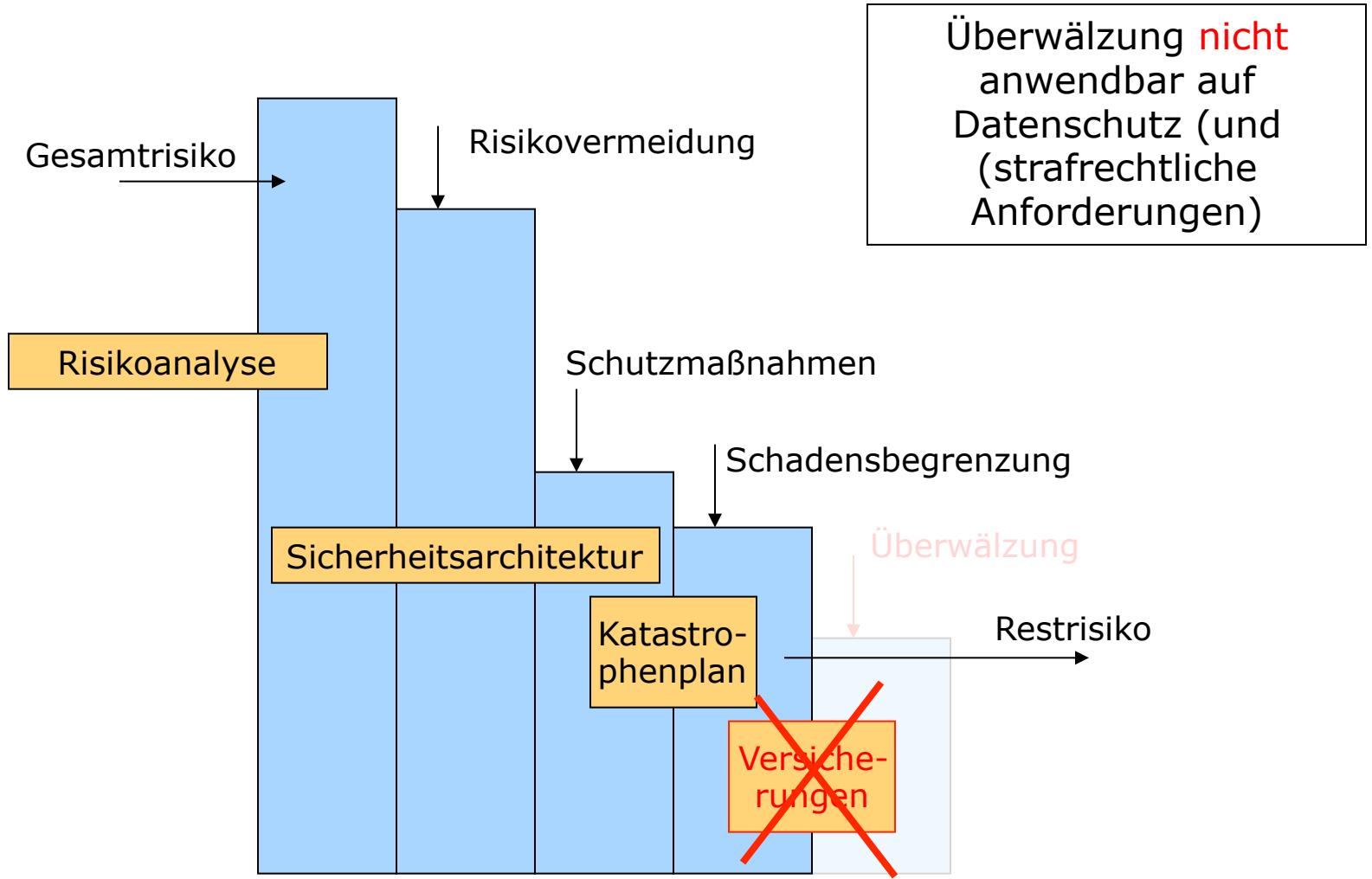
nach: Faisst et al., 2007

Risiko-Management für IT-Systeme



nach: Schaumüller-Bichl

Risiko-Management im Datenschutz

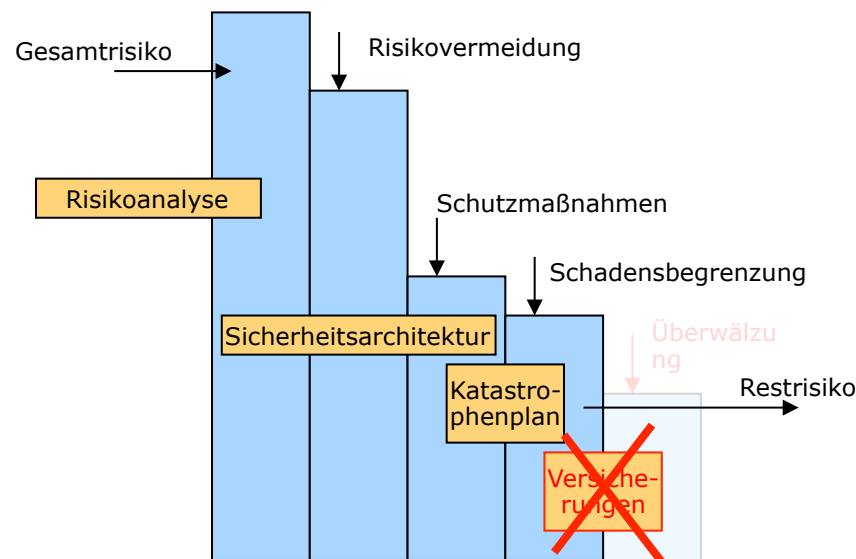
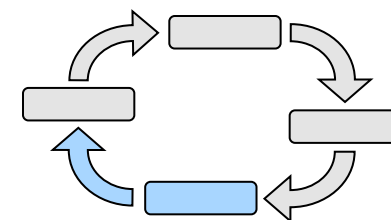


nach: Schaumüller-Bichl

Risiko-Management im Datenschutz

- IT-Sicherheit:
 - Risiko = Wahrscheinlichkeit · Schadenshöhe
 - Schäden sind systematisch tolerierbar

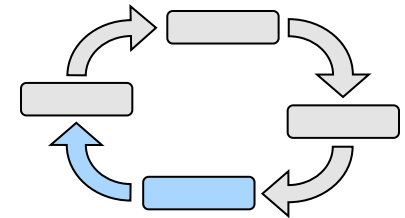
- Datenschutz:
 - Alles-Oder-Nichts-Ansatz
 - Rechtliche Vorgaben müssen umgesetzt werden



nach: Schaumüller-Bichl

Risiko-Management für IT-Systeme

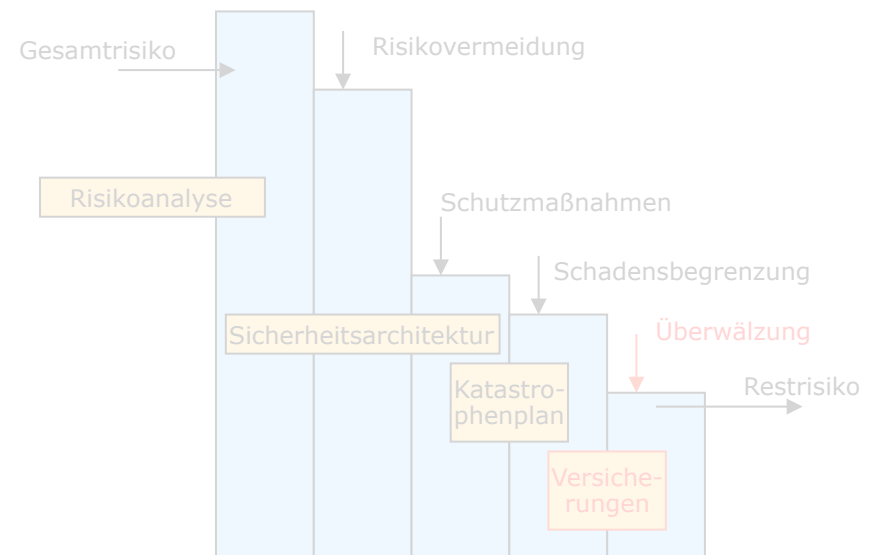
Typische Positionen für Vermeidung, Akzeptanz und Überwälzung:



Schadenswahrscheinlichkeit

| | | | |
|------|-------------|-----------------|------|
| | low | med | high |
| low | Akzeptanz | Vermeidung | |
| med | | Schutzmaßnahmen | |
| high | Überwälzung | | |

Schadenshöhe



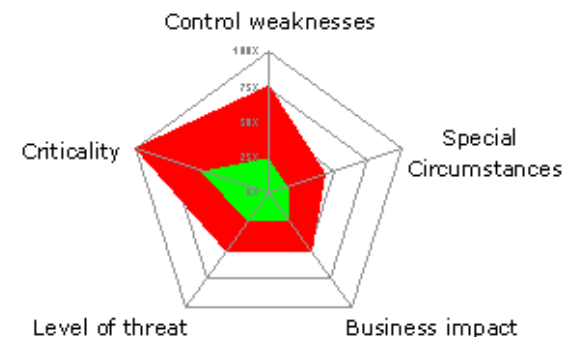
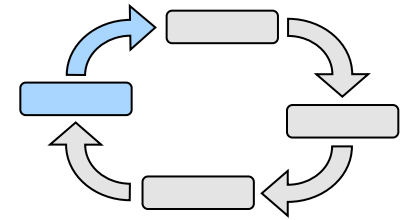
nach: Schaumüller-Bichl

Überwachung der Risiken und Maßnahmen

- Frage
 - »Waren die Maßnahmen effektiv und effizient? Wie sicher ist die Organisation?«

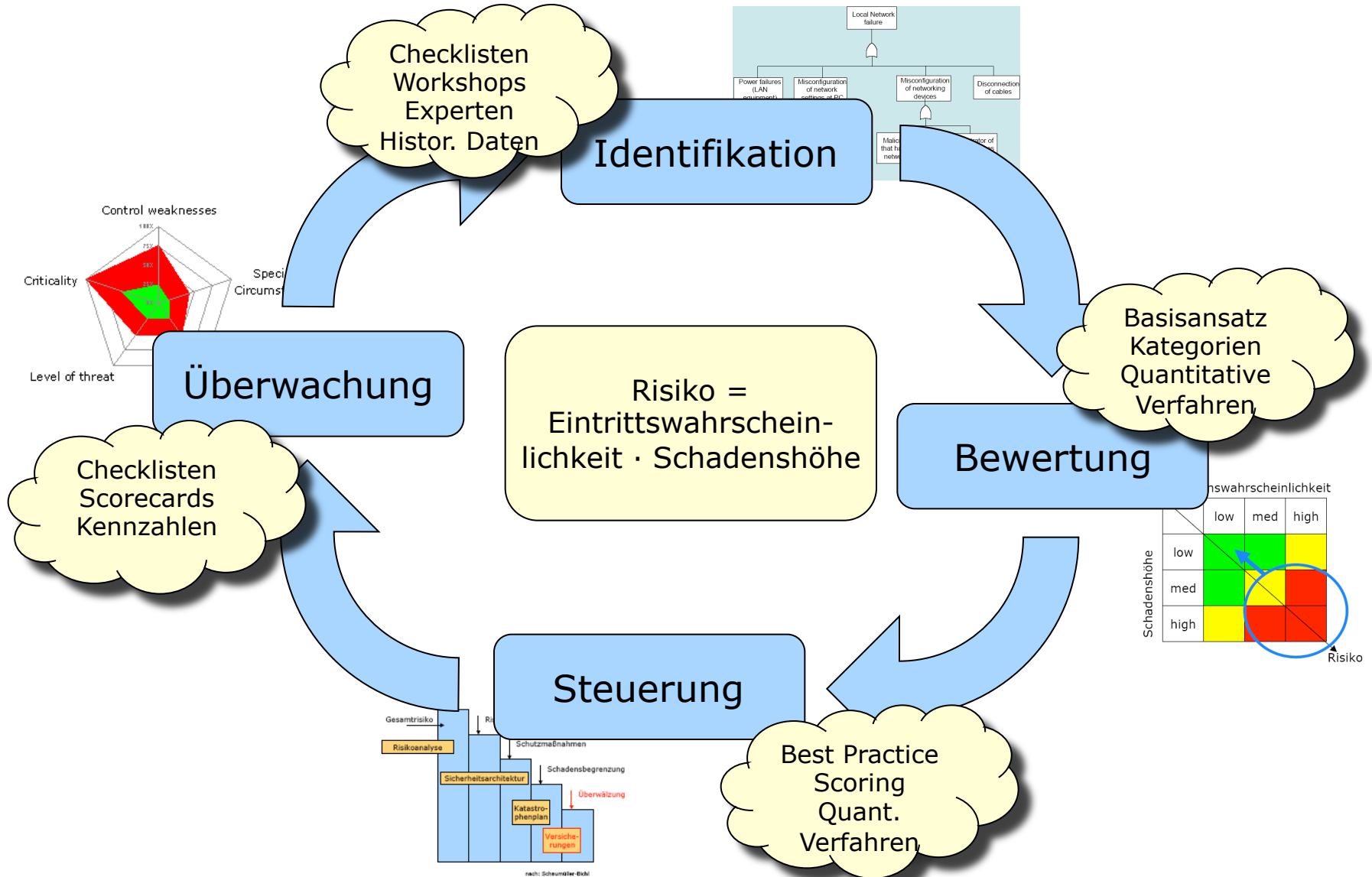
- Methoden
 - Kennzahlen Systeme (z.B. TÜV Secure IT)
 - Security Scorecard oder Integration in Balanced Scorecard

- Herausforderungen
 - Die „richtigen“ Kennzahlen verwenden
 - Kennzahlen „richtig“ ermitteln/messen
 - Kennzahlen aktuell halten



nach: Loomans, 2002

Risikomanagement Kreislauf



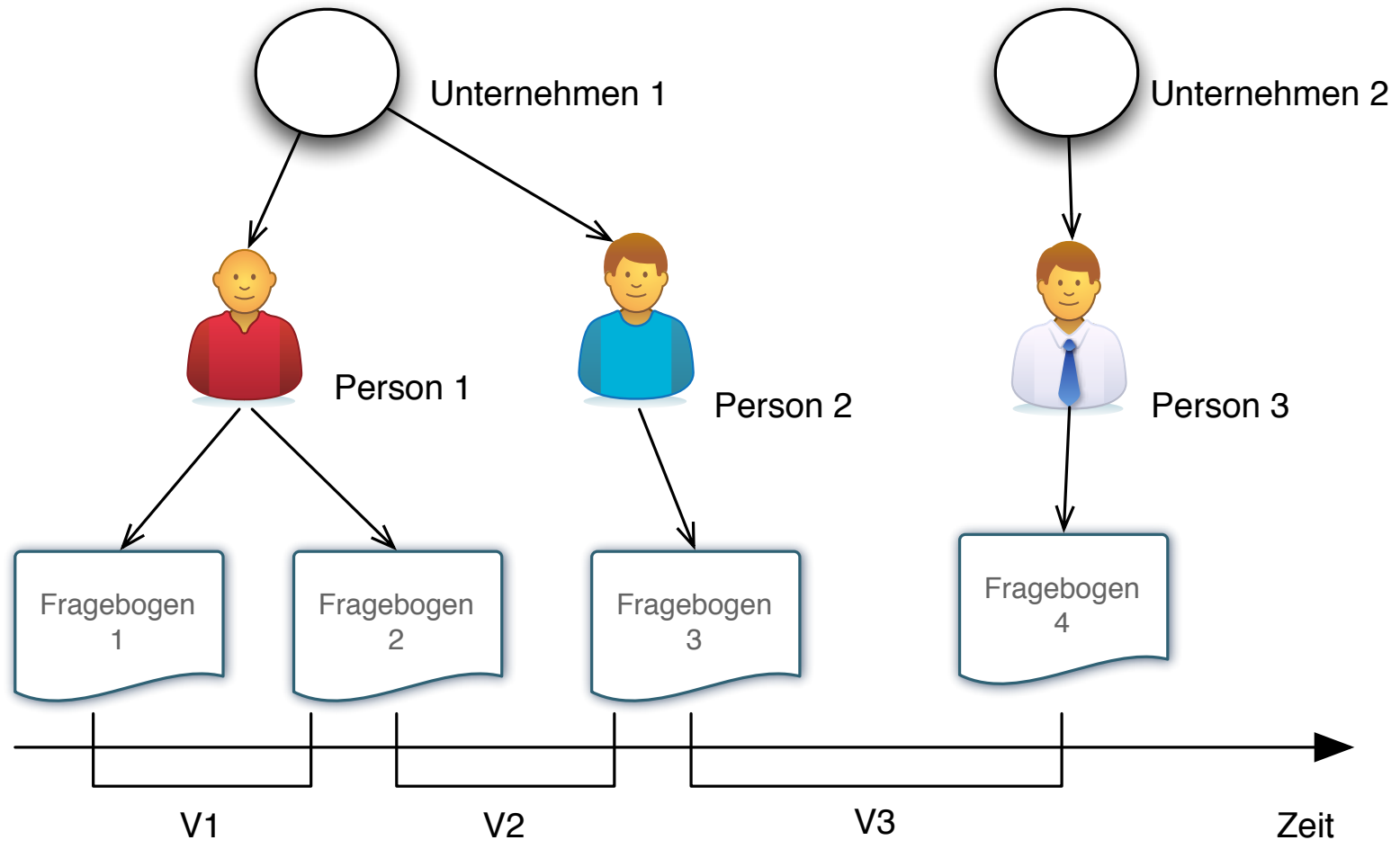
Mögliche Quellen für quantitative Daten

| Quelle | Beispiel | Bewertung |
|-------------------|--|---|
| Expertenurteile | Interviews mit internen oder externen Experten CSI/FBI Survey | Häufig verwendet, aber nicht messbar Subjektiv, unvollständig |
| Simulationen | Historische oder Monte Carlo Simulationen | Noch kaum verbreitet Gut, wenn Ausgangsdaten vorhanden |
| Marktmechanismen | Kapitalmarktanalysen Bug Challenges Derivative Produkte | Nicht für alle Bereiche anwendbar Noch nicht verfügbar |
| Historische Daten | CERTs/CSIRTs Interne Vorfallsbearbeitungssysteme | In anderen Bereichen weit verbreitet Prognosequalität? Kaum verfügbar |

Sammlung und Austausch historischer Daten

- Idee
 - Entwurf eines Systems zur Sammlung von quantitativen historischen Daten über Sicherheitsvorfälle in Organisationen.
- Ziel
 - Aufbau einer Datenbasis die Informationen über Schadenshöhe, Eintrittswahrscheinlichkeit und Wahrscheinlichkeitsverteilungen von Sicherheitsvorfällen in verschiedenen Organisationen gibt.
- **Verschiedene Möglichkeiten zur Verwendung der generierten Daten**
 - Risikobewertung, Evaluation von Investitionsentscheidungen
 - Benchmarking zwischen Organisationen
 - Untersuchung Korrelationen zwischen Schadensereignissen
 - Wissenstransfer von Organisation zu Organisation

Security Benchmarking

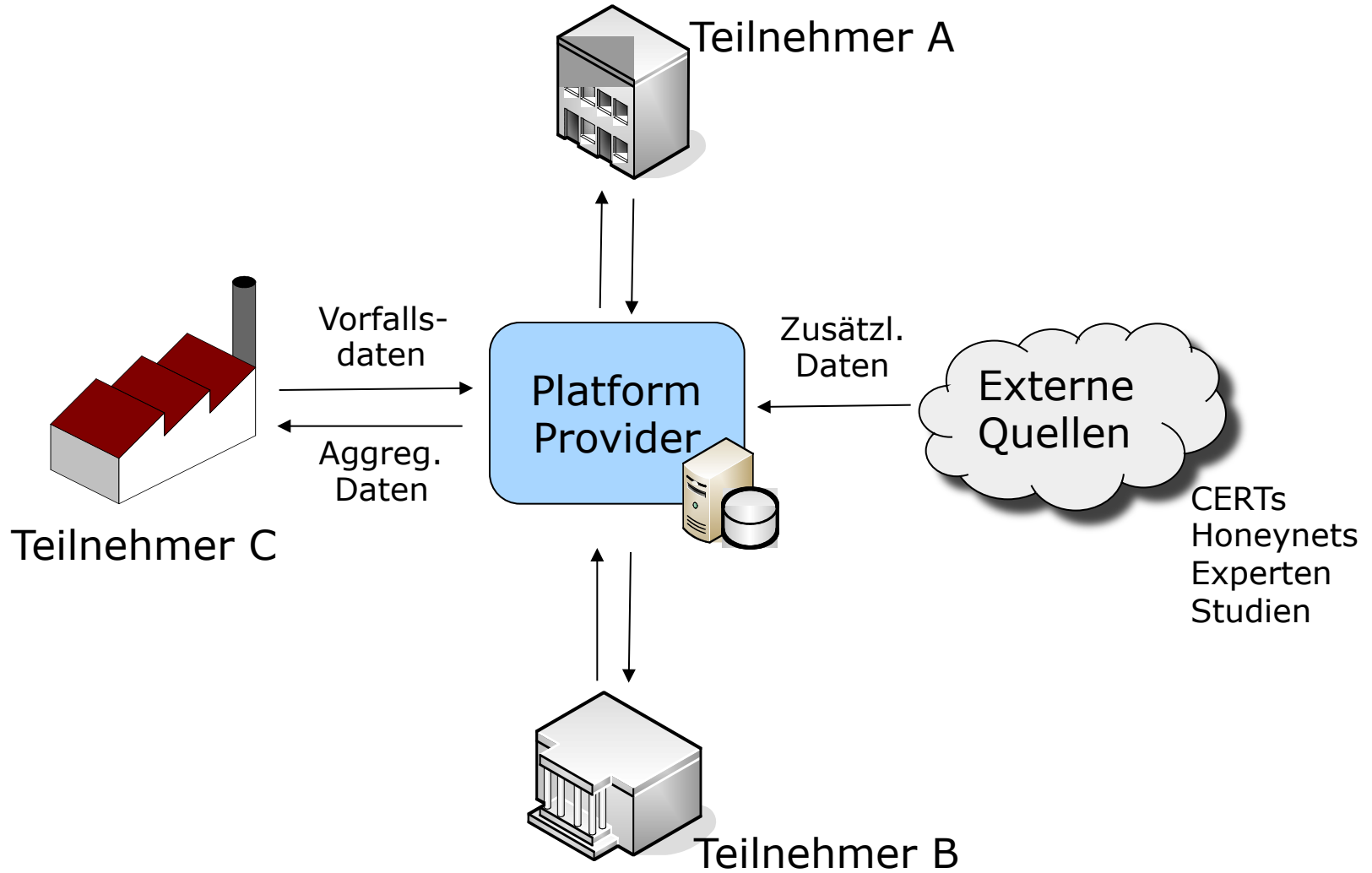


V1: Vergleiche im Zeitverlauf

V2: Vergleiche hinsichtlich der Interpretation eines Kollegen

V3: Vergleiche mit anderen Unternehmen

Basisarchitektur



Security Benchmarking

- Einfache Teilnahme
 - Keine Anmeldung notwendig
 - Angabe von Unternehmensdaten optional
- Schnelle Einschätzung
 - Derzeit sind 80 Fragen hinterlegt
 - Dauer ca. 30 – 60 min
- Vergleichsmöglichkeiten
 - Mit anderen Unternehmen (Grundgesamtheit)
 - Mit ausgewählten Fragebögen
 - Beantwortung durch Kollegen, Berater, Vorgesetzte...
 - Eigene Fragebögen im Zeitverlauf vergleichen
- Dient einer ersten Selbsteinschätzung, ersetzt aber keine umfassende Grundschutzanalyse

Kostenlos nutzbar unter
<http://sec-compare.de>



Sec-Compare

Vergleichen Sie Ihre IT-Sicherheitskonzeption!



Prof. Dr. Hannes Federrath
FB Informatik, AB SVS
Universität Hamburg
Vogt-Kölln-Straße 30
D-22527 Hamburg

E-Mail federrath@informatik.uni-hamburg.de

Telefon +49 40 42883 2358

<http://svs.informatik.uni-hamburg.de>