

T.I.S.P. Community Meeting

Frankfurt a.M., 10. - 11.11.2016

Risikomanagement

Knapp vorbei ist auch daneben: Wo wir beim (...) seit Jahren unbemerkt am Ziel vorbeischießen

Sebastian Klipper

CycleSEC - Exzellenz und Wissenstransfer

Sebastian Klipper

CycleSEC GmbH, Gründer und CEO

Fachbuchautor bei Springer Vieweg und Beuth

Kursautor an der Wilhelm Büchner Hochschule

15 Jahre 100% IT-Security

Risikomanagement: Drei zentrale Fehlercluster

Zeit

- In diesem Vortrag nur kurz vorgestellt...*

Adaption

- In diesem Vortrag nur kurz vorgestellt...*

Mathematik

- Schwerpunkt in diesem Vortrag*

* Weitere Folien finden Sie in der Dokumentation

Risikomanagement: Weitere Fehlercluster

Abstützung auf
Angriffs- statt auf
Verteidigungsszenarien

Keine
Berücksichtigung
der Risikorentabilität

Die Probleme der Zeit

Fehlende Datenbasis

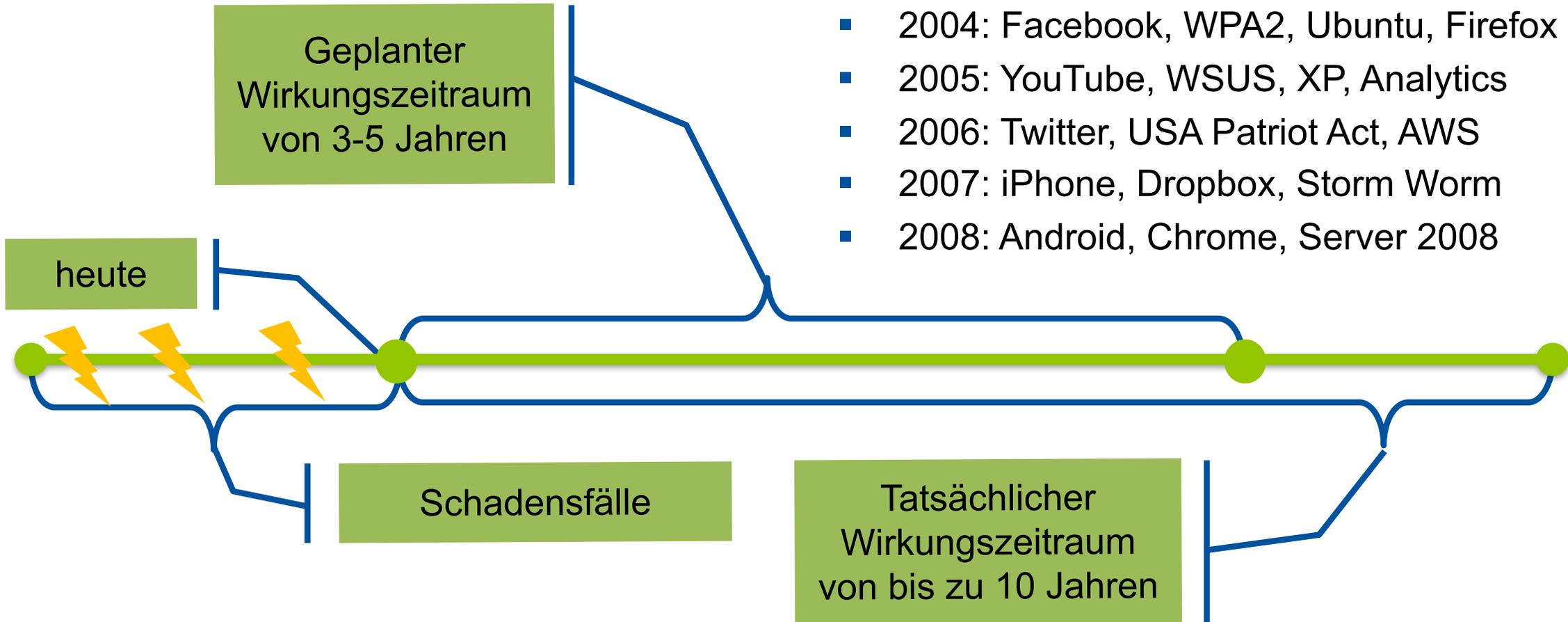
Technischer Fortschritt

- Fehler: Wir schließen aus der Vergangenheit in die Zukunft.
- Fehler: Wir arbeiten mit gleichverteilten Wahrscheinlichkeiten.

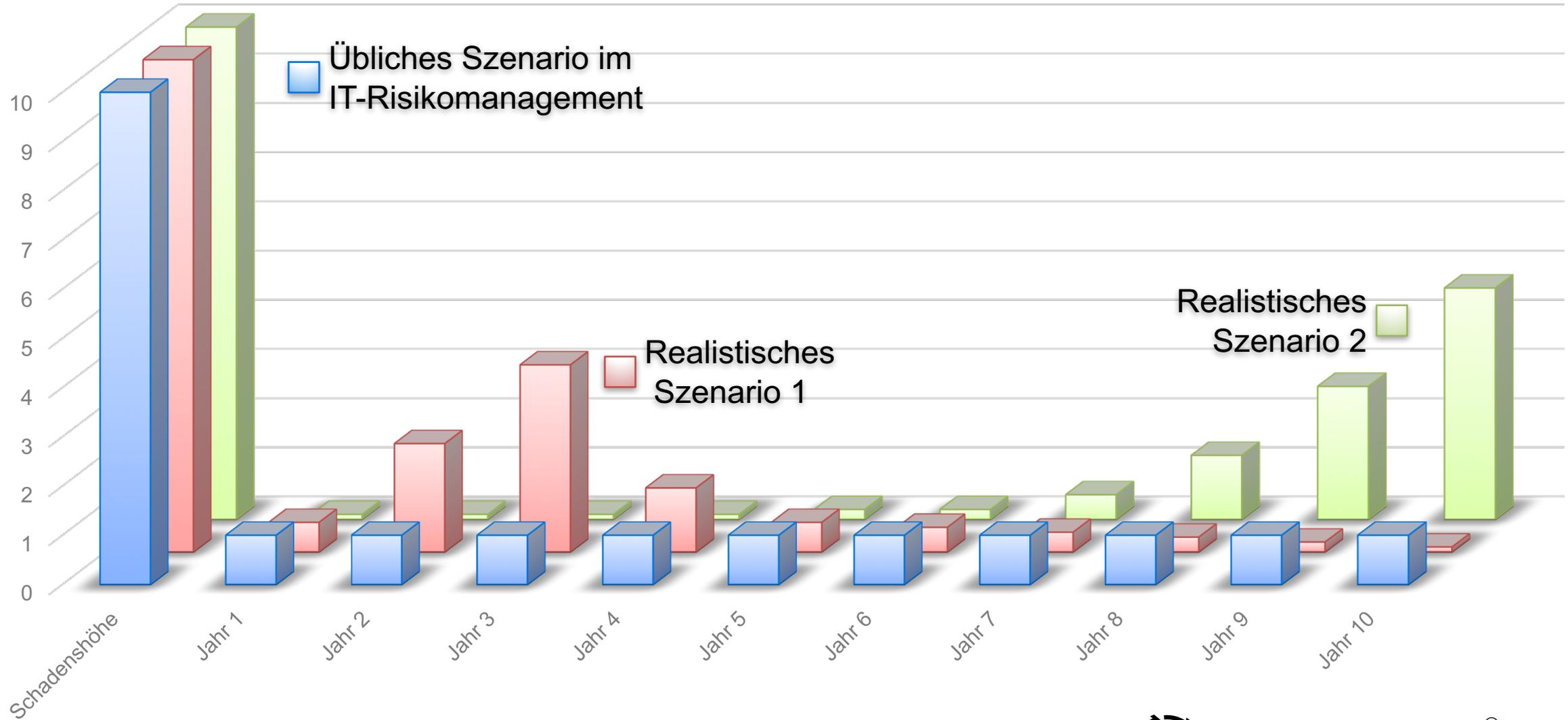
Fehlende Datenbasis

10 Jahre zurück...

- 2004: Facebook, WPA2, Ubuntu, Firefox
- 2005: YouTube, WSUS, XP, Analytics
- 2006: Twitter, USA Patriot Act, AWS
- 2007: iPhone, Dropbox, Storm Worm
- 2008: Android, Chrome, Server 2008



Gleichverteilung des Risikos

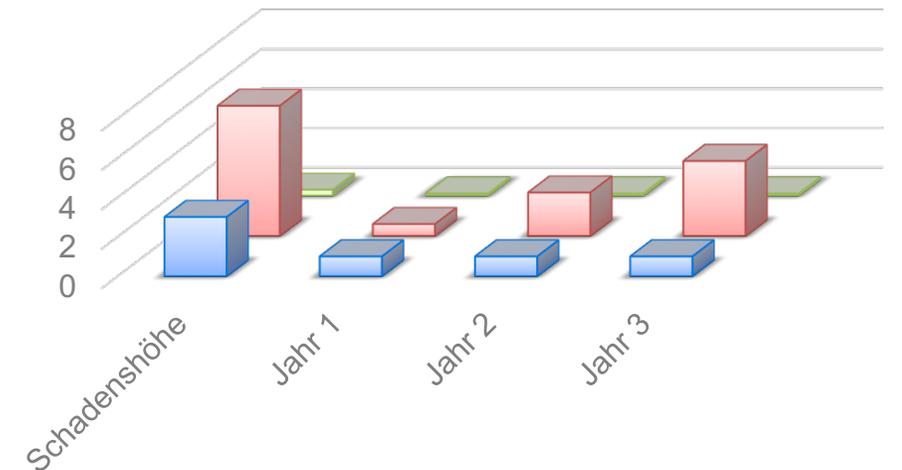
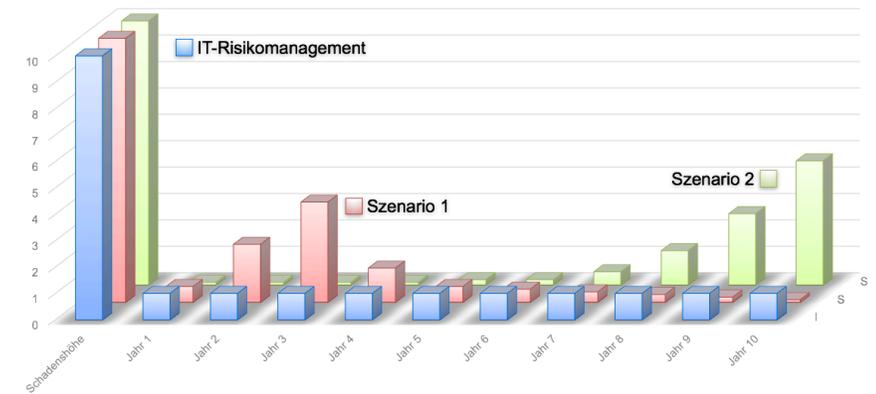


Falsche Bezugsgröße

- IT-relevanter Zeitraum
 - maximal 1 - 3 Jahre
 - auch bei $P(A) < 0,33$

- ungeeignet:
 - Wahrscheinlichkeit auf Zeit

- besser:
 - Wahrscheinlichkeit innerhalb einer Vergleichsgruppe



Die Probleme der Adaption

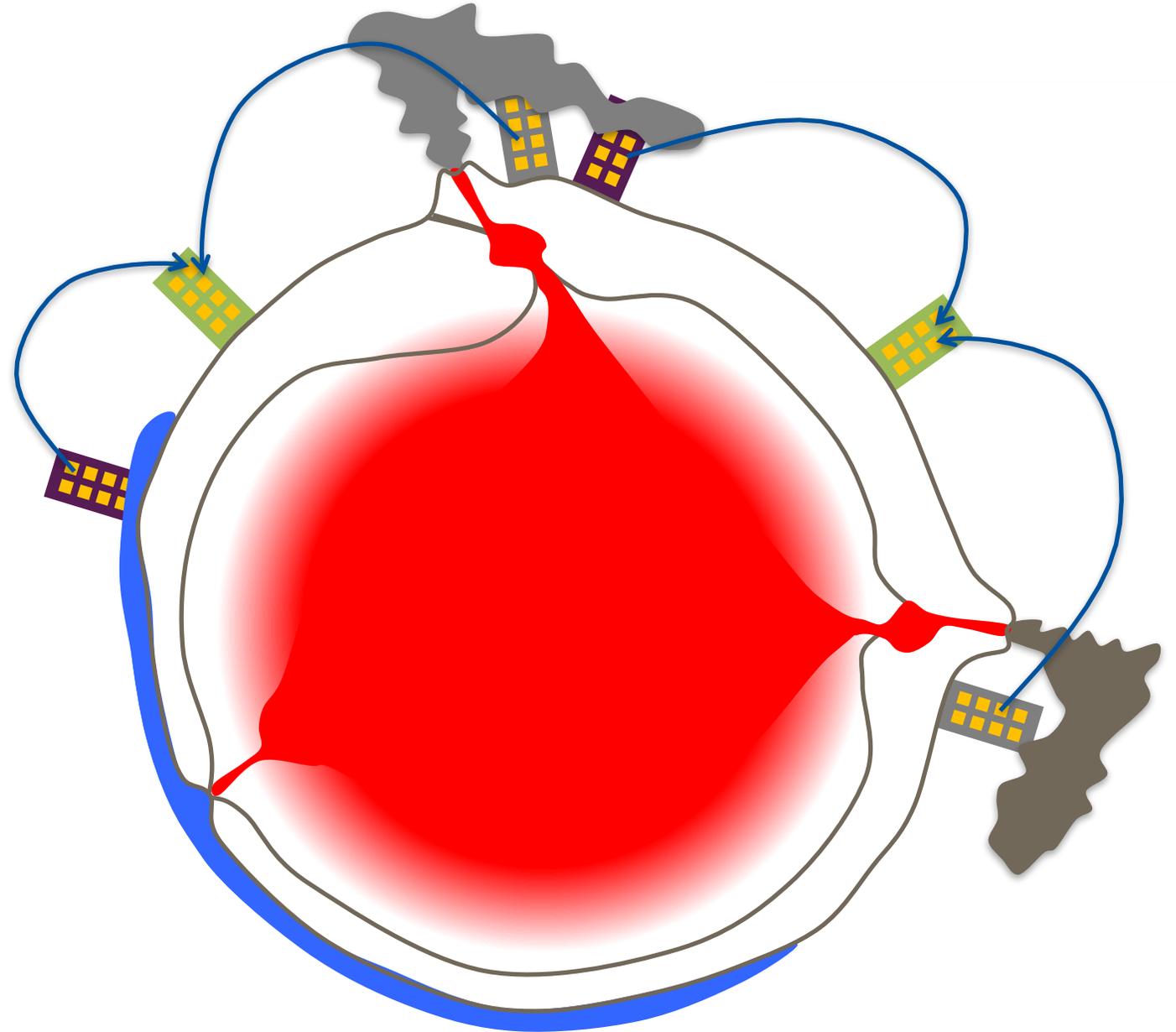
...der Angreifer

...der Verteidiger

- Fehler: Wir hoffen auf entnervte, unmotivierte Angreifer.
- Fehler: Wir vernachlässigen unsere eigene Resilienz.

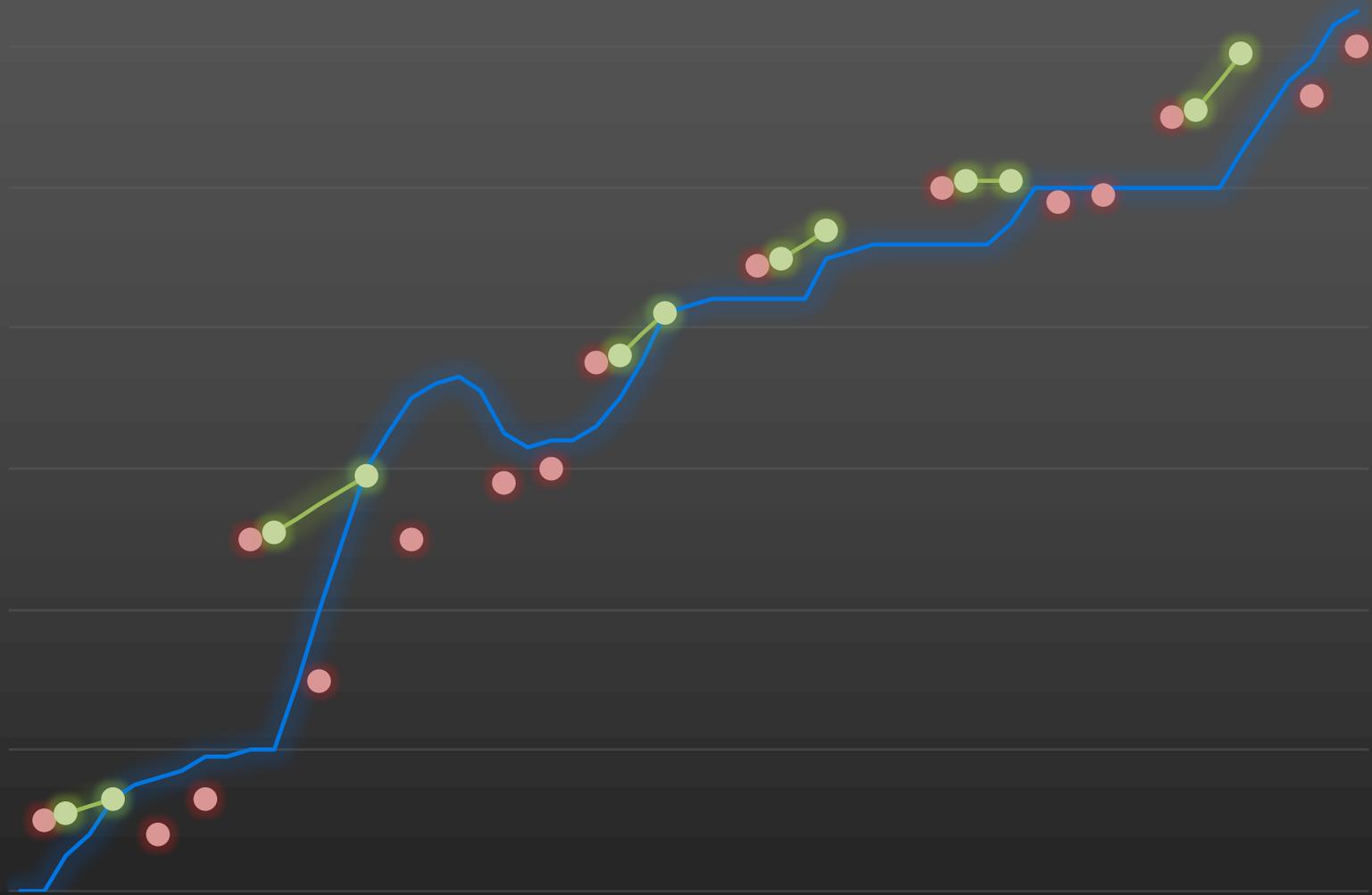
Wenn der Erdkern ein Hacker wäre...

...würde er wissen, wohin man zieht und sein Verhalten adaptieren!

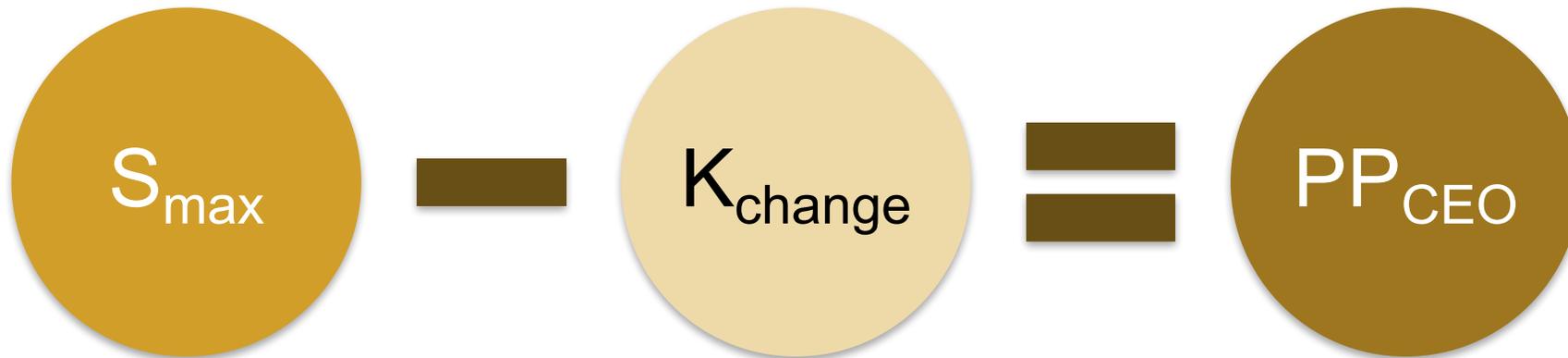


Schema der Adaption von Angreifern und Verteidigern

- Sicherheitsniveau geplant
- IT-Sicherheitsvorfälle
- Ad-hoc-Sicherheitsmaßnahmen



Schwellwerte für Risikoentscheidungen



- S_{\max} = Maximalschaden vor Liquiditätskollaps
- K_{change} = Kosten eines Kurswechsels
- PP_{CEO} = PainPoint des CEO bei fortgesetzten Schadensszenarien

Probleme der Mathematik

Additionsproblem

Skalenproblem

Matrizenproblem

- Fehler: Wir haben in Mathe nicht aufgepasst.
- Fehler: Scheingenauigkeit durch fehlerhafte Risikomatrizen.
 - Siehe Risiko-Isoquanten-Analyse <kes> Nr. 2 / 2016
 - oder hier: <https://cyclesec.com/2016/07/11/risiko-isoquanten-analyse-ria/>

Das Additionsproblem

Grenzschaden

- Manche Schäden werden von Vorfall zu Vorfall kleiner.

Kontravalente Szenarien

- Szenarien schließen sich gegenseitig aus.

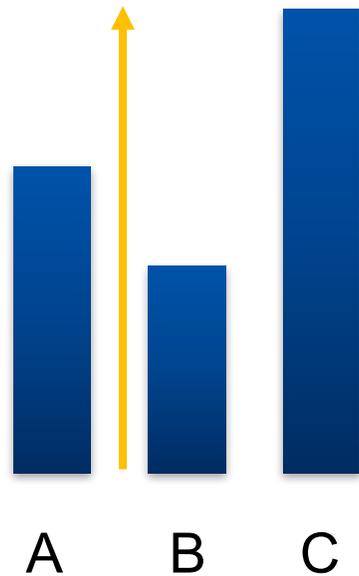
Boiling Frog Syndrom

- Fortgesetzte Szenarien können unterbrochen werden.

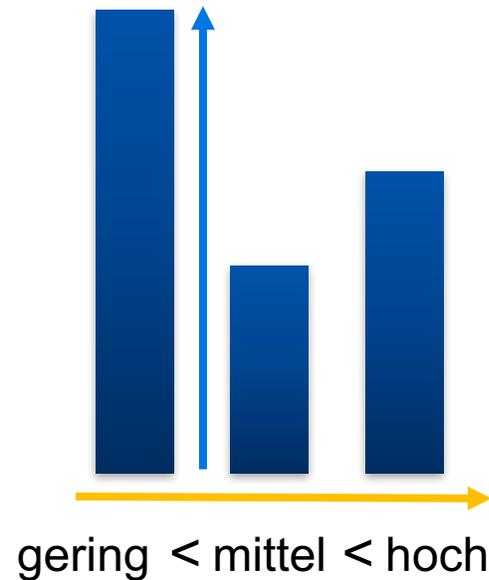
Einzelrisiken können nicht ohne Weiteres addiert werden.

Das Skalenproblem

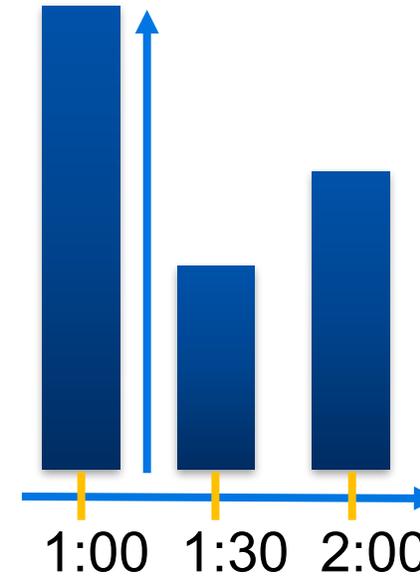
Nominalskala



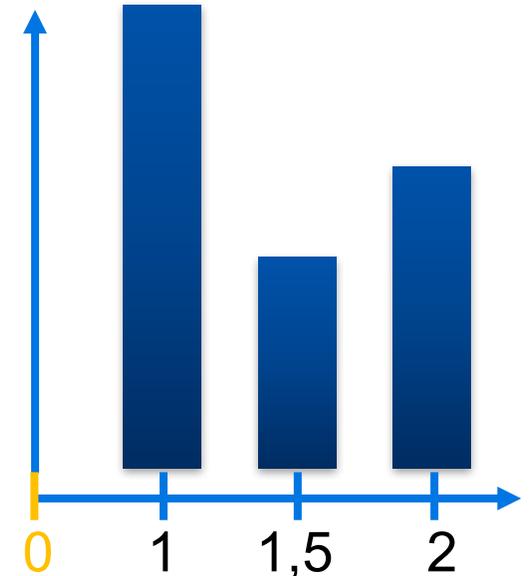
Ordinalskala



Intervallskala



Verhältnisskala

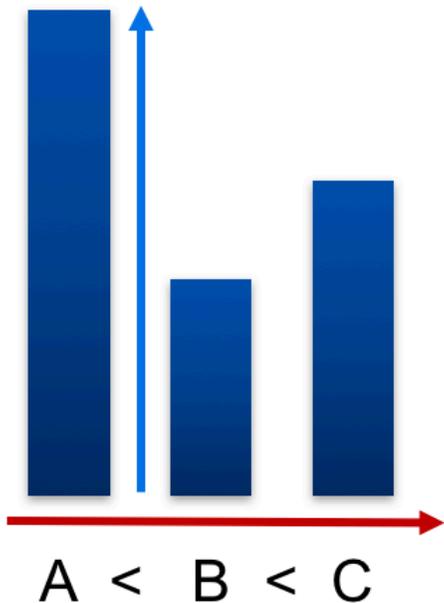


Orange: Die auf diesem Skalenniveau jeweils neu hinzugekommenen Eigenschaften.

Nominal: nur Häufigkeiten, ordinal: Reihenfolge, intervall: Abstände, verhältnisskaliert: Nullpunkt

Das Skalenproblem am Beispiel von Schulnoten

Ordinalskala



- Sehr gut, gut, befriedigend, ausreichend, mangelhaft, ungenügend
 - Ordinalskala
 - Möglich:
 - Häufigkeitsdarstellungen
 - Median (halbiert eine Verteilung)
 - Nicht möglich:
 - Durchschnitt
- 1, 2, 3, 4, 5, 6
 - Scheinbar intervallskaliert
 - ist aber immer noch Ordinalskala
 - Größe des Abstandes zwischen zwei Werten lässt sich nicht sachlich begründen.
 - Eine 2 ist z.B. nicht doppelt so gut wie ein 4.



- Business Impact
 - Nur Schäden sind business-critical.
 - Wahrscheinlichkeit sind nicht business-critical!
- Auch wenn wir Multiplizieren:
 - Nur die Rechenoperation ist kommutativ.
 - Die reale Welt nicht!

■ International anerkanntes Verfahren

- ISO/IEC 27005 Annex E
- ISO/IEC 31010 Annex B29
- BSI IT-Grundschutz

Table E.1 b)

		Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low		0	1	2	3	4
	Low		1	2	3	4	5
	Medium		2	3	4	5	6
	High		3	4	5	6	7
	Very High		4	5	6	7	8

Likelihood rating	E	IV	III	II	I	I	I
	D	IV	III	III	II	I	I
	C	V	IV	III	II	II	I
	B	V	IV	III	III	II	I
	A	V	V	IV	III	II	II
			1	2	3	4	5

Consequence rating

Figure B.15 – Part example of a probability criteria matrix

MATRIX ZUR RISIKOBEWERTUNG

Wahrscheinlichkeit	Auswirkung/Schaden			
	Niedrig	Mittel	Hoch	Sehr hoch
Sehr wahrscheinlich	gering	mittel	hoch	sehr hoch
Wahrscheinlich	gering	mittel	hoch	hoch
Möglich	gering	gering	mittel	mittel
Unwahrscheinlich	gering	gering	gering	gering

Risiko-Isoquanten-Analyse (RIA) und Vorstellung des Risiko-Stacks

Durchführung und Ergebnisse anhand einer Beispiel-Matrix

Übersicht mehrerer Isoquanten des Risikos

$f(x)=0,1/x$ Risiko = 0,1 Mio.

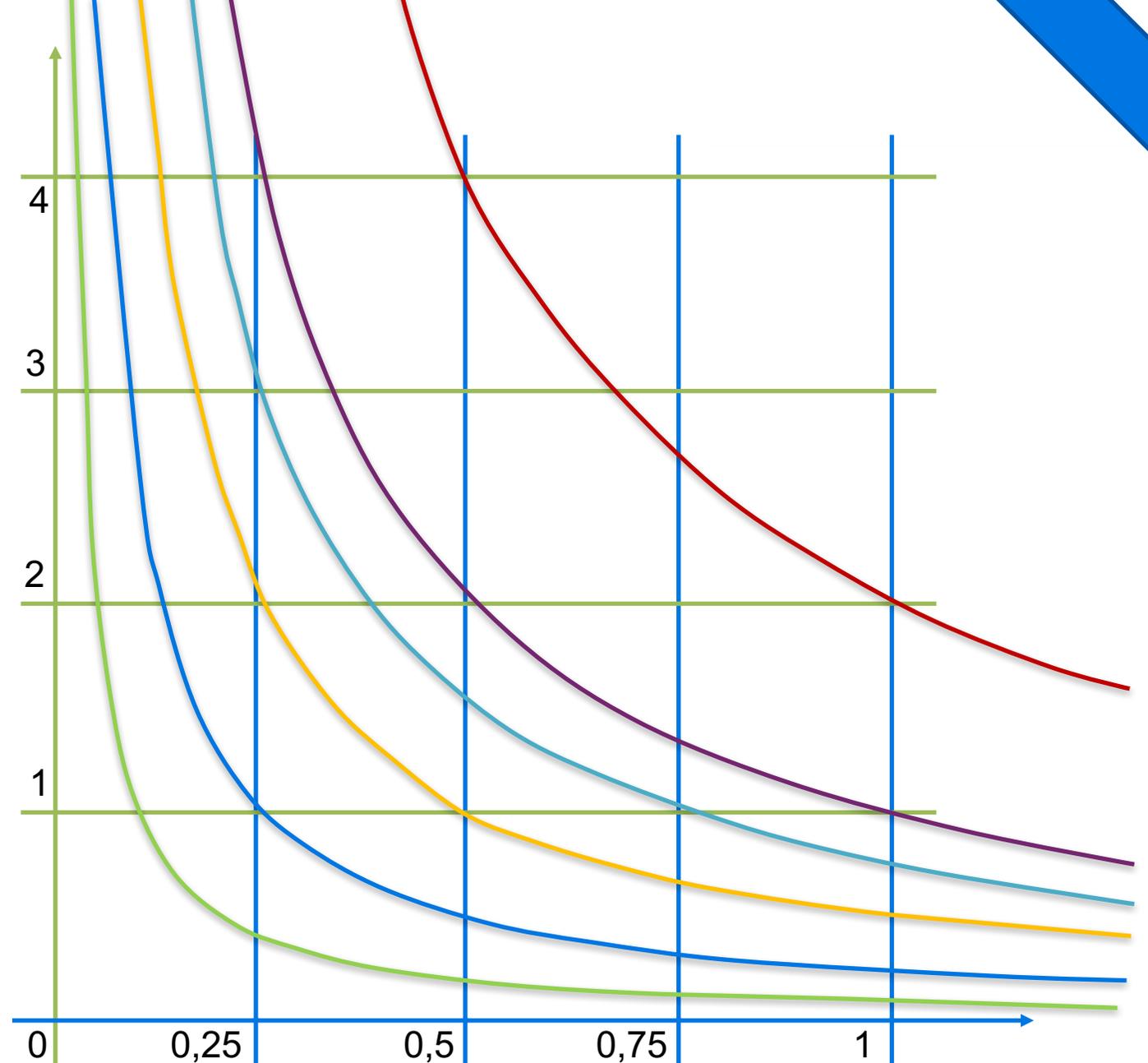
$g(x)=0,25/x$ Risiko = 0,25 Mio.

$h(x)=0,5/x$ Risiko = 0,5 Mio.

$i(x)=0,75/x$ Risiko = 0,75 Mio.

$j(x)=1/x$ Risiko = 1 Mio.

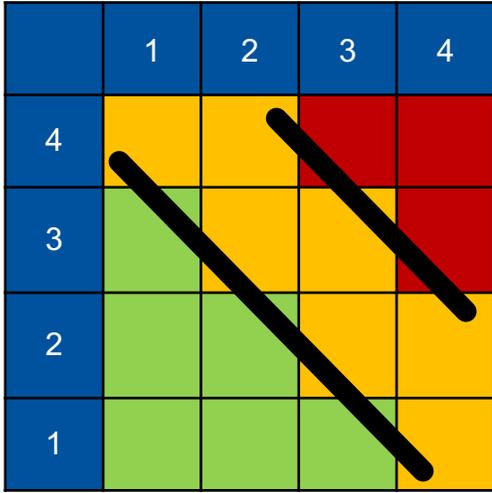
$k(x)=2/x$ Risiko = 2 Mio.



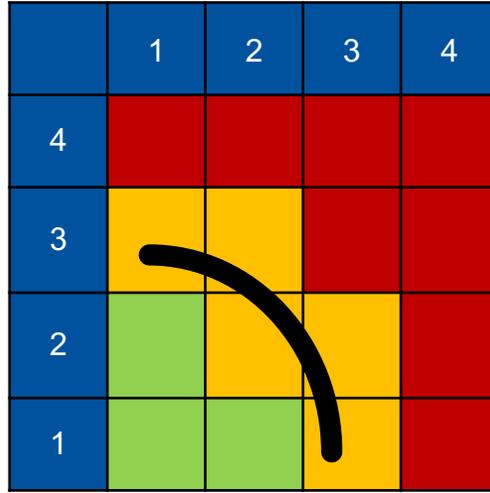
Beispiel einer Risikomatrix

Risikomatrix	Unwahrscheinlich 0 - 1 pro 10 J	Möglich 1 - 2 pro 10 J	Wahrscheinlich 2 - 5 pro 10 J	Sehr wahrscheinlich 5 - 10 pro 10 J
Sehr hoch >2.500.000	mittel	hoch	hoch	hoch
Hoch <2.500.000 >1.000.000	mittel	mittel	mittel	hoch
Mittel <1.000.000 >250.000	gering	gering	mittel	mittel
Gering <250.000	gering	gering	gering	mittel

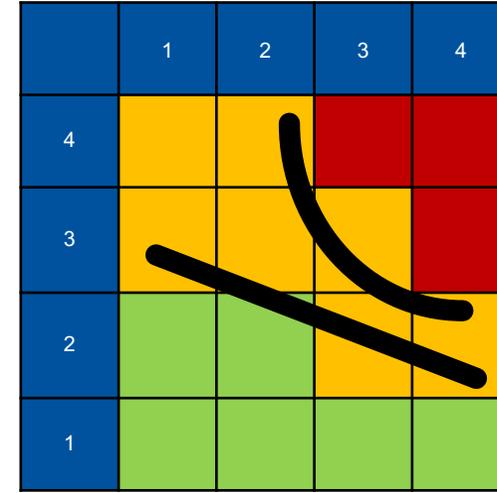
Beispiele gängiger Fehler



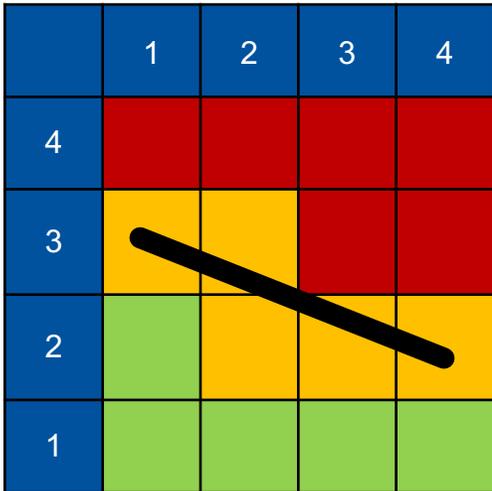
Verwendung der Diagonalen



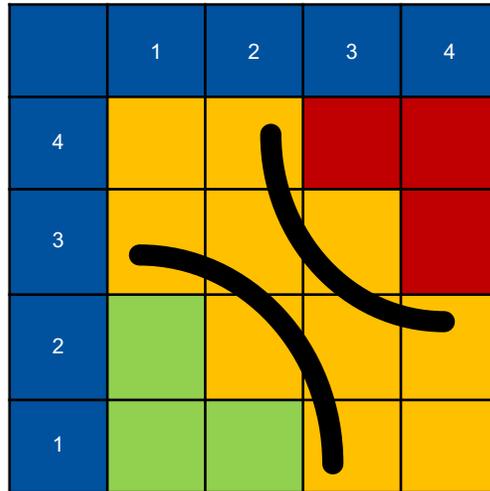
Verwendung eines Kreisbogens



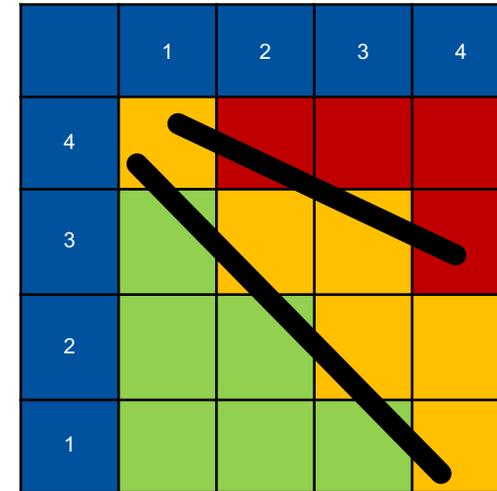
Kombination aus Diagonale und Kreisbogen



Verwendung einer Diagonalen

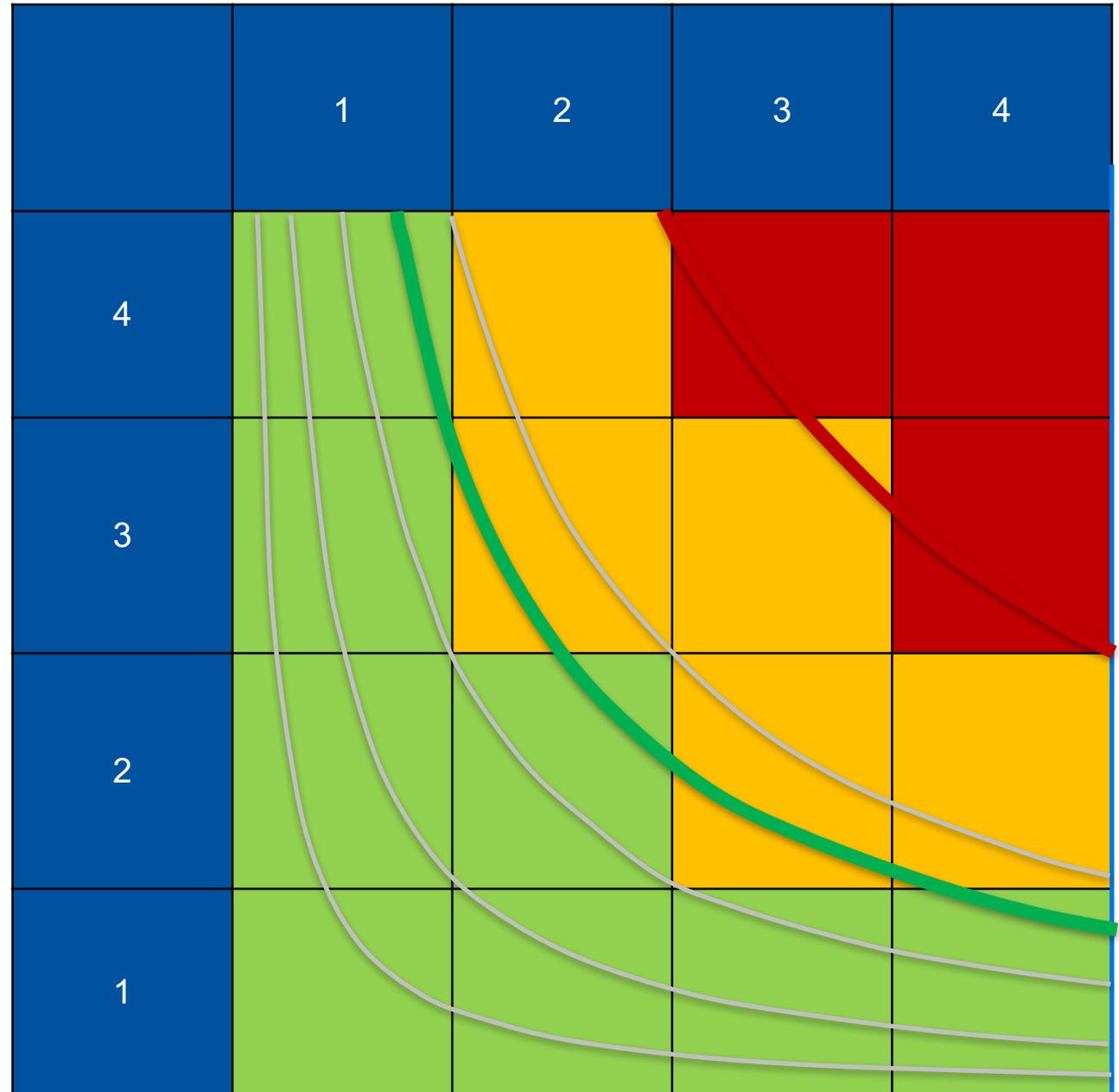


Verwendung gegensätzlicher Kreisbögen



Kombination verschiedener Diagonalen

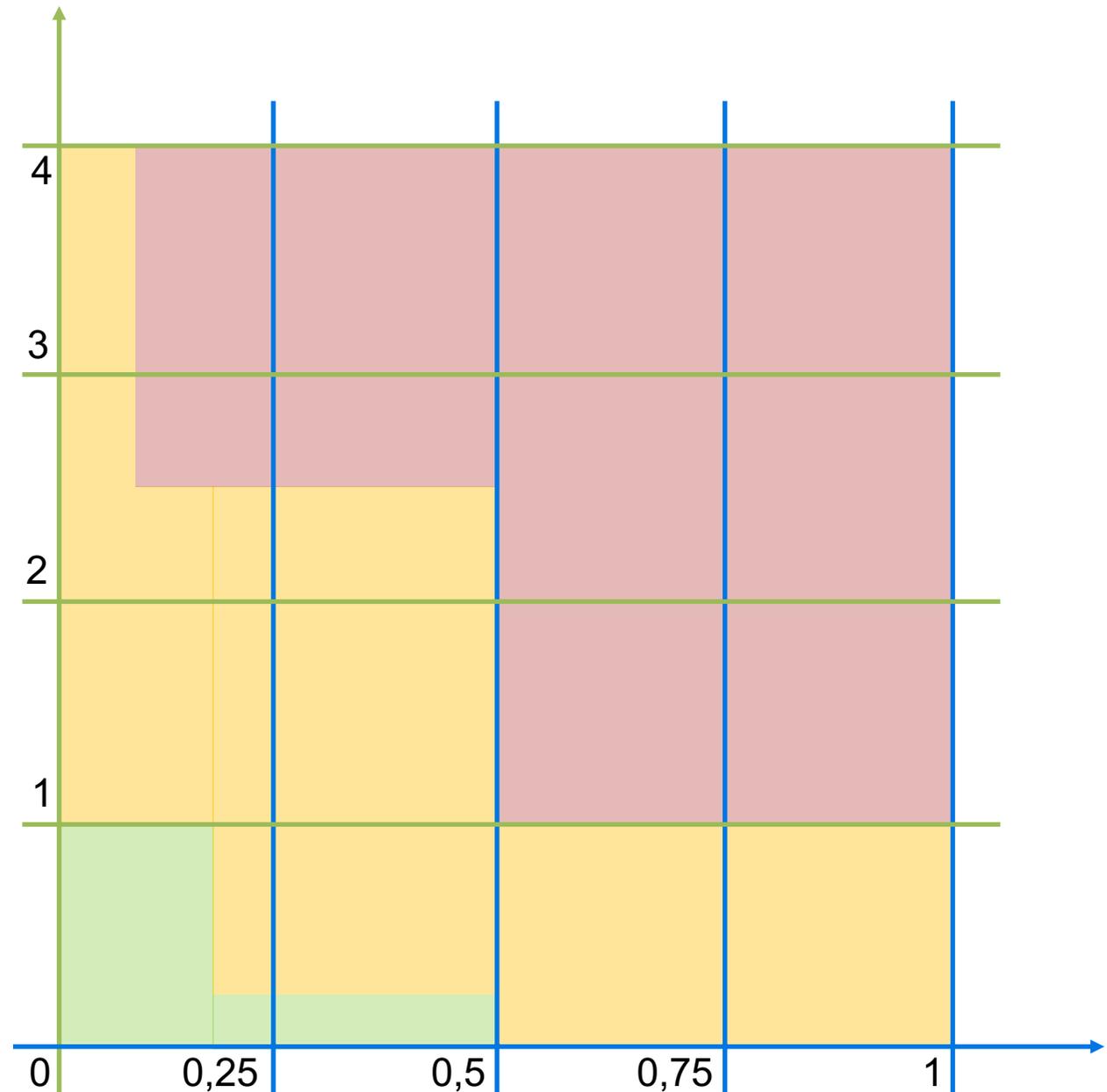
Festlegung entlang der Risiko-Isoquanten



Übertragung ins Koordinatensystem

Schadenshöhe und Wahrscheinlichkeit in einem Koordinatensystem mit Bildung von Risikoklassen

Risikomatrix	Unwahrscheinlich 0 - 1 pro 10 J	Möglich 1 - 2 pro 10 J	Wahrscheinlich 2 - 5 pro 10 J	Sehr wahrscheinlich 5 - 10 pro 10 J
Sehr hoch >2.500.000	mittel	hoch	hoch	hoch
Hoch <2.500.000 >1.000.000	mittel	mittel	mittel	hoch
Mittel <1.000.000 >250.000	gering	gering	mittel	mittel
Gering <250.000	gering	gering	gering	mittel



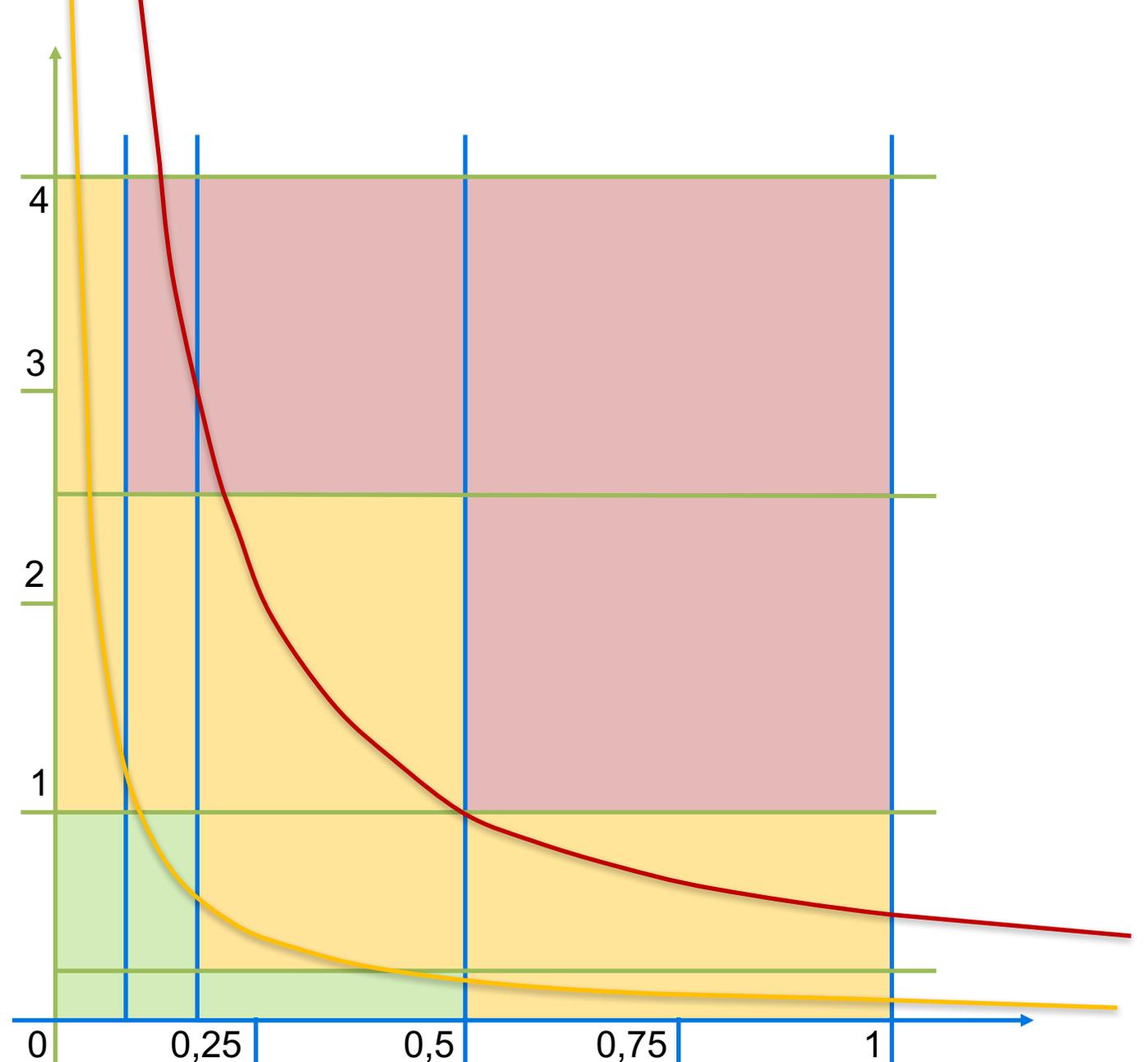
Übertragung ins Koordinatensystem

Schadenshöhe und Wahrscheinlichkeit in einem Koordinatensystem mit Bildung von Risikoklassen

Isoquanten des Risikos

$f(x)=0,1/x$ Risiko = 0,1 Mio.

$h(x)=0,5/x$ Risiko = 0,5 Mio.



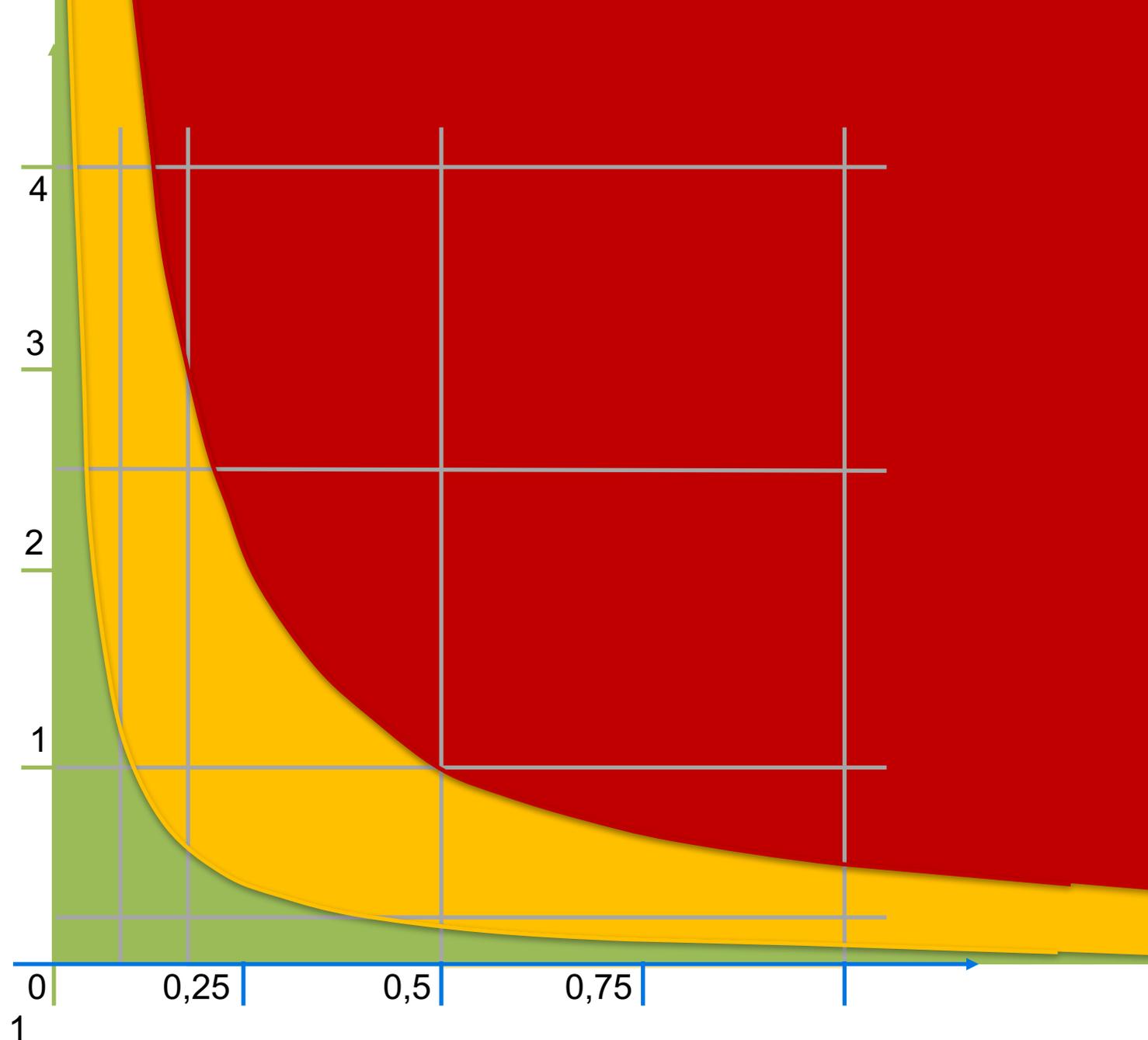
Übertragung ins Koordinatensystem

Schadenshöhe und Wahrscheinlichkeit in einem Koordinatensystem mit Bildung von Risikoklassen

Isoquanten des Risikos

$f(x)=0,1/x$ Risiko = 0,1 Mio.

$h(x)=0,5/x$ Risiko = 0,5 Mio.



Das Matrizenproblem

Risikomatrix	Unwahrscheinlich 0 - 1 pro 10 J	Möglich 1 - 2 pro 10 J	Wahrscheinlich 2 - 5 pro 10 J	Sehr wahrscheinlich 5 - 10 pro 10 J
Sehr hoch >2.500.000	mittel	hoch	hoch	hoch
Hoch <2.500.000 >1.000.000	mittel	mittel	mittel	hoch
Mittel <1.000.000 >250.000	gering	gering	mittel	mittel
Gering <250.000	gering	gering	gering	mittel

Das Matrizenproblem (Details)

Risikomatrix	Unwahrscheinlich 0 - 1 pro 10 J	Möglich 1 - 2 pro 10 J	Wahrscheinlich 2 - 5 pro 10 J	Sehr wahrscheinlich 5 - 10 pro 10 J
Sehr hoch >2.500.000	< 0,4 Mio.	> 0,25 Mio. < 0,8 Mio.	> 0,5 Mio. < 2 Mio.	> 1,25 Mio. < 4 Mio.
Hoch <2.500.000 >1.000.000	< 0,25 Mio.	> 0,1 Mio. < 0,5 Mio.	> 0,2 Mio. < 1,25 Mio.	> 0,5 Mio. < 2,5 Mio.
Mittel <1.000.000 >250.000	< 0,1 Mio.	> 0,025 Mio. < 0,2 Mio.	> 0,05 Mio. < 0,5 Mio.	> 0,125 Mio. < 1 Mio.
Gering <250.000	< 0,025 Mio.	< 0,05 Mio.	< 0,125 Mio.	< 0,25 Mio.

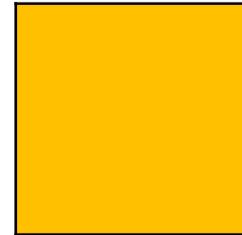
Elemente der Risiko-Matrix

5 Möglichkeiten für
16 Matrix-Zellen

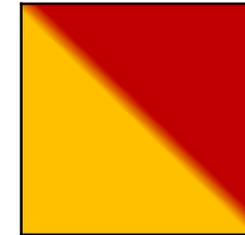
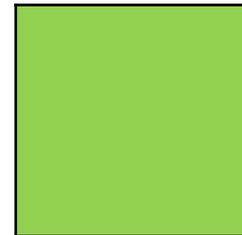
Risiken zwischen
0,5 und 4 Mio.



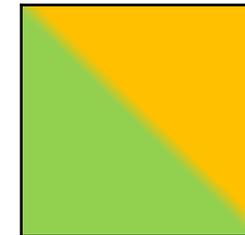
Risiken zwischen
0,05 und 0,5 Mio.



Risiken bis
0,125 Mio.



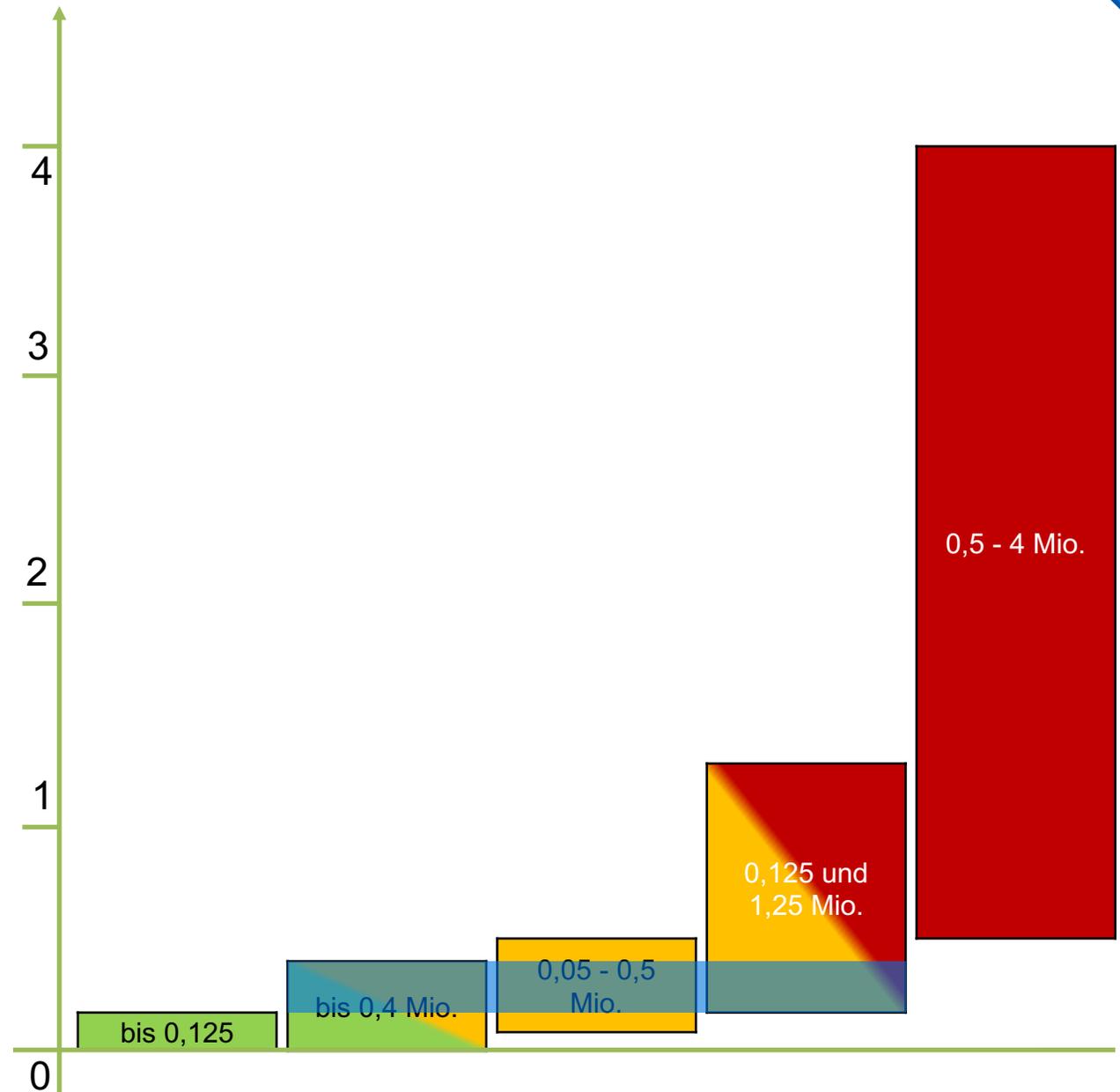
Risiken zwischen
0,125 und 1,25 Mio.



Risiken bis 0,4 Mio.

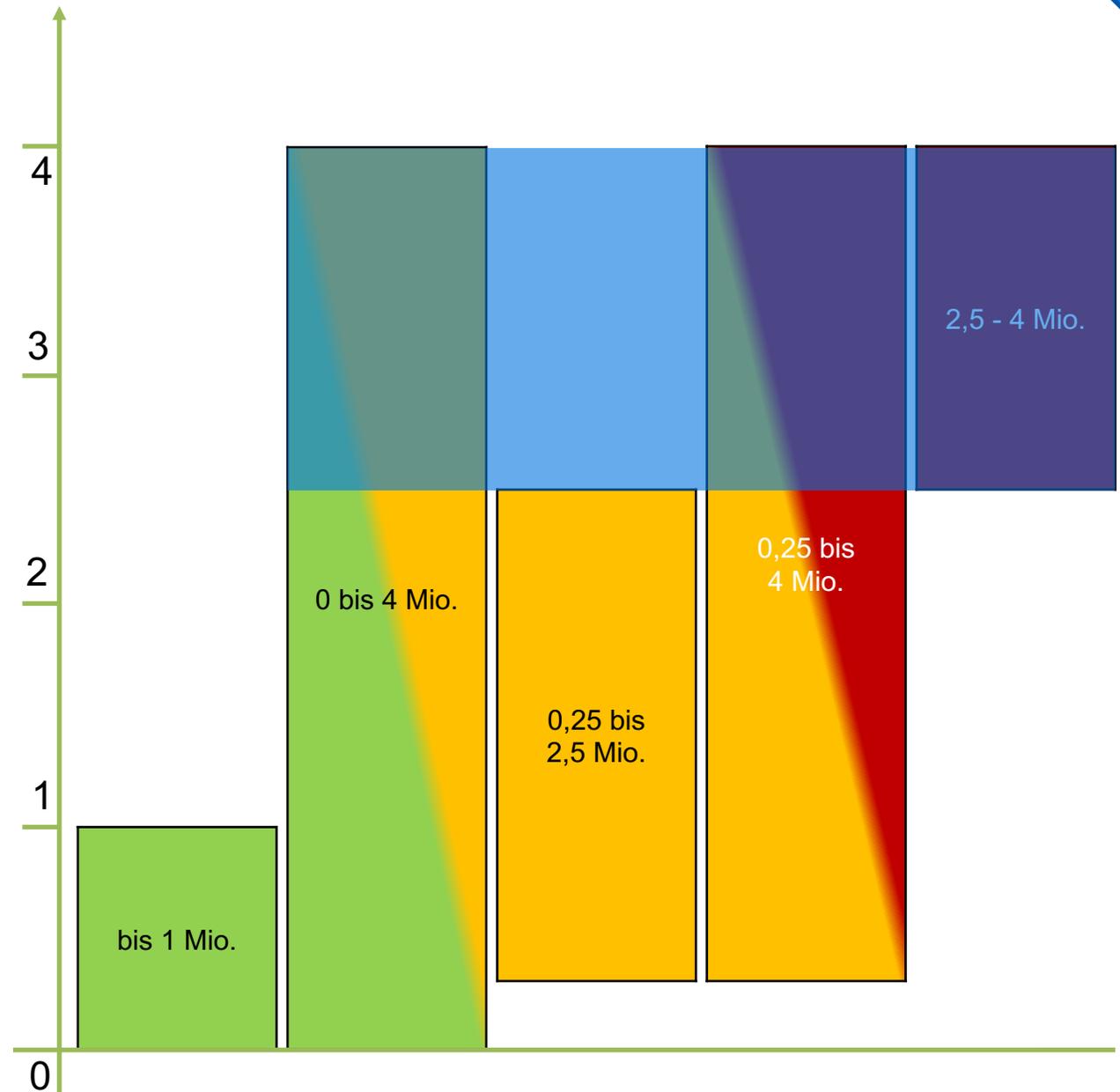
Das Matrizenproblem

Elemente der Risiko-Matrix
sortiert nach Risiko-Höhe



Das Matrizenproblem

Elemente der Risiko-Matrix
sortiert nach Schadenshöhe

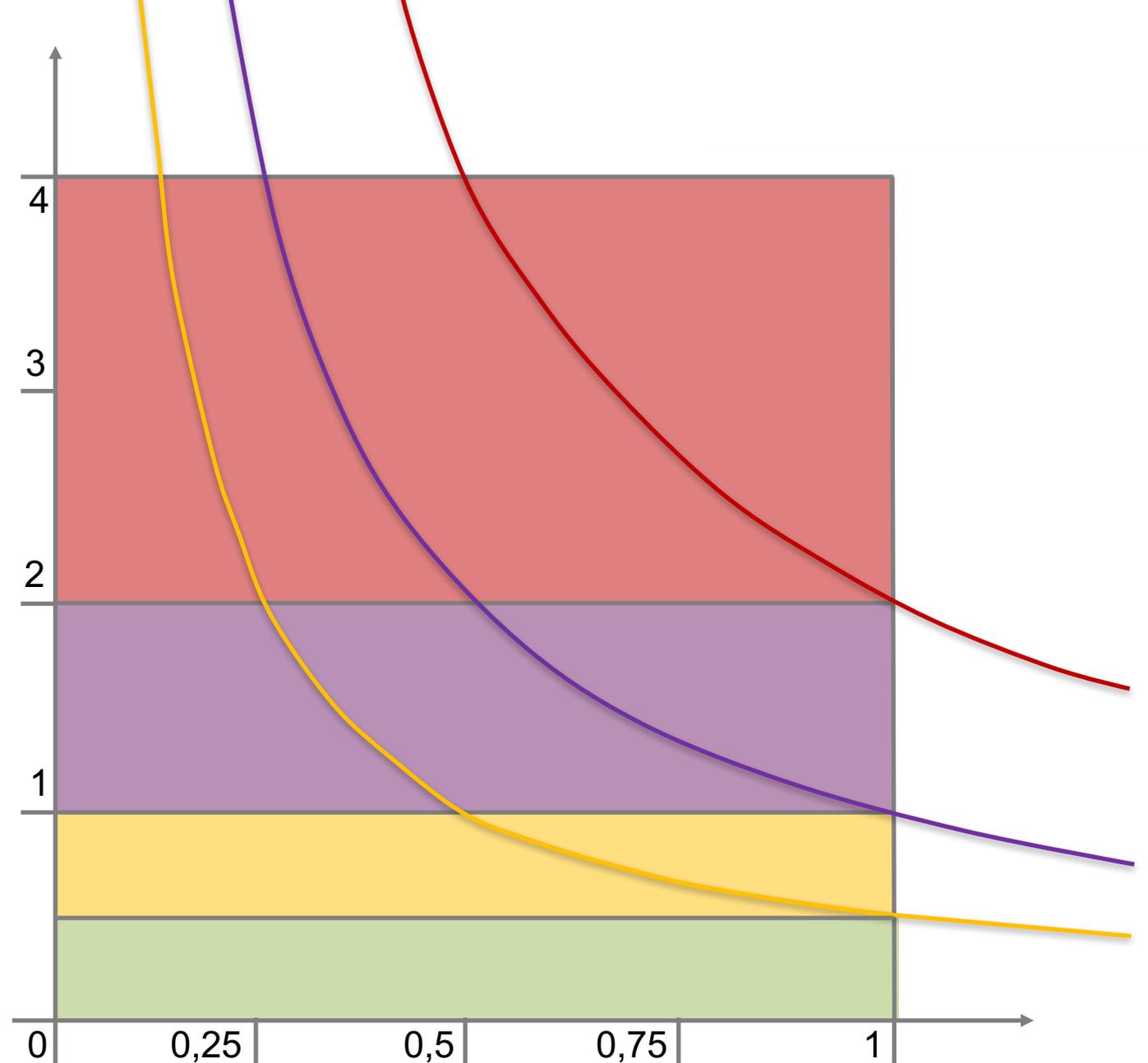


Die Lösung des Matrizenproblems

$k(x)=2/x$ Risiko = 2 Mio.

$j(x)=1/x$ Risiko = 1 Mio.

$h(x)=0,5/x$ Risiko = 0,5 Mio.

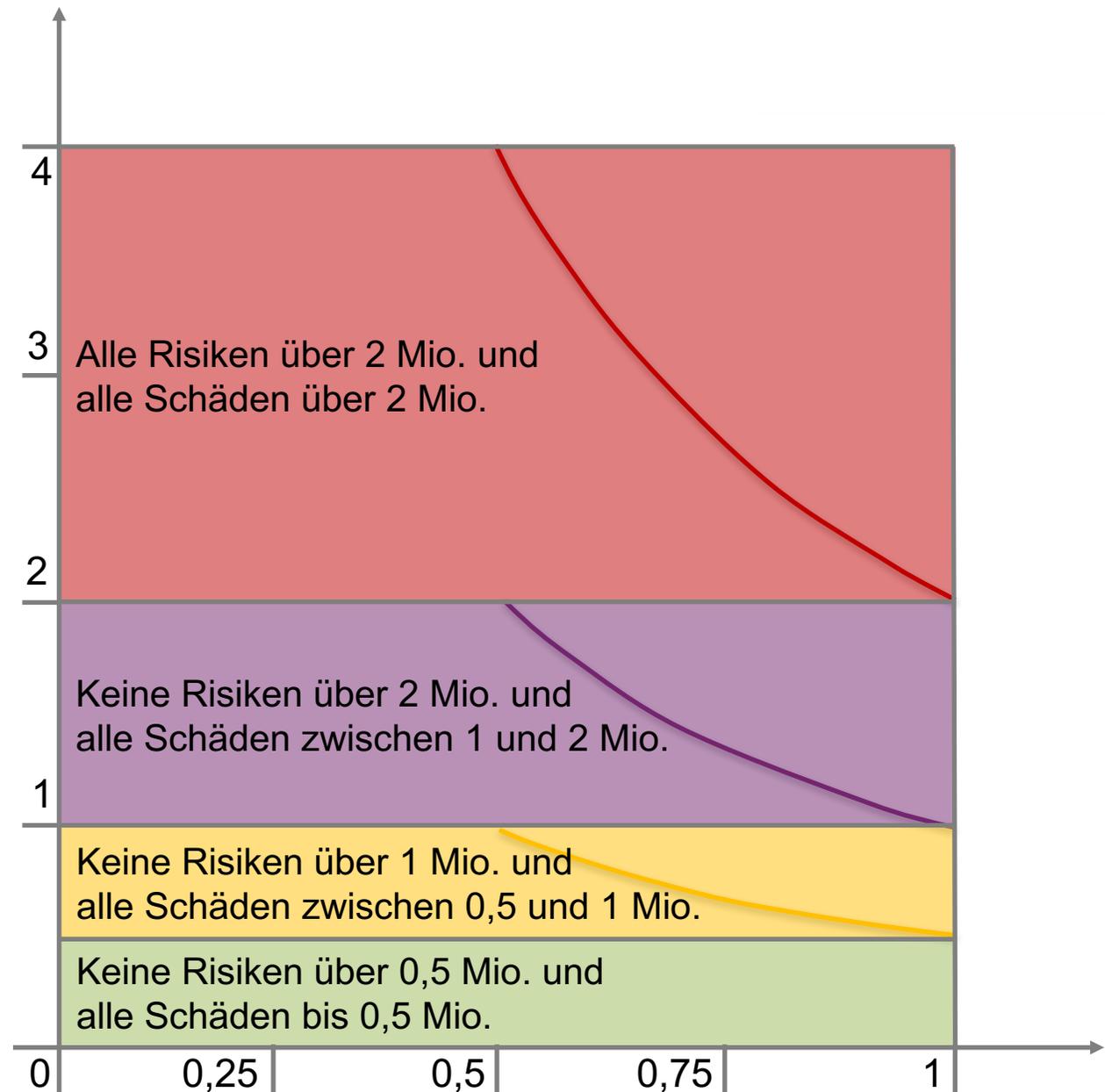


Die Lösung des Matrizenproblems: Der Risiko-Stack

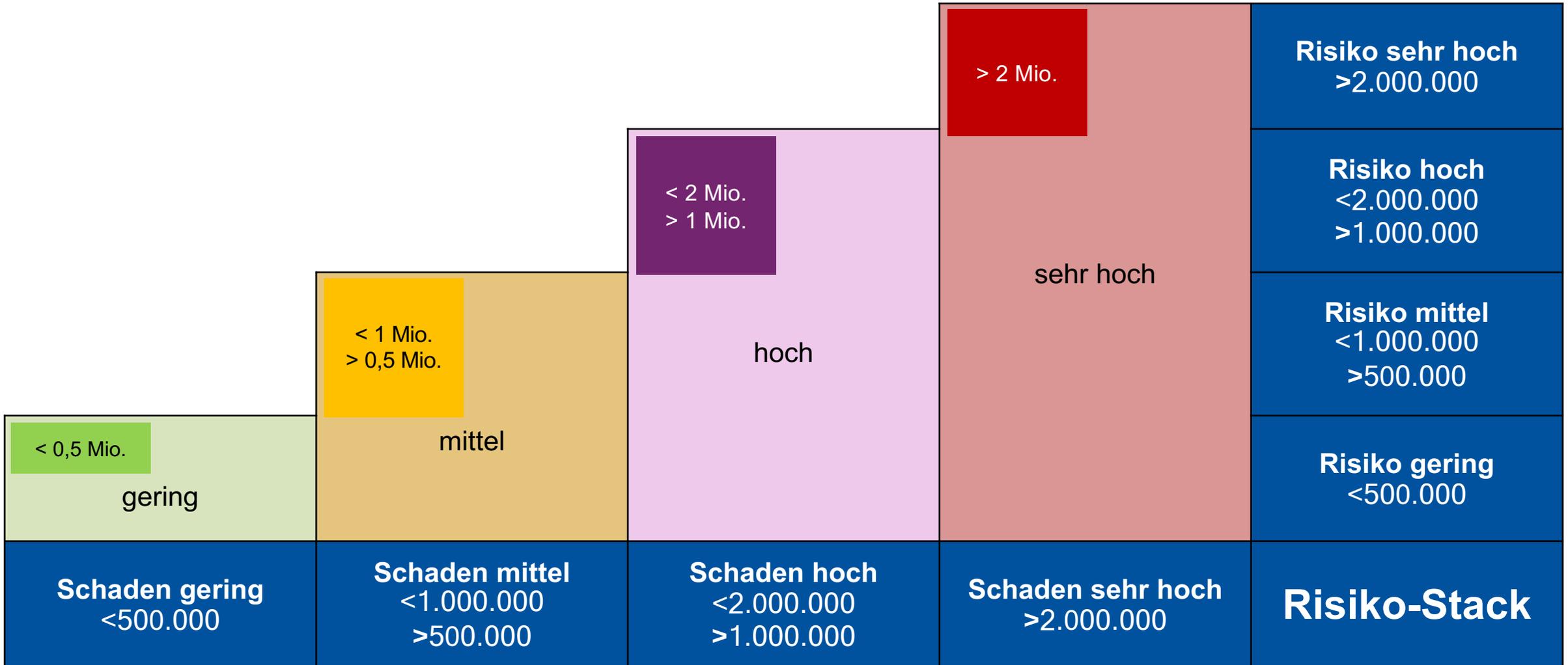
$k(x)=2/x$ Risiko = 2 Mio.

$j(x)=1/x$ Risiko = 1 Mio.

$h(x)=0,5/x$ Risiko = 0,5 Mio.



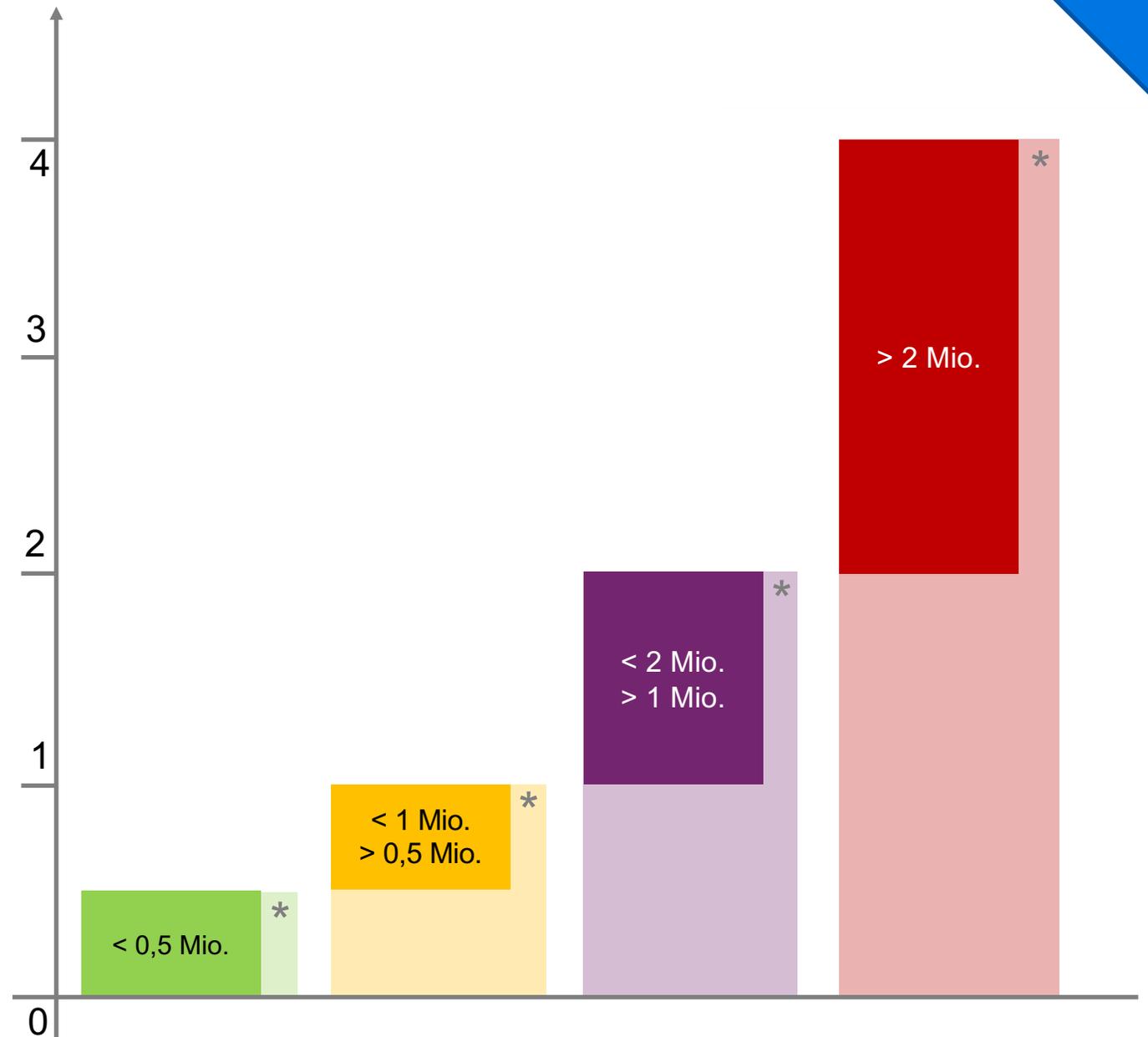
Der Risiko-Stack



Die Lösung des Matrizenproblems

Der Risiko-Stack

Elemente des Risiko-Stacks sortiert nach Schadenshöhe und Risiko-Höhe* liefern eine konsistente Entscheidungsgrundlage



- Weitere Untersuchungen in einer Studie



ria@cyclesec.com

- Senden Sie mir Ihre Risikomatrix
 - Matrix + Wertbereiche
- Die ersten 10 Einsendungen erhalten eine kostenlose Risiko-Isoquanten-Analyse (RIA)

Zusammenfassung:

- Das heutige IT-Risikomanagement ist fehlerhaft bis unbrauchbar.
- Viele der Fehler sind durch sorgfältige Analyse vermeidbar.
- Es gibt bereits Ansätze, das IT-Risikomanagement zu verbessern.

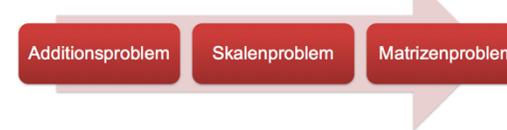
Die Probleme der Zeit



Die Probleme der Adaption



Probleme der Mathematik



Weitere Fehlercluster



Widerstand? Fragen?



Kontakt Daten:

- **CycleSEC GmbH**
Sebastian Klipper
Geschäftsführer (CEO)
sk@CycleSEC.com
+49(0)176-62986101
- **Web:**
<https://CycleSEC.com/Blog>
<https://www.Facebook.com/CycleSEC>
<https://Twitter.com/CycleSEC>
<https://www.facebook.com/SebastianKlipper>



Technische Sicherheit

- Penetrationstests
- Code-Reviews (Java, C++, Python, PHP,...)
- Hacking Workshops (z.B. OWASP Top 10)
- Live Hackings
- Schulungen

Security Management

- Aufbau eines ISMS
- ISO/IEC 27001 Implementierung
- Reifegradmessung der Security-Prozesse
- Risikomanagement mit 27005, etc.
- BSI IT-Grundschutz
- CISO und ISMS Coaching
- Guidelines, Konzepte, Policies...

Sicherheitskultur

- Live Hackings (Messen, Firmenevents,...)
- Awareness Giveaways
- Studien zur Sicherheitskultur
- Tools aus dem Awareness Koffer
- Social Engineering (Schulungen und simulierte Angriffe)
- Security Games (Awareness Gamification)
- Schulungen (Trainings, Workshops,...)
- Vorträge (Firmenevents, Keynotes)

Forschung und Entwicklung

- Industrieforschung (Spin-off der Fachhochschule Münster)
- Abschlussarbeiten (Informatik, Wirtschaftsinformatik,...)
 - Bachelor
 - Master
- Promotionen