

Inventarisierung + Bewertung von IT-Risiken

Thomas Maus
Maus IT-Consulting

thomas.maus@alumni.uni-karlsruhe.de

Inhalt

- Wo soll die Reise hingehen?
- Was ist Risiko eigentlich?
- Ein pragmatisches Modell für Risiko
- Die Risikokultur Ihrer Organisation
- Das Risikoinventar Ihrer Organisation
- Risikostruktur an Beispiel-Szenarien
- A-Risk-Methics
- Aus- und Rückblick

Wo soll die Reise hingehen?

- Verstehen der eigenen Sicherheitslage
- Kommunikationshilfsmittel für Gespräche zwischen Management, Fachseite + Administratoren
- Grundlage für nachvollziehbare, objektivierbare Entscheidungen
- Planungshilfsmittel für Sicherheitsarchitektur
- Priorisierung und Wirtschaftlichkeit von Maßnahmen

Was ist Risiko eigentlich?

- Mathematisch/Ingenieurwissenschaftlich
- Moralisch/Politisch
- Psychologisch

Was ist Risiko?

Mathematisch/Ingenieurwissenschaftlich

- DIN, VDE 31000:

Risiko(Schadensereignis)

= (mittleres) Schadensausmaß

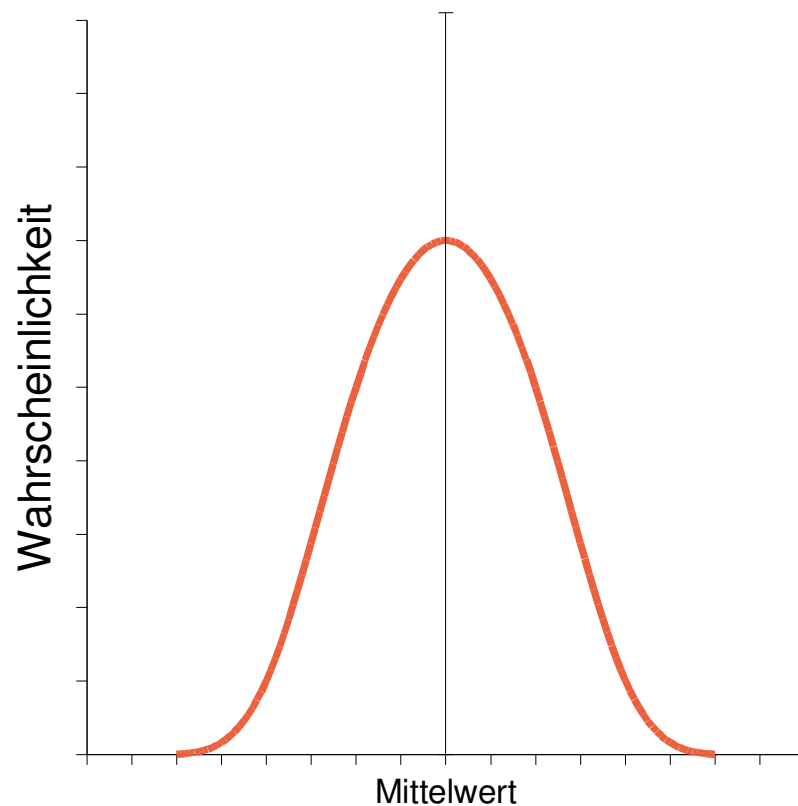
x (mittlere) Eintrittswahrscheinlichkeit

- aber:
 - wann gilt das?
 - Schadensausmaß?
 - Eintrittswahrscheinlichkeit?
 - Schadensverlauf und Beherrschbarkeit???

Was ist Risiko?

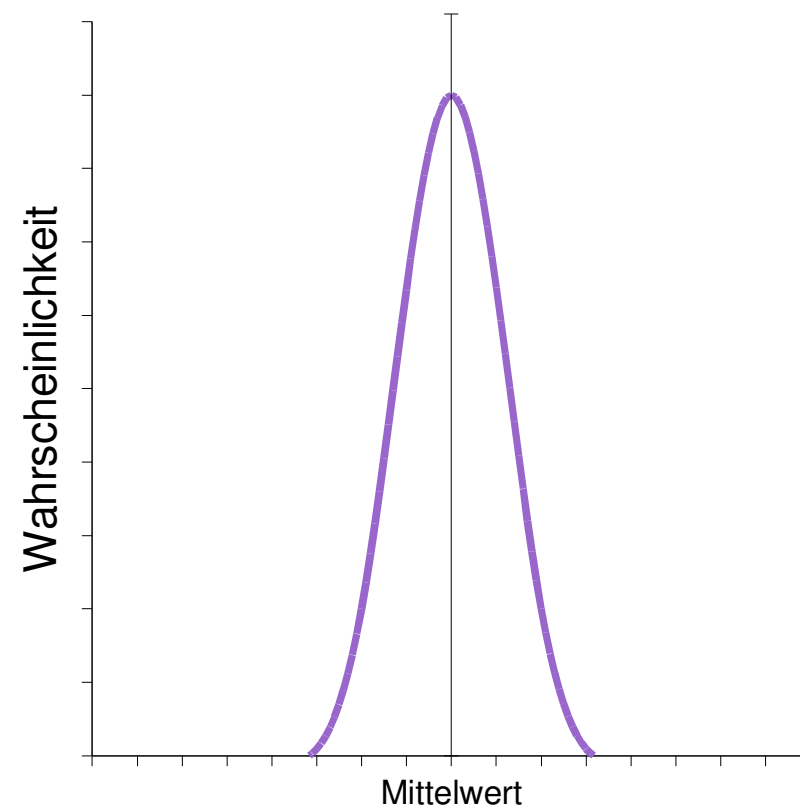
Mathematisch/Ingenieurwissenschaftlich

Schadensausmaß



X

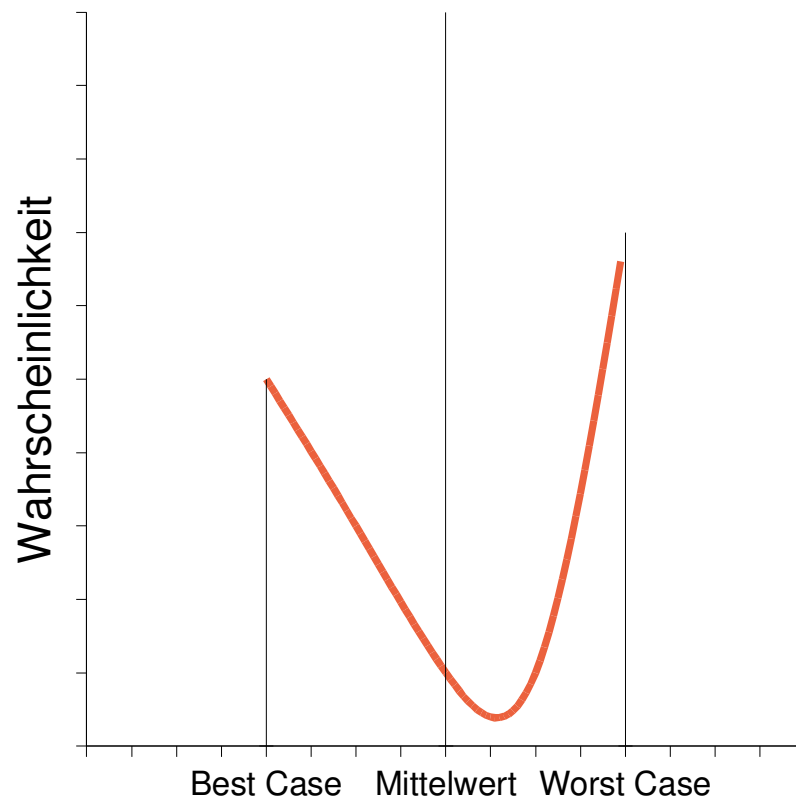
Eintrittshäufigkeit



Was ist Risiko?

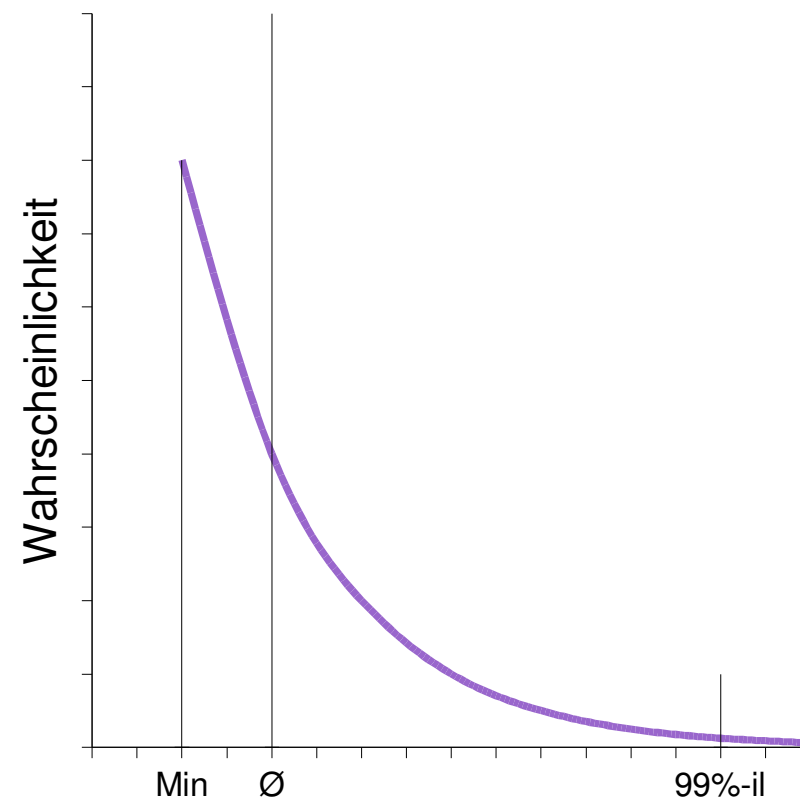
Mathematisch/Ingenieurwissenschaftlich

Schadensausmaß



X

Eintrittshäufigkeit



Was ist Risiko?

Moralisch/Politisch

Beispiel: Friedliche Nutzung der Kernenergie

- Statistisch (BRD):
 - 6–12 Tote/Kernkraftwerk/Jahr
 - ~ 200 Kernkrafttote/a \ll ~ 5000 Verkehrstote/a
- Schadensfall: SuperGAU Hüllenbruch $> 10^7$ a
 - 1–2 Millionen Tote
 - 10–20 Millionen Dauergeschädigte
 - weite Teile 100–200 Jahre unbewohnbar
- Akzeptabel? – Welche Prävention, Reaktion?

Was ist Risiko?

Psychologisch

- Beispiel: Hausbesitzer
 - 100% Beitrag – normale Gebäudeversicherung
 - 120% Beitrag + Elementarschäden
 - 130% Beitrag + Allgefahrenversicherung
- Welchen Versicherungsschutz?
- Begrenztes Budget: lieber
 - Allgefahrengebäude- und kein Hausrat-V oder
 - Normale Gebäude- und Hausrat-V?

Was ist Risiko?

Psychologisch

Saalexperiment – Was würden Sie wählen?

- **500 € Gewinn** / **Münzwurf: nichts oder 1.000 € Gewinn**
- **500 € Verlust** / **Münzwurf: nichts oder 1.000 € Verlust**
- **500 € Gewinn** / **Würfel: 6 = 10.000 € Gewinn**
- **500 € Verlust** / **Würfel: 6 = 10.000 € Verlust**

Was ist Risiko?

Psychologisch

Gedankenexperiment zur IT-Sicherheit:

- Stellen Sie sich Ihren persönlichen GAU vor: Unter denen Zuhörern ohne blauen Hut wird einer ausgelost – den trifft sein persönlicher Gau ...
- Sie können jetzt blaue Hüte kaufen, 50 €.
- **Zweite Chance: Blaue Hüte zu 1.000 € ...**
- **Drei Hüte hab' ich noch. Gebote?**

Was ist Risiko?

Psychologisch

Risiko-Psychologie:

- Chancen und Risiken werden asymmetrisch wahrgenommen
- Tendenz zur Verlustvermeidung
- Auswirkung von Informationsmangel/defiziten
- Wahrnehmbarkeit von Risiken
- Verdrängung von Risiken
- Gruppendynamische Effekte

Ein pragmatisches Modell für Risiko

Anforderungen an das Modell:

- Politische Grundsatzentscheidungen dokumentieren und abbilden
- Psychologischen Effekten entgegen wirken
- sinnvolle Risiko-Arithmetiken ermöglichen
- Schadensausmaß und Eintrittswahrscheinlichkeiten handhabbar machen

Risiko-Modell: Eine Klasse für sich ...

Vorgehensweise:

- Definition von Klassen für
 - Schaden
 - Eintrittshäufigkeit
 - Risiko
- Verwendung von Liebert-Skalen
- Anpassung an Unternehmenssicht

Risiko-Modell: Eine Klasse für sich ...

Risikobewertungstableaux

Szenario

Vorschlag: Zwei unabhängige Firewalls, funktionales Interface zur DB, Grundschutz:

Die Eingabefelder sind **blau** hervorgehoben. Es sollte jeweils ein Grund für die Ent-
Beliebige Texteinträge (z.B. Entscheidungsgründe) stellen die Verbindung zwischen
Die Kalkulationslogik berechnet auf Grundlage der Eingaben die kumulierten techni

Managementperspektive

<i>Gesamtlage</i>		Oops
Vorsorge		4.026
1.932.000 €	###	extremes Risiko

Technisch

<i>Gesamtlage</i>	
Vor- sorge	1.260.300 €
Oops	4.026
	0,00 €
	extremes Risiko

*Prognose-
zeitpunkt*
02.11.03

Risikokultur

Risikobewertungstableaux

Szenario

Ist-Zustand Internet-Portal-zentr

Vorschlag: Zwei unabhängige Firewalls, funktionales Interface zur DB, Grundschutz für Arbeitsplätze

Die Eingabefelder sind blau hervorgehoben. Es sollte jeweils ein Grund für die Entscheidung angegeben werden.

Beliebige Texteinträge (z.B. Entscheidungsgründe) stellen die Verbindung zwischen technischen und geschäftlichen Bedrohungen her.

Die Kalkulationslogik berechnet auf Grundlage der Eingaben die kumulierten technischen und geschäftlichen Einzelrisiken sowie Gesamtrisiken.

Managementperspektive

<i>Gesamtlage</i>		Oops
Vorsorge	1.932.000 €	4.026
	###	extremes Risiko

Technische Perspektive

<i>Gesamtlage</i>	
Vorsorge	1.260.300 €
Oops	4.026
	0,00 €
	extremes Risiko

Prognosezeitpunkt
02.11.03

Äußere Firewall	Web-Server in der DMZ (Web-Portal)	Schwachstellen in der Applikationslogik	Innere Firewall
0,00	0,00	0,00 €	0,00
mittleres Risiko	minimales Risiko	extremes Risiko	minimales Risiko
B	B	B	B
f	h	d	h
W7	W9	W5	W7
0,10000	0,10000	0,10000	0,00000
1,00000	1,00000	1,00000	0,00005
1,00000	1,00000	1,00000	0,00005
500,00000	500,00000	500,00000	0,02268
60.000,00000	60.000,00000	60.000,00000	2,72218
01.01.03	01.01.03	01.04.02	01.01.03

Risikoinventar

- Werte
 - Image
 - Kundendaten
 - Geschäftsdaten
 - Unterstützende Daten- + Funktionsbestände
 - Betriebsgeheimnisse
 - I+K-Ressourcen
 - Produktivität
 - Mitarbeiter
- Prozeßwirkungen
 - Wertschöpfende ...
 - Kostenerzeugende...
 - Rechtswirksame ...
 - Administrative ...
 - Operative Prozesse
 - Sonstige Prozeßwirkg.

Risikoinventar

- Rechtl.+Vertragl. Risiken
 - Bundesdatenschutzgesetz
 - Haftungspflichten (BGB, vertragl.)
 - KonTraG
 - Betriebsverfassungsgesetz
 - Fernmeldegeheimnis
 - Kryptoregulierungen
 - Telekommunikationsdienste-Gesetze
 - ...

Risikostruktur an Beispiel-Szenarien

Zwei Beispielszenarien für Risikobewertung:

- K-Fall-Vorsorge für ein (kleines) fiktives RZ, Vergleich verschiedener Lösungsvarianten hinsichtlich Schutz und Wirtschaftlichkeit
- Sicherheitsanalyse, Vergleich von Sicherheitsarchitekturen, und Wirtschaftlichkeitsbetrachtung der Sicherheitsmaßnahmen

Risikobewertungstableaux

Szenario Ist-Zustand

Vorschlag: Zwei unabhängige Firewalls, funktionales Interface zur DB, Grundschutz für Arbeitsplätze

Die Eingabefelder sind blau hervorgehoben. Es sollte jeweils ein Grund für die Entscheidung angegeben werden w
Beliebige Texteinträge (z.B. Entscheidungsgründe) stellen die Verbindung zwischen technischen und gesch
Die Kalkulationslogik berechnet auf Grundlage der Eingaben die kumulierten technischen und geschäftliche

Managementperspektive

<i>Gesamtlage</i>		Oops
Vorsorge		4.026
1.932.000 €	###	extremes Risiko

Technische Perspektive

<i>Gesamtlage</i>	
Vor-sorge	1.260.300 €
Oops	4.026
	0,00 €
	extremes Risiko

Äußere Firewall
0,00
mittleres Risiko
B
f
W7
0,10000

Prognosezeitpunkt
02.11.03

A-Risk-Methics

Ein Blick hinter die Kulissen:

- Schaurige Formeln in wohlweislich versteckten Zellen

Aus- und Rückblick

- Interview-Technik und resultierende Tabellen werden von Management und Technikern als hilfreich befunden.
- Viele Fragestellungen können nach Initialaufwand effizient beleuchtet werden.
- Graphisches Werkzeug und etwas ausführlichere mathematische Modellierung wären wünschenswert.

Ende

Vielen Dank für Ihre Aufmerksamkeit!

Für Fragen:

thomas.maus@alumni.uni-karlsruhe.de