GmbH für DV-Architekturen
Unternehmensberatung für IT-Sicherheit

IT-Incident Management & IT-Forensic

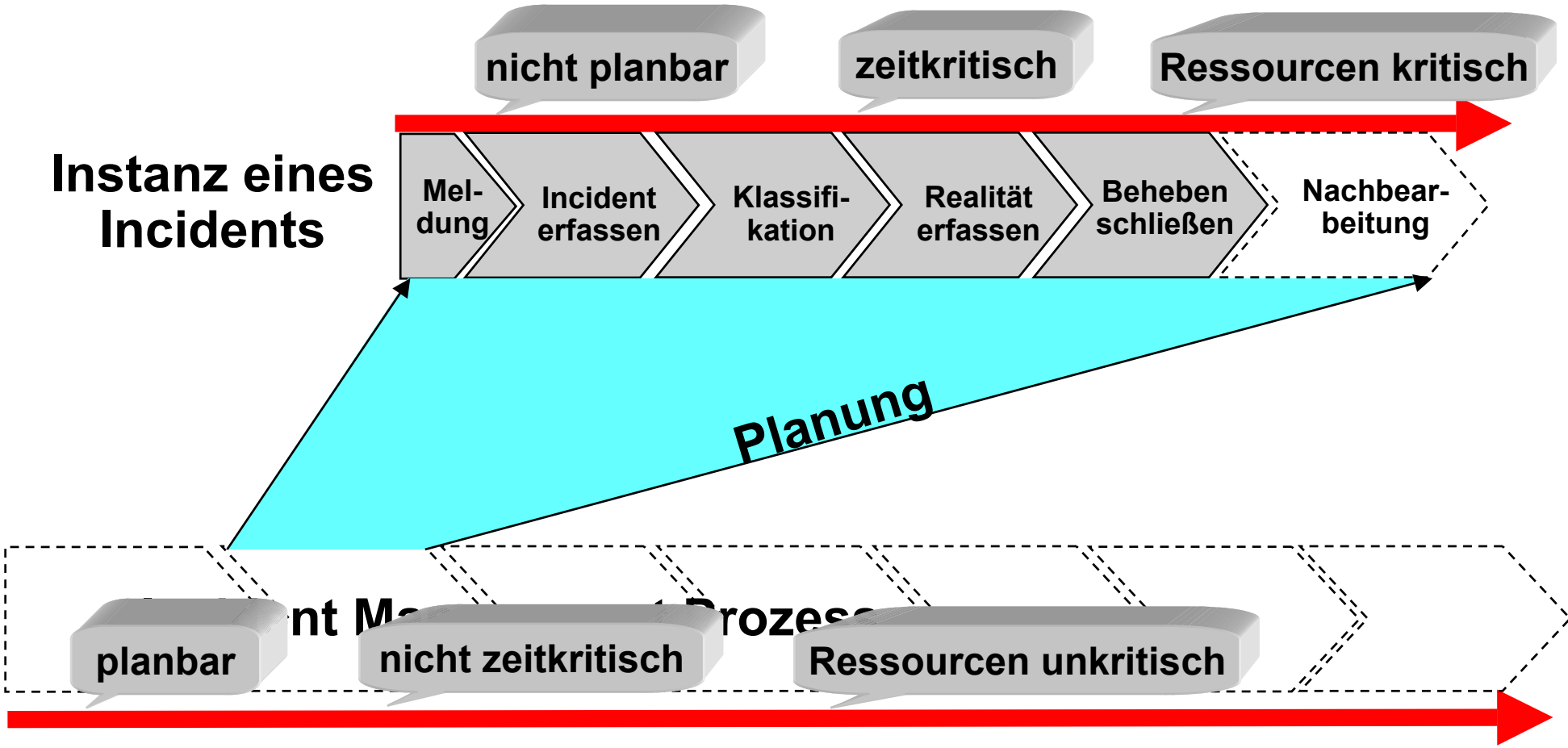
24.11.03

Eine Informationsbasis für zeitoptimiertes Incident Management

Inhalt

- Motivation und Themenabgrenzung
- Vertrauensketten und Informationsqualität
- Kostenaspekte und Hebel zur zeitlichen Optimierung
- Riskcharts und Risknodes als Informationsbasis

Der Incident Management Prozesses



Thema und Abgrenzung

Thema

- Durch Mehraufwände in dem planerischen Prozess des Incident Managements lassen sich die kritischen Aspekte der Abwicklung **sicherheitskritischer Incidents** positiv beeinflussen
- Es erfordert eine Planung, z.B. die richtigen Qualitäten einer Vertrauenskette zu definieren und eine Infrastruktur bereitzustellen, diese zu kommunizieren, um die kritischen Faktoren Zeit und Ressourcen bei der Abwicklung positiv zu beeinflussen

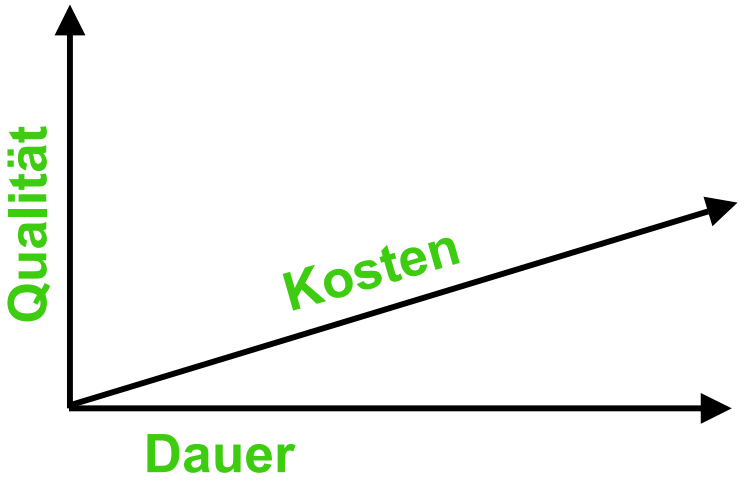
Abgrenzung

- Die technische Infrastruktur zum Herstellen oder Verbessern der Vertrauensbeziehung ist nicht trivial aber mit marktüblichen Mitteln zu implementieren
- Es geht also nicht um die technische Realisierung einer Vertrauenskette, sondern darum,
  - bereits im Vorfeld Kriterien verbindlich festzulegen, welche die **Belastbarkeit** von **Information** bewerten und
  - vorhandene **Vertrauensdefizite** zu **identifizieren** und durch einen planerischen Prozess **verbessern** zu können

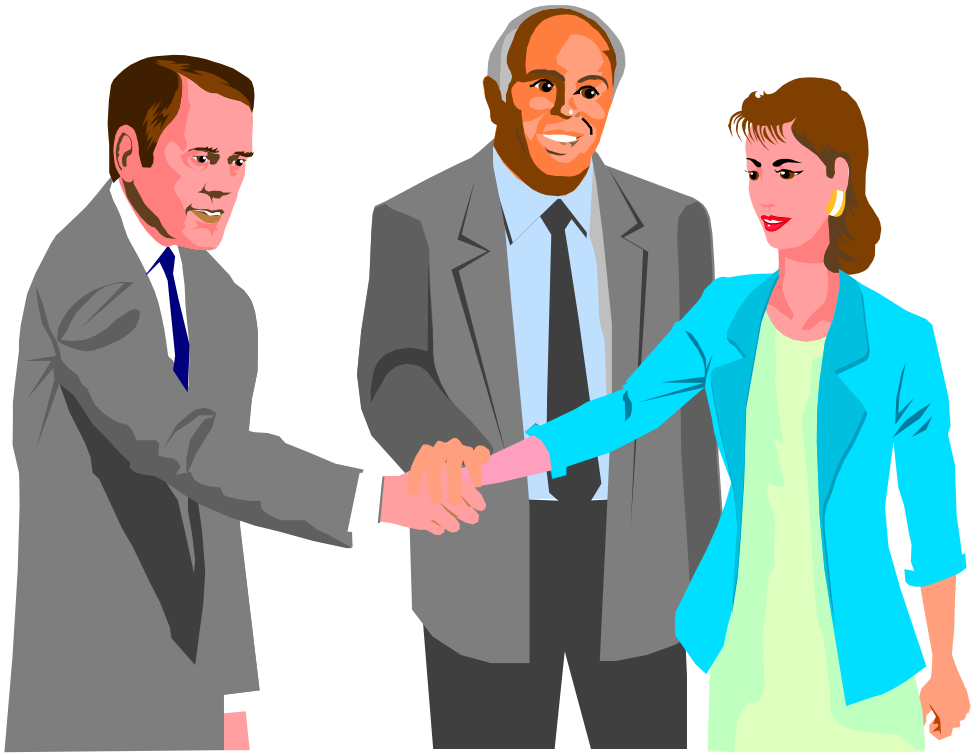
Inhalt

- Motivation und Themenabgrenzung
- Vertrauensketten und Informationsqualität
- Kostenaspekte und Hebel zur zeitlichen Optimierung
- Riskcharts und Risknodes als Informationsbasis

Vertrauenskette



- Vertrauensketten im alltäglichen Leben:
  - ***Nachrichten***
    - Informationsträger
    - Reporter
    - Verleger oder Redakteur
    - Leser
  - ***Brief***
    - Autor
    - öffentlicher Postkasten
    - Post
    - Briefträger
    - Empfänger



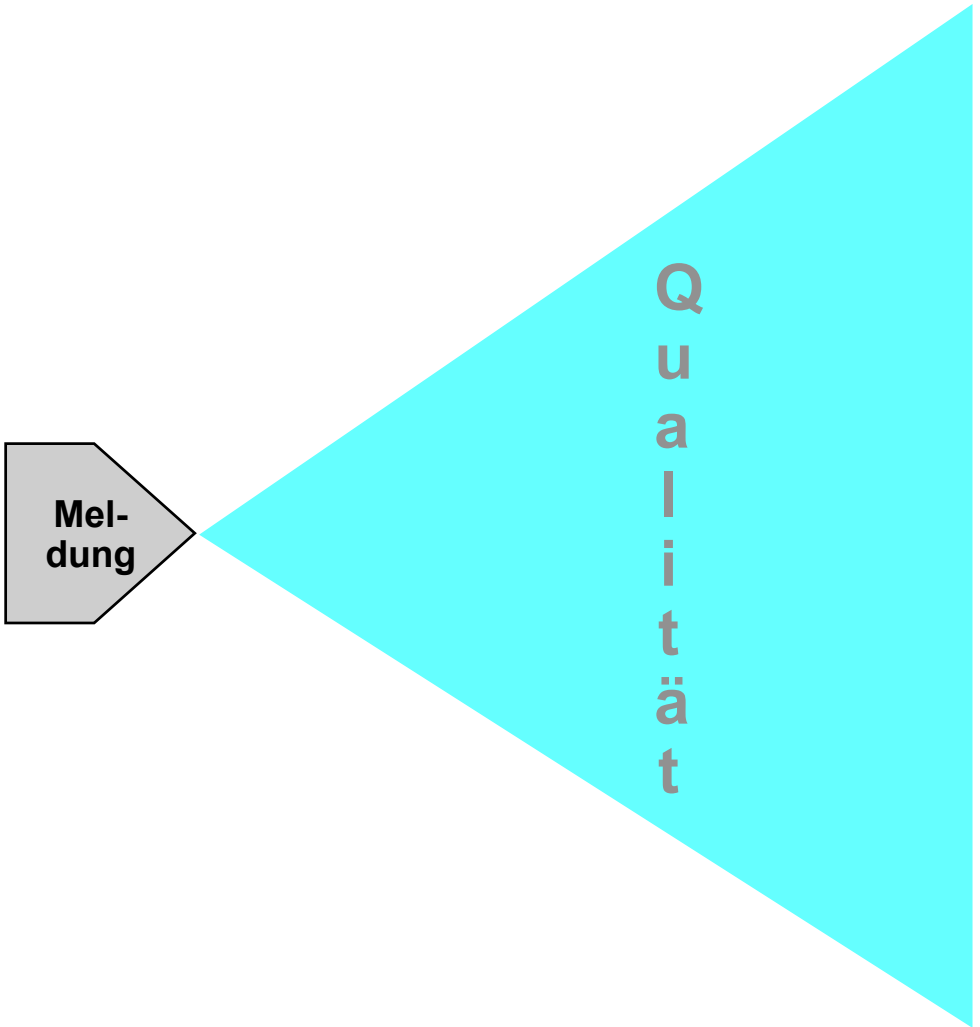
Vertrauenskette

- Vertrauensketten im alltäglichen Leben:
  - ***Kreditkarte*** Bank, Kreditkartenorganisation, Postweg, Empfänger ... Zahlung
  - ***Übersetzer*** Sprecher, Übersetzer, Zuhörer
- Einer Information wird durch die / trotz der Beteiligung von mehreren Subjekten Vertrauen entgegengebracht
  - Vertrauen zwischen Subjekten herstellen, die sich nicht kennen
  - Vorhandenes Vertrauen erhöhen
  - Das Vertrauen ist nicht notwendigerweise in beiden Richtungen gleich
  - Das schwächste Glied ist von jedem Mitglied der Kette nach subjektiven Kriterien zu identifizieren
  - Es gibt unterschiedliche Qualitäten / Eigenschaften, welche durch eine Vertrauenskette gewährleistet werden sollen
    - ***Risikobereitschaft, Reputation, Regressmöglichkeit, Haftung ...***

Wer stellt das Vertrauen in eine Incident-Meldung her?

- Was ist passiert
  - Der Originalschauplatz ist häufig informationstechnisch abgeriegelt
  - Die kompetenten Ansprechpartner sind mit ihren Aktivitäten überlastet und deshalb nicht ansprechbar
  - Es gibt wahrscheinlich keine direkte vorher etablierte Vertrauens-beziehung zu dem Originalplatz
- Was könnte noch passieren
  - Analytiker weltweit beschäftigen sich mit dem Vorfall und geben möglichst zeitnah Einschätzungen der Ursache
  - Erst nach der Ursachenabgrenzung kann das Schadenspotential untersucht werden
- Welche Schäden können in der unterrichteten Organisation eintreten
  - Hebel: Inventory, Assetmanagement
  - Hebel: dynamische Business Impact Analyse, welche Planspiele erlaubt
  - Hebel: dynamisches Riskmanagement
- Welche Vorkehrungen sind deshalb für das Unternehmen angebracht
  - Präventivmaßnahmen mit geringem Business Impact können auf Basis „unsicherer“ Meldungen durchgeführt werden
  - Entscheidungs- / Eskalationspfad für hohen Business Impact vorab gut absichern

Die Qualität der Meldung ist nicht „binär“



Hoax

Incident hat nicht stattgefunden, wäre aber möglich

Incident hat stattgefunden, die Beschreibung ist aber übertrieben

Incident hat stattgefunden, Beschreibung ist korrekt, aber die Rückschlüsse auf die Ursachen sind fehlerhaft

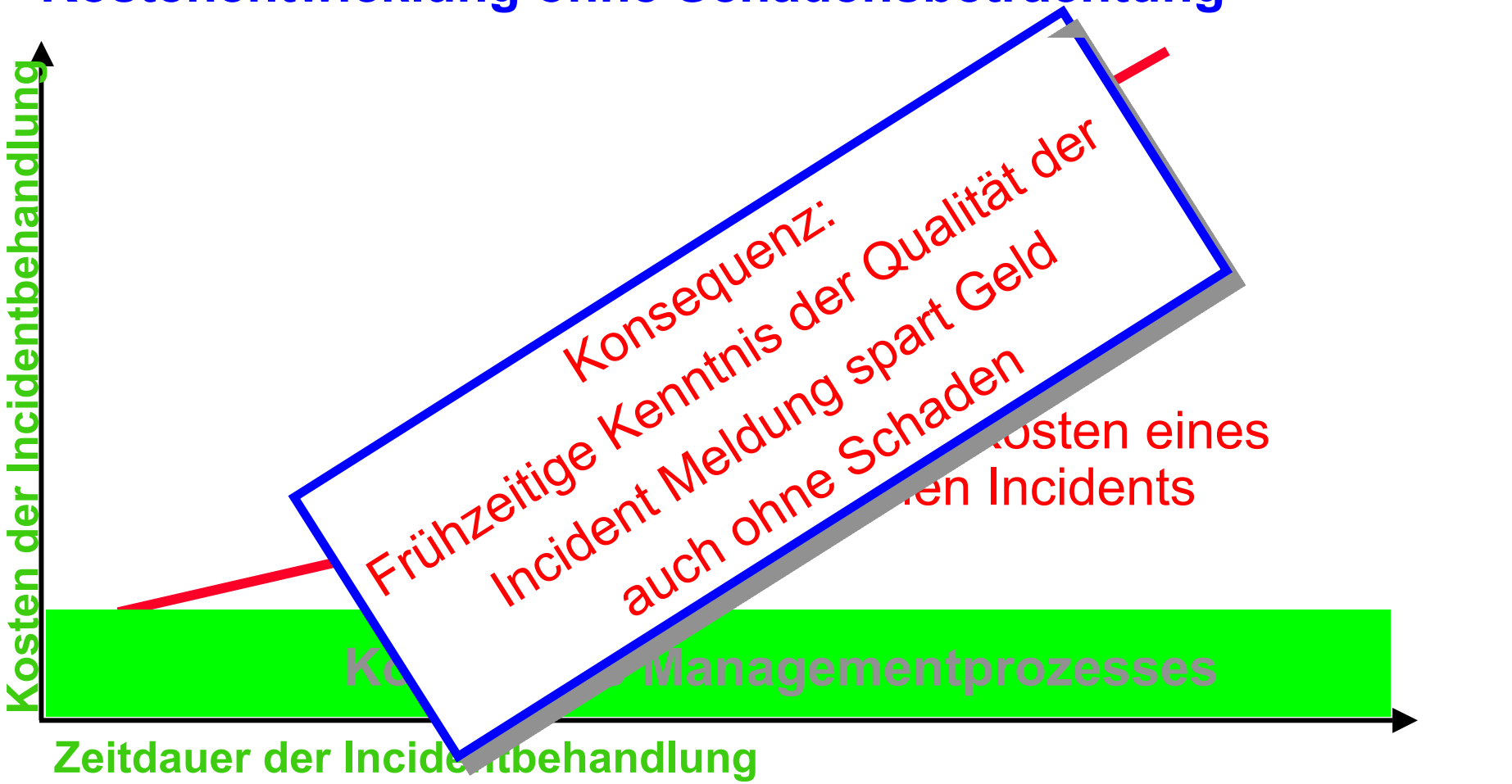
Die Handlungsanweisungen sind fehlerhaft

100% Übereinstimmung mit Realität und vollständige Beschreibung des Incidents

Inhalt

- Motivation und Themenabgrenzung
- Vertrauensketten und Informationsqualität
- Kostenaspekte und Hebel zur zeitlichen Optimierung
- Riskcharts und Risknodes als Informationsbasis

Kostenentwicklung ohne Schadensbetrachtung



Hebel bei der zeitlichen Optimierung

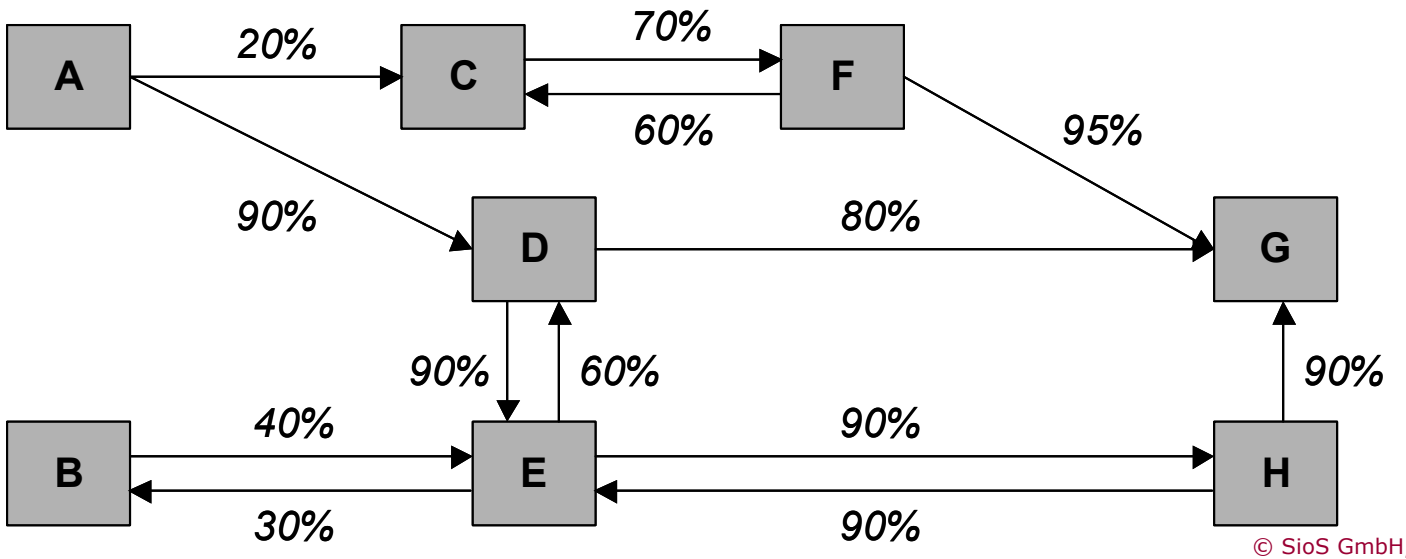
- Bewertung der Vertrauenswürdigkeit der Herkunft der Information
  - Hebel: Vorab die Vertrauenswürdigkeit der Informationskanäle definieren und gegebenenfalls positiv beeinflussen
- Genaue Kenntnis der eigenen Systeme ermöglicht Präzisierung der Schadensszenarien
  - Voraussetzung: Inventory, Assetmanagement
- Genaue Kenntnis der Auswirkungen der potentiellen Schäden auf das Business ermöglicht zeitgenaues Risikomanagement
  - Hebel: dynamische Business Impact Analyse, welche Planspiele erlaubt
  - Hebel: dynamisches Riskmanagement
- Es werden 2 oder mehr Planspiele durchgeführt und jeweils deren business impact bewertet
  - Schaden in Kauf nehmen und danach reagieren
  - Schaden verhindern z.B. durch Außerbetriebsetzen der potentiell betroffenen Systeme
- Die Kostenfunktionen sind online vorzuhalten
- Die Risikofreudigkeit der beteiligten Prozessowner einbeziehen
  - Das Krisenteam wird für alle Planspiele mit aussagefähigen Business-verantwortlichen besetzt

Parameter zum Bewerten von Vertrauensketten

- Übermittlungskanal
  - E-Mail
  - Telefon
- (un-)Bekannter Benutzer, der akustisch oder mit technischen Mitteln authentisiert wurde
- Kryptographische Anteile
  - CA
  - Zertifikat
  - Schlüssellänge
  - Verfahren
- Ist die gesamte Informationskette technisch beglaubigt
- Anzahl der Meldungen
- Presse
- Plausibilität der Meldung
- Verstrichene Zeitdauer
- Beteiligte Organisationen
- Haftung
- Potentielle Motivation für Falschmeldungen
- Vertragsverhältnis

Vorhandene Vertrauensketten prüfen

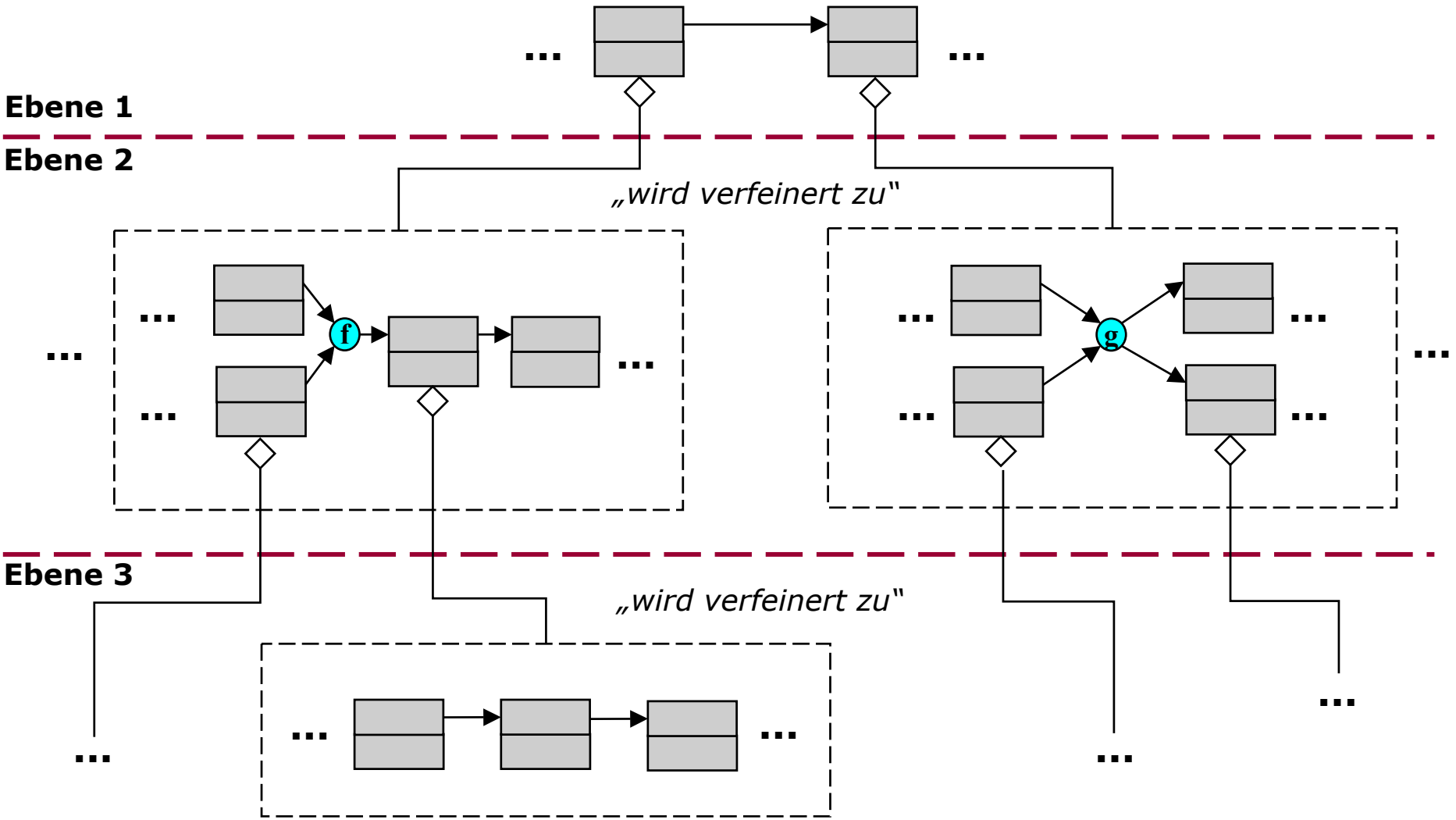
- In der Policy Schwellwerte bzw. Vertrauensbereiche festlegen, welche konkrete Handlungsanweisungen definieren
- Prüfung der Belastbarkeit der vorhandenen Vertrauensketten auf diese Schwellwerte
- Gegebenenfalls Maßnahmen zur Verbesserung der Belastbarkeit einleiten



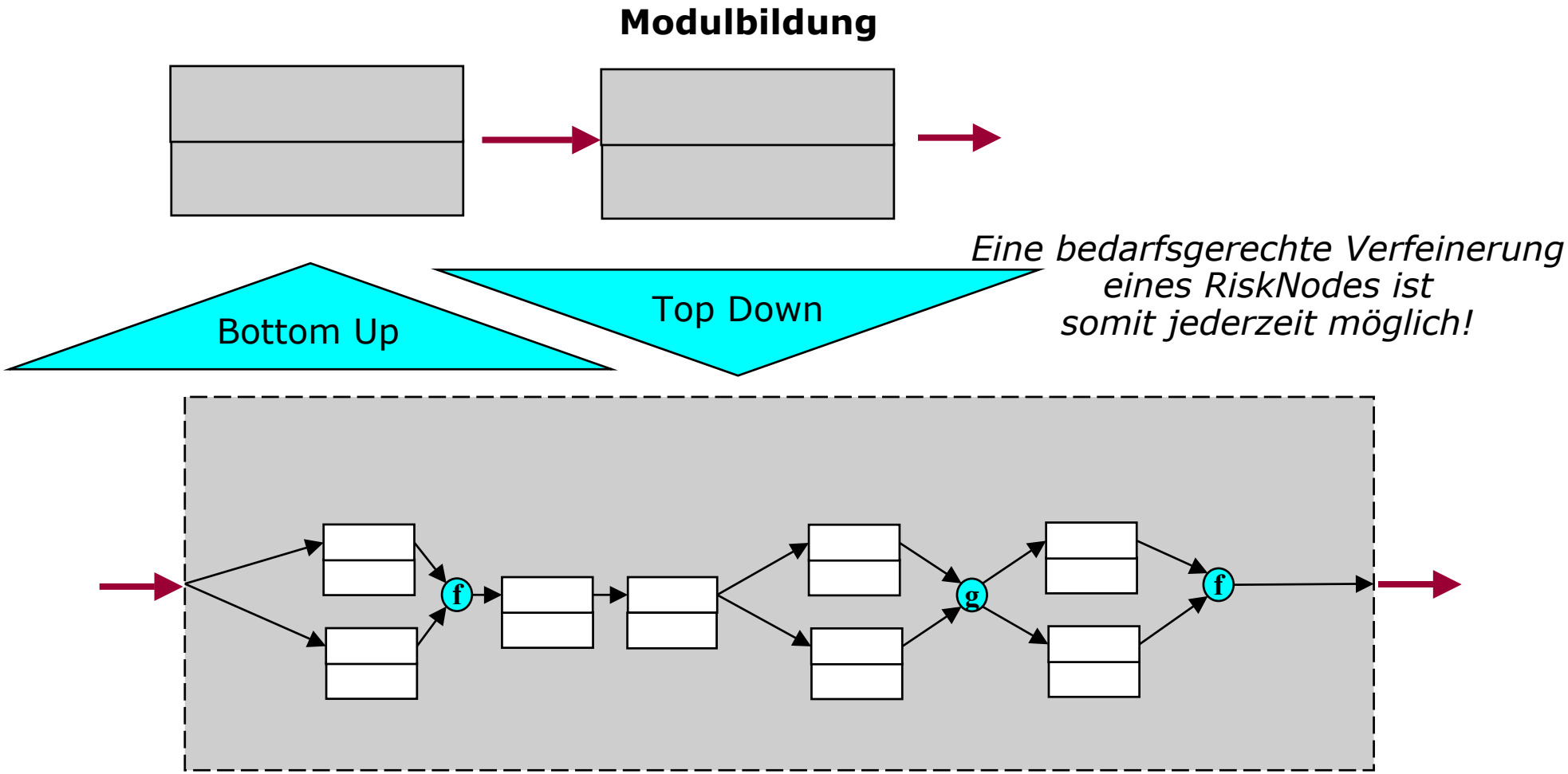
Inhalt

- Motivation und Themenabgrenzung
- Vertrauensketten und Informationsqualität
- Kostenaspekte und Hebel zur zeitlichen Optimierung
- Riskcharts und Risknodes als Informationsbasis

Riskcharts und Risknodes als Informationsbasis

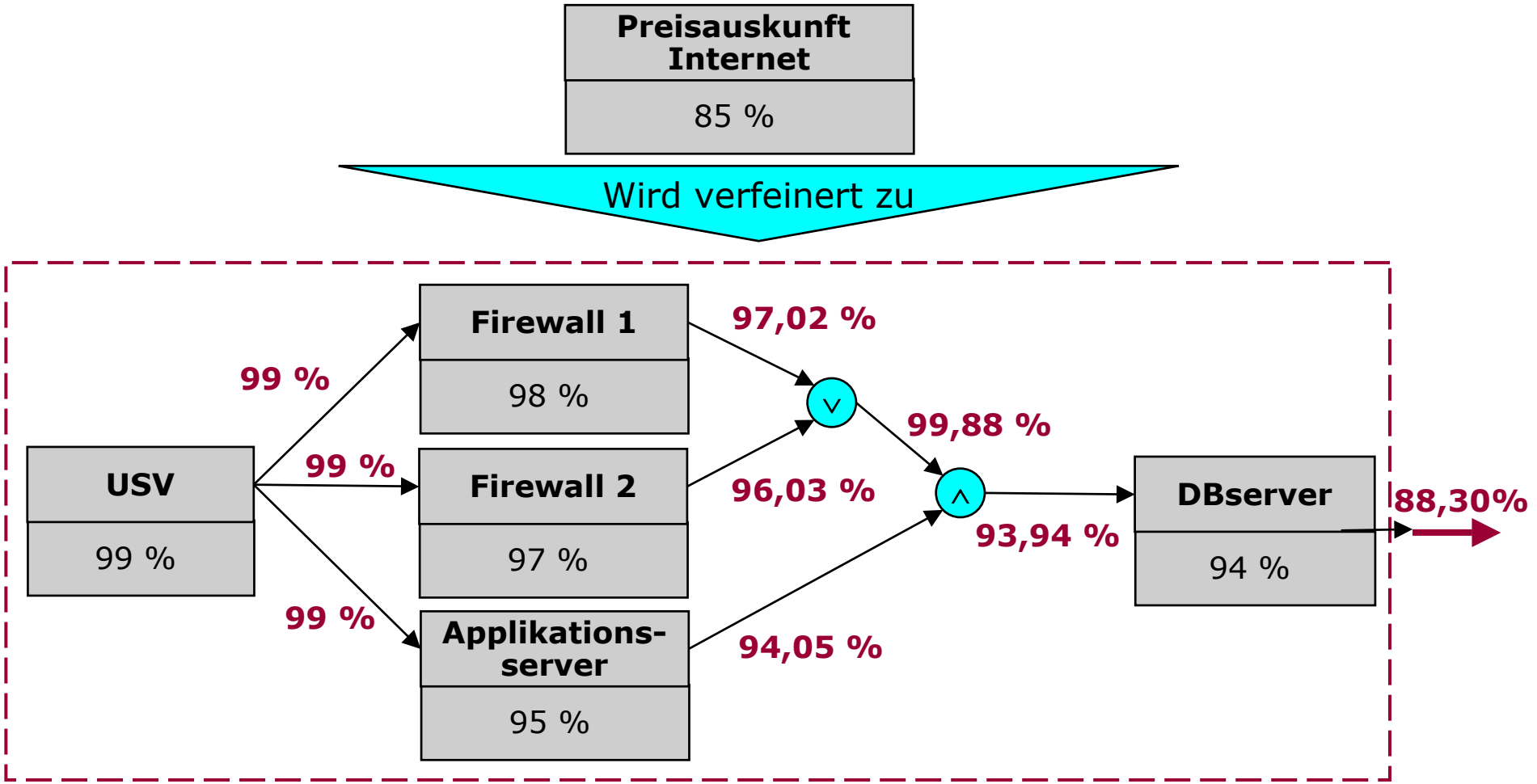


Riskcharts und Risknodes Detailsicht einer „Verfeinerung“



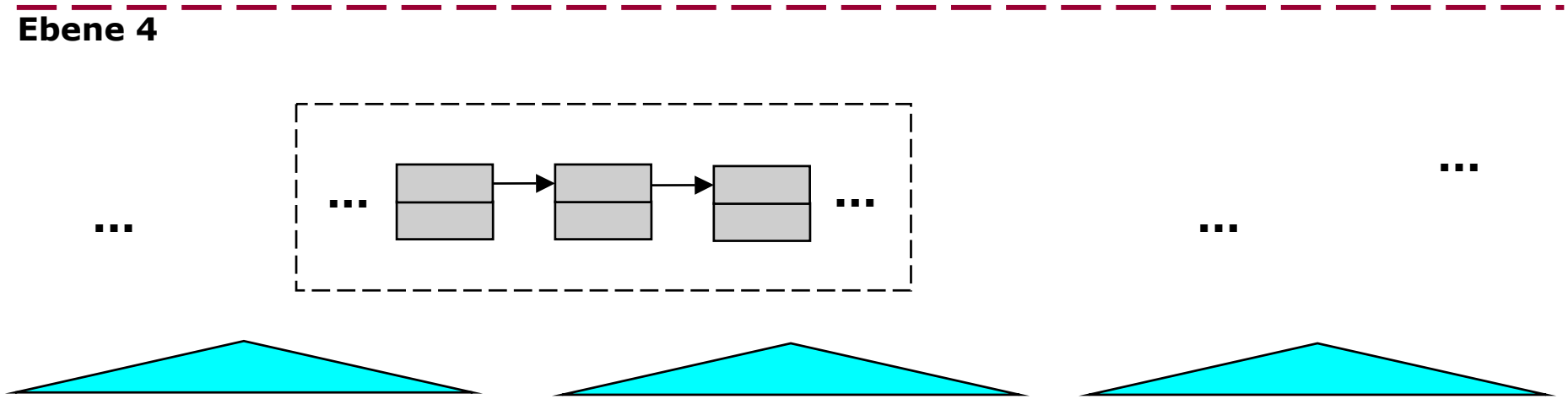
Riskcharts und Risknodes Detailsicht einer „Verfeinerung“

Der RiskNode „Applikation: Preisauskunft Internet“ soll auf Ebene 4 (IT Landscape) im Aspekt Verfügbarkeit weiter verfeinert werden

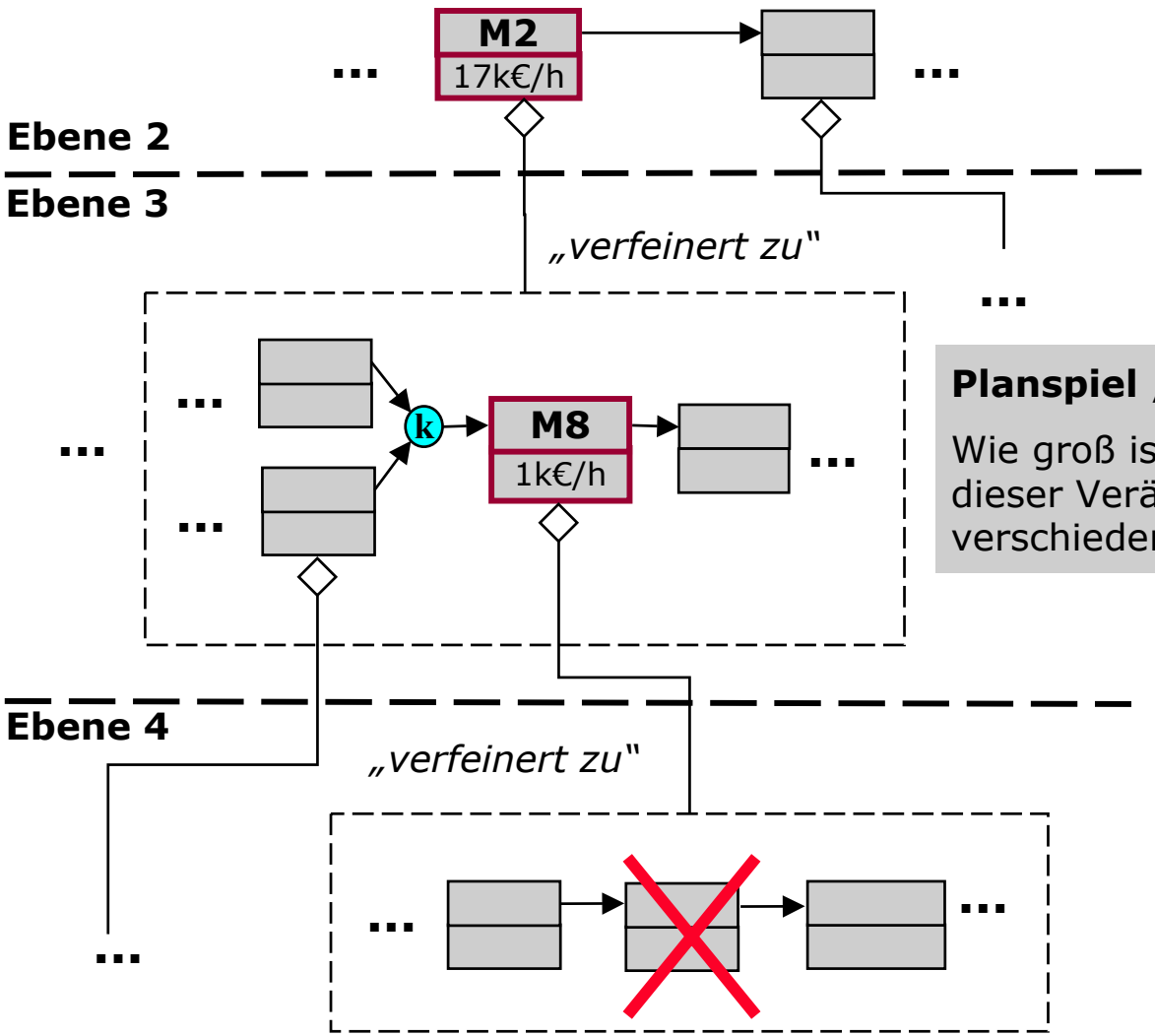


Massendaten

- Massendaten können durch etablierte Systeme importiert werden
  - Kommunikationseigenschaften und Netztopologie durch Netzwerkmanagement
  - Ist-Stand der Verfügbarkeit von einzelnen Komponenten durch Monitoringwerkzeuge



Schadensszenarien mit Kostenfunktion



Annahme im Planspiel:

Jedes Schadensszenario entspricht einem Planspiel

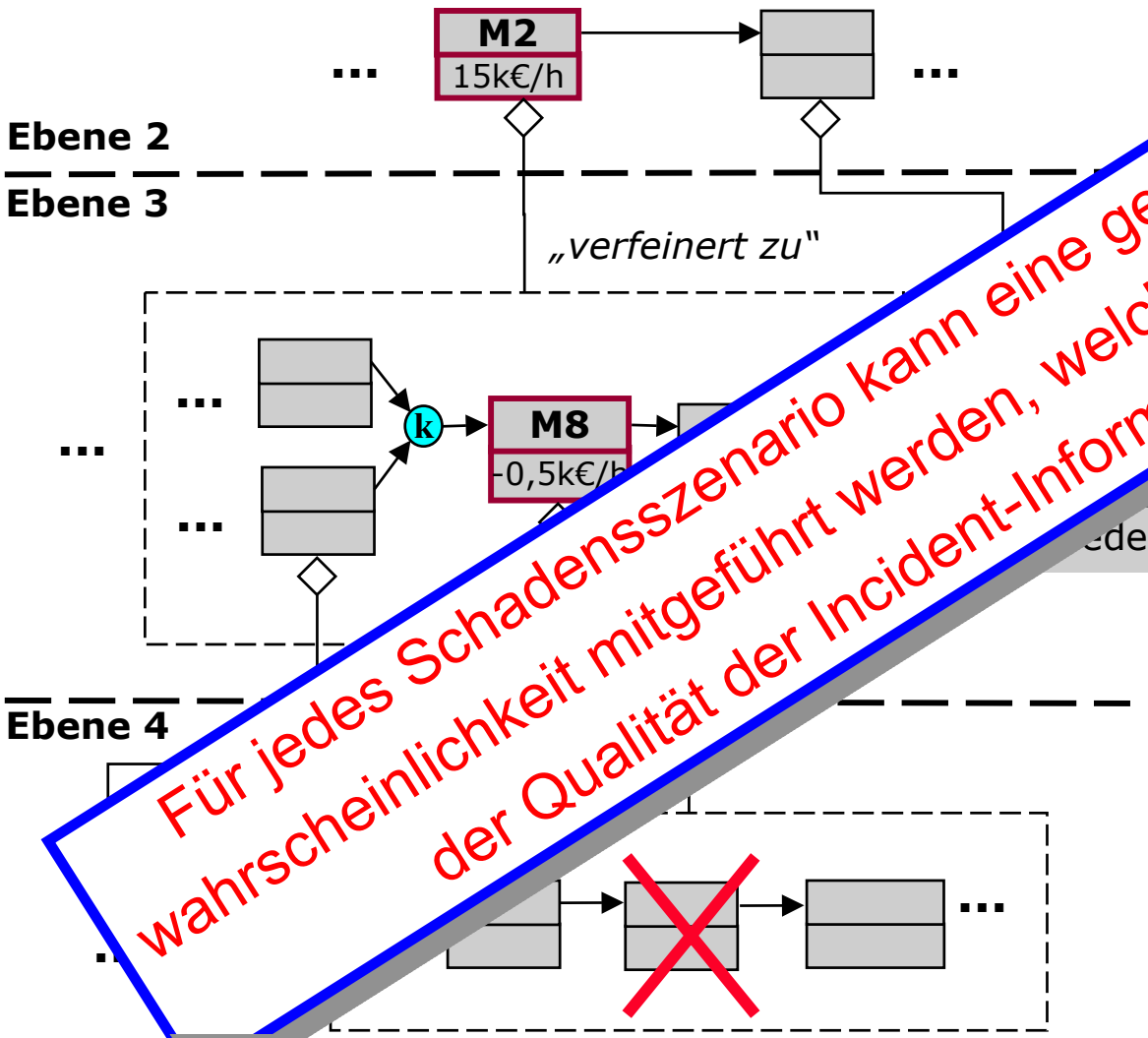
Auf Ebene 4 wird zur Verteidigung die Firewall 1 vom Netz genommen, bis ein adäquater Patch zur Verfügung steht

Planspiel / Schadensszenario:

Wie groß ist der Business Impact dieser Veränderung auf den verschiedenen Ebenen?

Planspiel Schadensszenario

Schadensszenarien mit Kostenfunktion



Annahme i

Jede
e

…m Netz
…adäquater
…gung steht

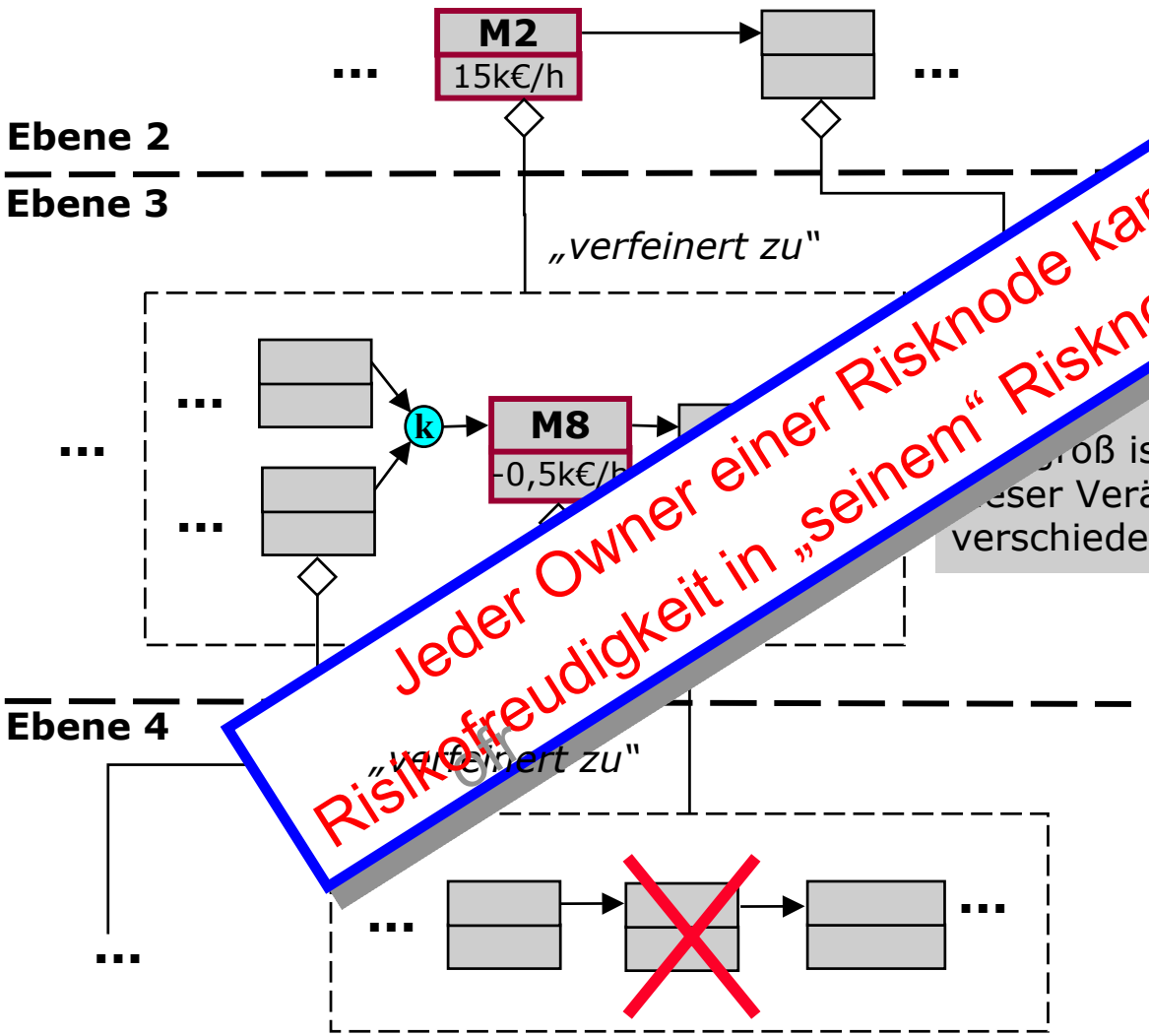
…nsszenario:

…r Business Impact
…nderung auf den
…edenen Ebenen?

Für jedes Schadensszenario kann eine geschätzte Eintritts-wahrscheinlichkeit mitgeführt werden, welche unter anderem von der Qualität der Incident-Information abhängt

Planspiel Schadensszenario

Schadensszenarien mit Kostenfunktion



Annahme i… …anspiel:

Jede… …enario
e… …lanspiel

…zur Vertei-
…ewall 1 vom Netz
…n, bis ein adäquater
…zur Verfügung steht

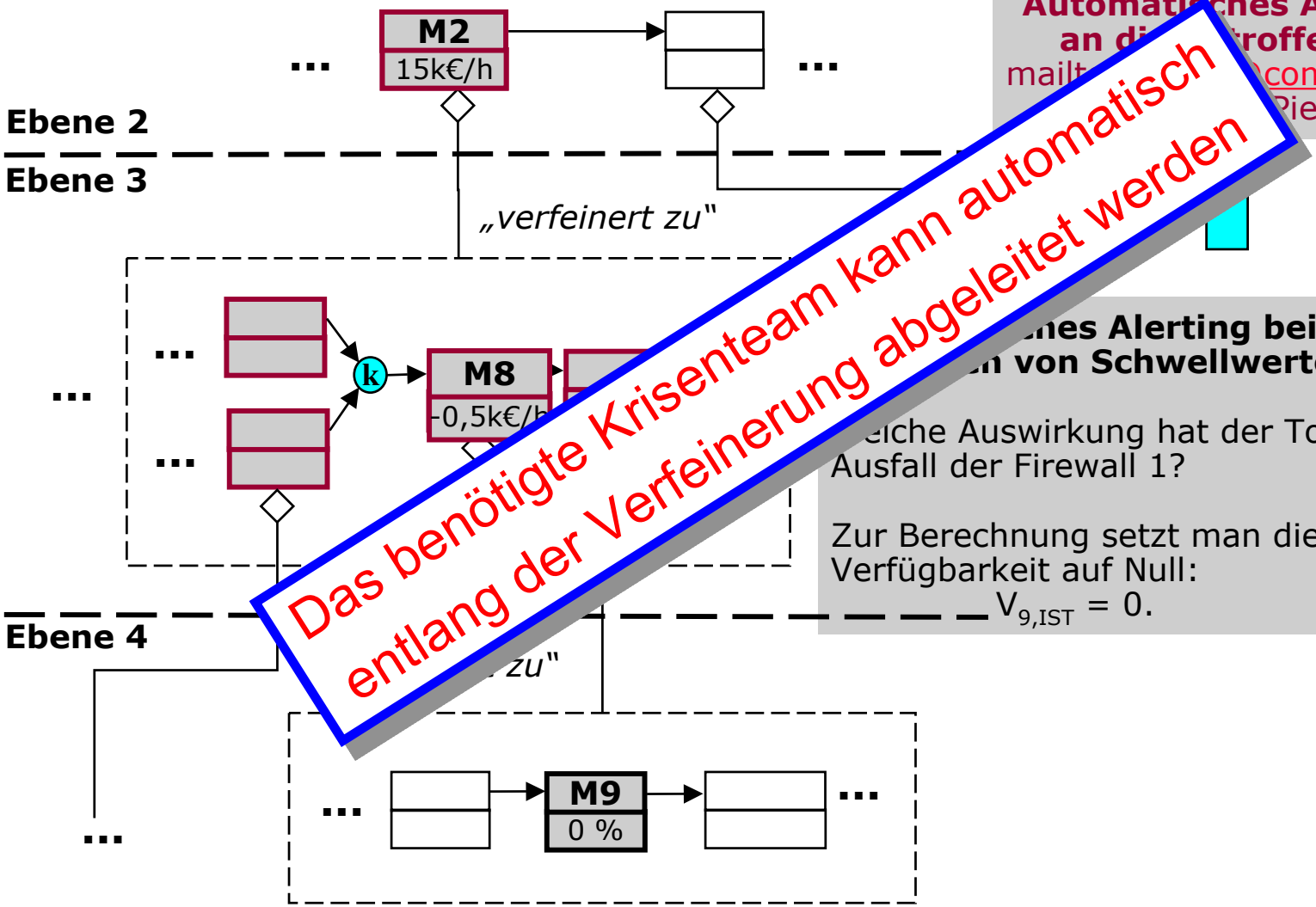
… Schadensszenario:

…roß ist der Business Impact
…eser Veränderung auf den
verschiedenen Ebenen?

Jeder Owner einer Risknode kann seine Risikofreudigkeit in „seinem" Risknode ausdrücken

Planspiel Schadensszenario

Automatische Information an die potentiell Beteiligten



Automatisches Alerting an di[illegible]roffenen:
mailt[illegible]@company.de
[illegible]Piepser

[illegible]hes Alerting bei [illegible]n von Schwellwerten:

[illegible]eiche Auswirkung hat der Total-Ausfall der Firewall 1?

Zur Berechnung setzt man die Ist-Verfügbarkeit auf Null:
$V_{9,IST} = 0$.

Das benötigte Krisenteam kann automatisch entlang der Verfeinerung abgeleitet werden

Summary

- Nach Unterscheidung der Prozesse im Incidentmanagement in kontinuierliche und spontan anfallende Prozessteile haben wir die zeitliche Optimierung der spontanen Prozesse zu Lasten der kontinuierlichen Prozesse motiviert
- Wir haben zeitliche Optimierungsmöglichkeiten aufgezeigt und eine Informationsinfrastruktur dargestellt, mit welcher alle identifizierten Verbesserungspotentiale realisiert werden können
  - Vertrauensketten vorab qualifizieren
  - Vorab Kategorien der Informationsqualität definieren
  - Dynamische Business Impact Analysen mittels Schadensszenarien in Form von Planspielen als Grundlage eines dynamischen Riskmanagements
  - Management der Kostenfunktionen
  - Integration der Risikofreudigkeit der Businessowner mit Hilfe von Schwellwerten

Besten Dank für Ihre Aufmerksamkeit

GmbH für DV-Architekturen
Unternehmensberatung für IT-Sicherheit

Ramon Mörl

Ramon.Moerl@SioS-GmbH.de
Tel: 089/89160050

