… noch ein CERT!

Prof. Dr. Klaus-Peter Kossakowski
HAW Hamburg

Interessante Frage:

Was waren 1973 im Internet mit 31 (!) Systemen die schwerwiegendsten Sicherheitsprobleme?

© 2017 by Klaus-Peter Kossakowski, Germany

Antwort aus dem RFC 602 von 1973

- Schwache und/oder Klartext-Passworte
- Systeme mit Sicherheitslücken ohne angemessene Gegenmaßnahmen
- Viele kreative Benutzer, denen ihre Möglichkeiten nicht ausreichen

© 2017 by Klaus-Peter Kossakowski, Germany

2. November 1988

- **2. November 1988: Internet-Wurm**
  - Internet besteht aus ca. 70.000 Rechner
  - Etwas weniger als 10% befallen
  - Kommunikationsinfrastruktur effektiv ausgeschaltet
- **6. Dezember 1988: DARPA-Krisensitzung**
  - Analyse der Angriffe: Okay
  - Korrektur der Ursachen: Okay
  - Behebung der Schäden: Teilweise
  - Kommunikation / Koordination: NULL

© 2017 by Klaus-Peter Kossakowski, Germany

Erstes CERT in Deutschland

- **1991 : Zu viele Vorfälle in Europa**
  - Europäische Forschungsnetze starten den Informationsaustausch
- **1992 : Ausschreibung des DFN**
  - ca. 70.000 Rechner in Deutschland
- **1993 : Das Internet hebt ab**
  - der Kollege nebenan programmiert einen Web-Server selbst
  - erste Vorfälle machen weitere Diskussion unnötig

© 2017 by Klaus-Peter Kossakowski, Germany

Interessante Frage:

Was waren 1993 im Internet mit etwas mehr als zwei Millionen Systemen die schwerwiegendsten Sicherheitsprobleme?

© 2017 by Klaus-Peter Kossakowski, Germany

Antwort immer noch ...

- Schwache und/oder Klartext-Passworte
- Systeme mit Sicherheitslücken ohne angemessene Gegenmaßnahmen
- Viele kreative Benutzer, denen ihre zugewiesenen Rechte nicht ausreichen

© 2017 by Klaus-Peter Kossakowski, Germany

Relevante Frage:

Wer ist denn

für Sie zuständig?

© 2017 by Klaus-Peter Kossakowski, Germany

Relevante Frage:

Wer ist denn

für Sie zuständig?

Sie ::=

Bürger | Firma | Community

© 2017 by Klaus-Peter Kossakowski, Germany

CERTs fördern ganzheitliche Sicherheit

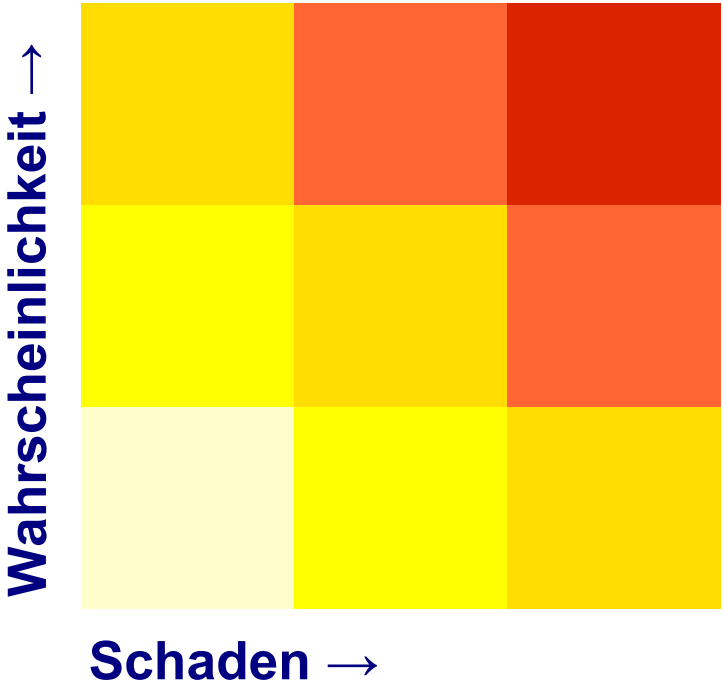
- **Alle Risiken bewerten und „im Blick“ halten**
  - Initiale Bewertung, dann kontinuierlich
  - Lagebild und
  - Sicherheitsmeldungen
- **Krisenmanagement etablieren und**

  ... auch mit den „kleinen“ Krisen fertig werden!
- **Ausreichend Ressourcen einsetzen**
  - Technik, aber immer auch
  - Personal

© 2017 by Klaus-Peter Kossakowski, Germany

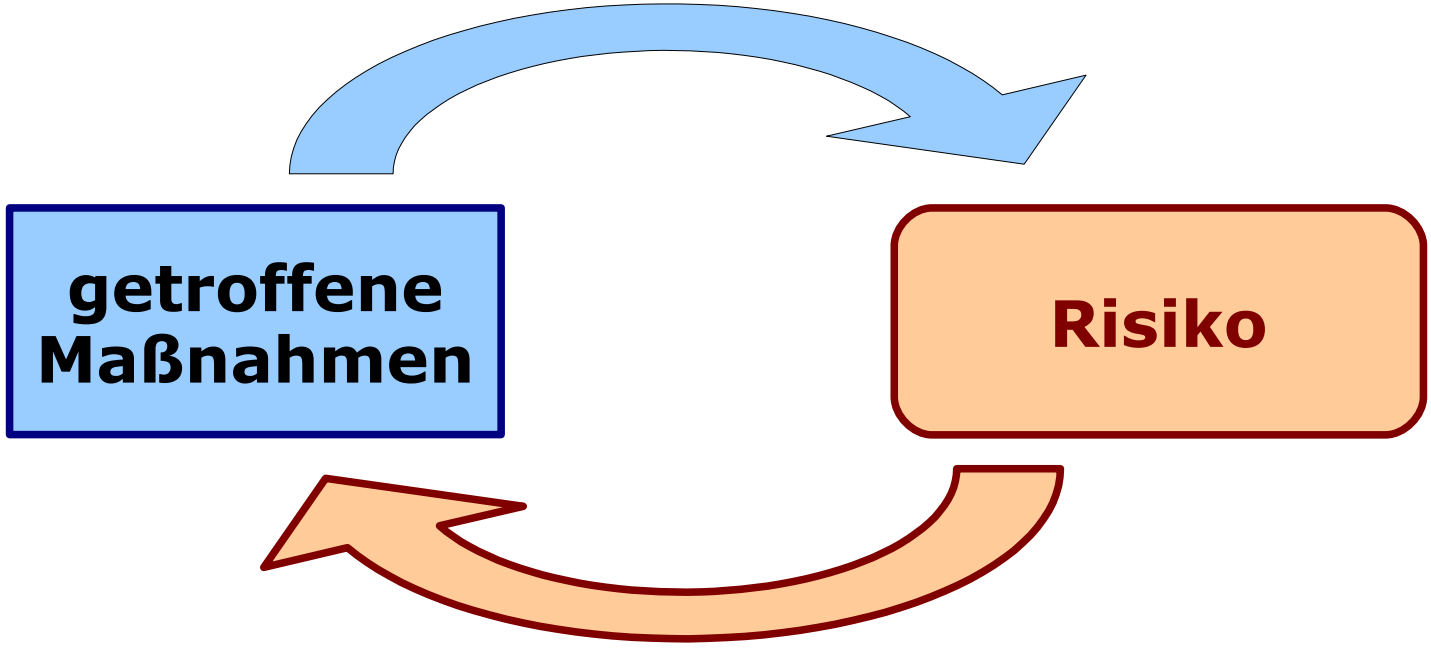
Aber was ist ein Risiko?

- **Traditionelle Definition:**
  Risiko = Wahrscheinlichkeit * Schaden



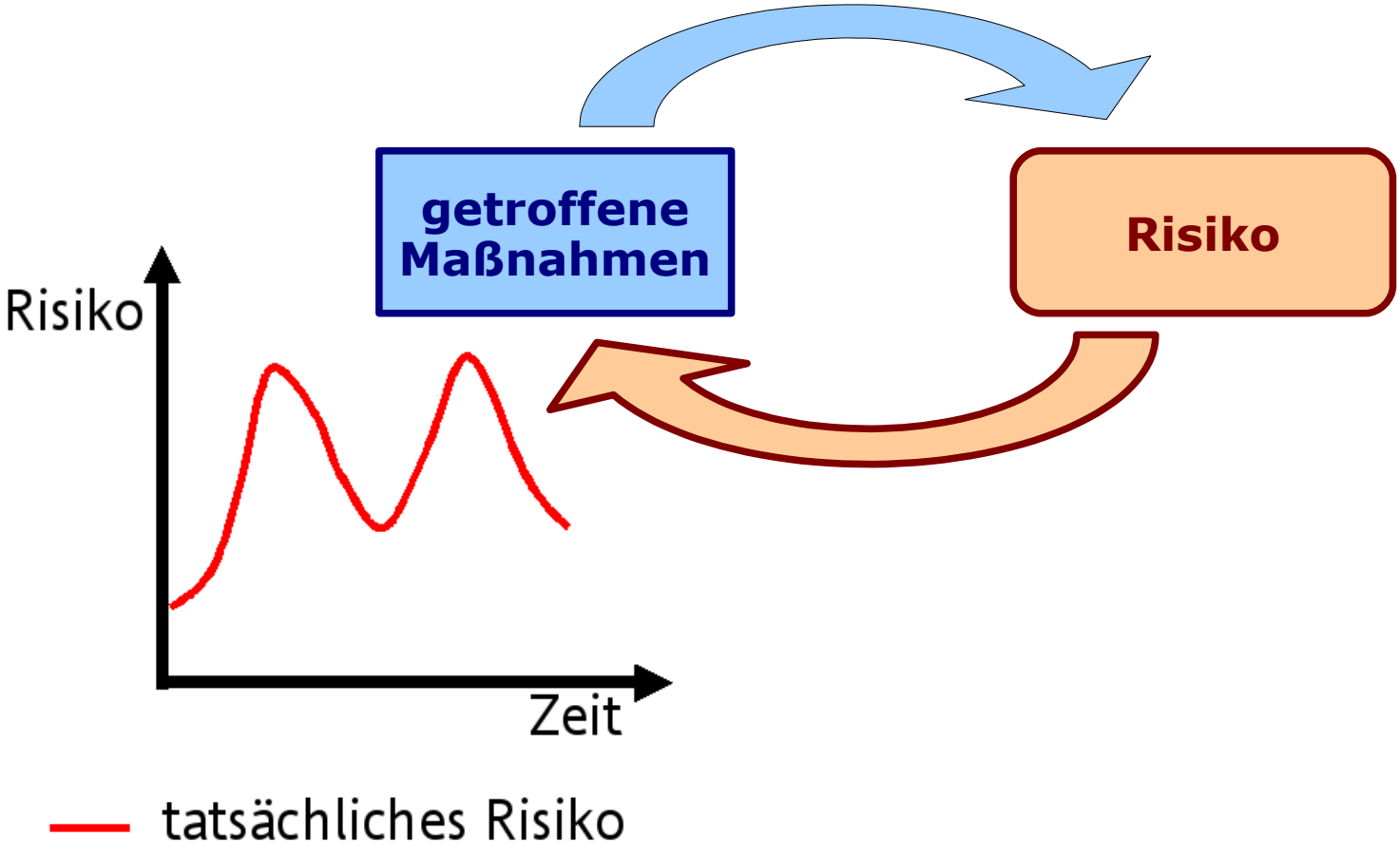
© 2017 by Klaus-Peter Kossakowski, Germany

Planung, Umsetzung, Messung



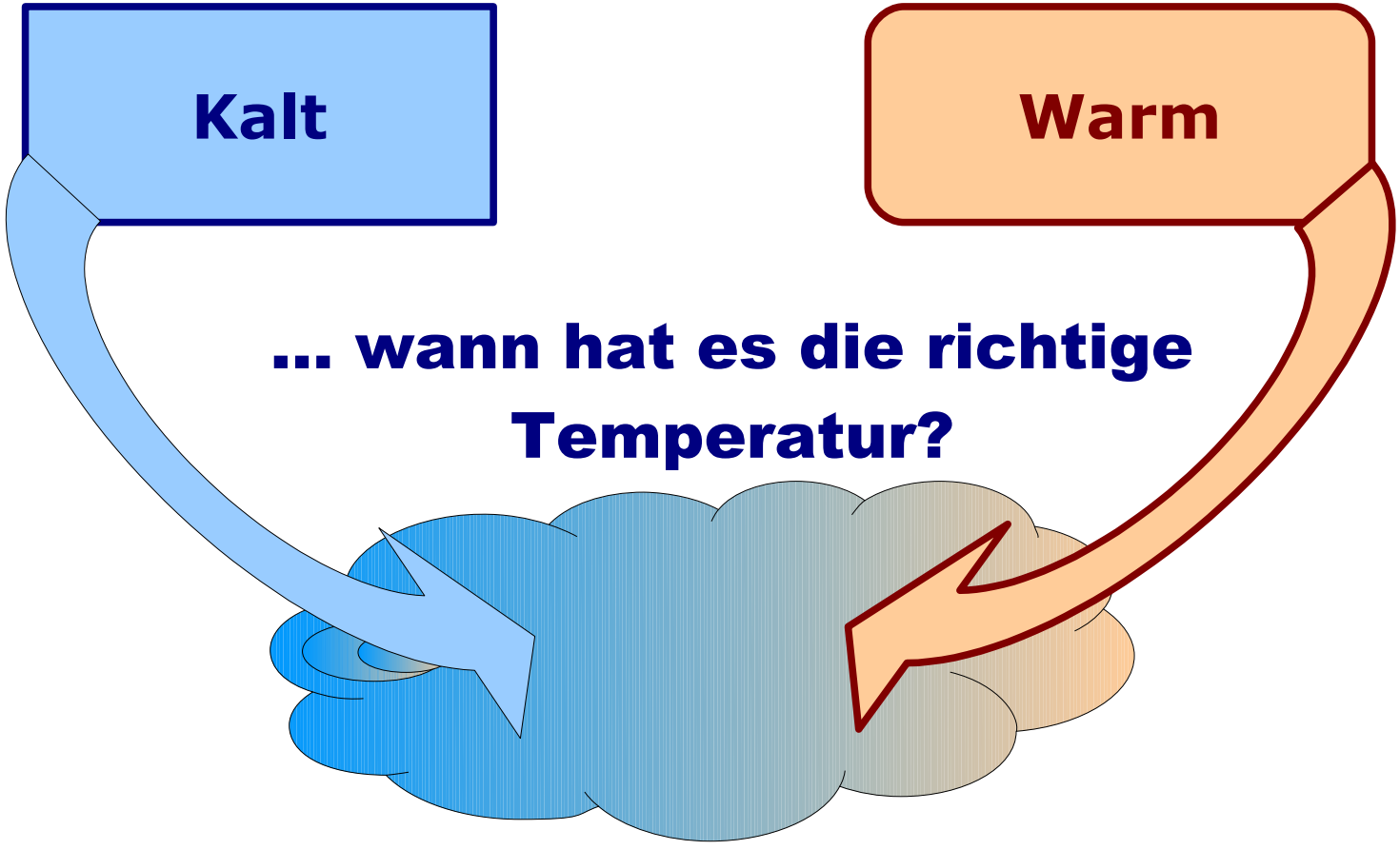
© 2017 by Klaus-Peter Kossakowski, Germany

Planung, Umsetzung, Messung



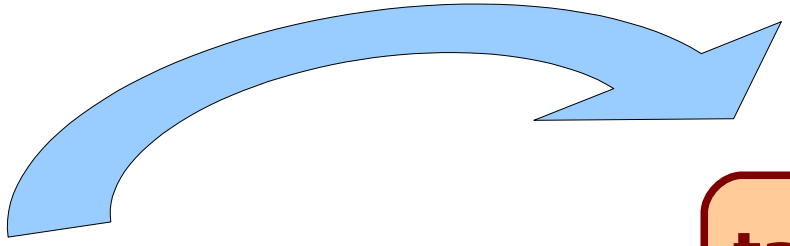
© 2017 by Klaus-Peter Kossakowski, Germany

Planung, Umsetzung, Messung - revisited



© 2017 by Klaus-Peter Kossakowski, Germany

Planung, Umsetzung, Messung - revisited



getroffene Maßnahmen

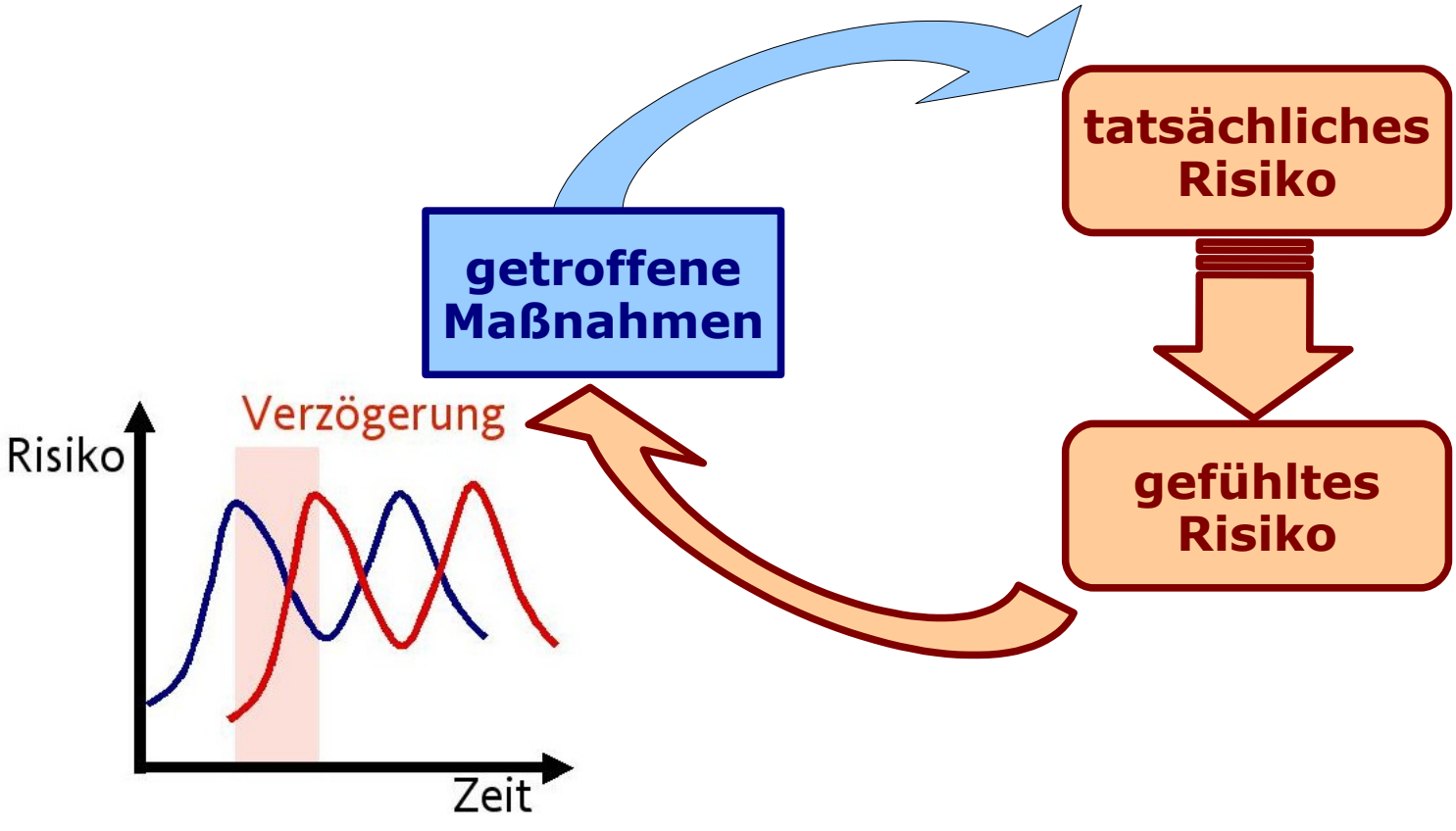
tatsächliches Risiko

gefühltes Risiko

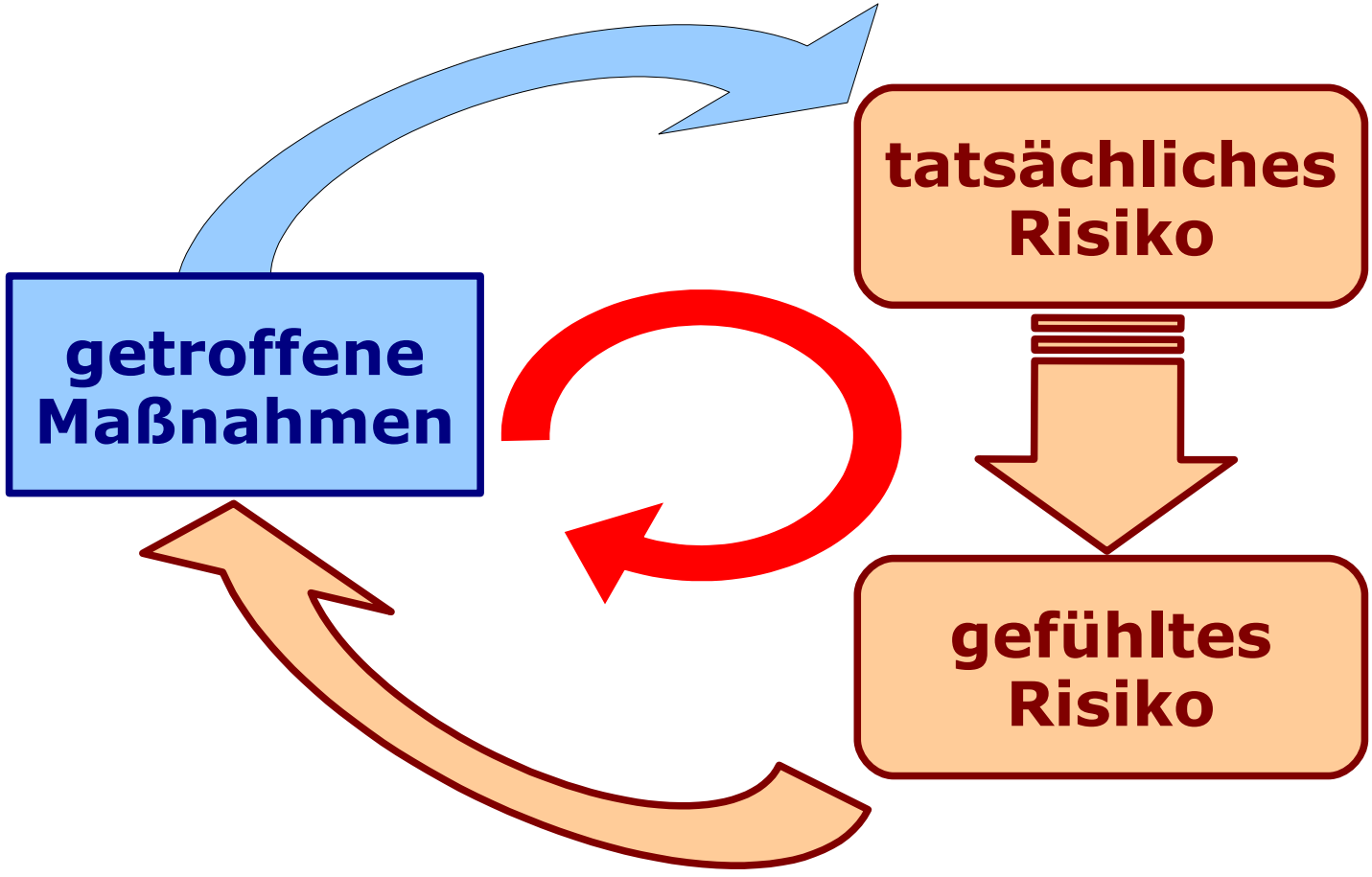
…feedback mechanisms may provide a systemic limit on the performance of some risk reduction systems

– Anderson (2001 p. 493)

Planung, Umsetzung, Messung - revisited



Das Risiko-Thermostat



© 2017 by Klaus-Peter Kossakowski, Germany

„DIE“ Herausforderung für jedes CERT

- **Es muss „strategisches Lernen“ seiner Zielgruppe ermöglichen!**
  - Mentale Modelle sind stark, müssen aber langsam und beharrlich verändert werden
- **Feedback ist elementar:**
  - Verkürzung der Feedbackphasen
  - Vorwegnehmen des erwarteten Feedbacks
- **Nur eine Veränderung der Kultur innerhalb der Zielgruppe ermöglicht eine echte und nachhaltige Verbesserung!**

© 2017 by Klaus-Peter Kossakowski, Germany

Interessante Frage:

Was werden 2018 im Internet mit immer mehr IoT-Systemen die schwerwiegendsten Sicherheitsprobleme sein?

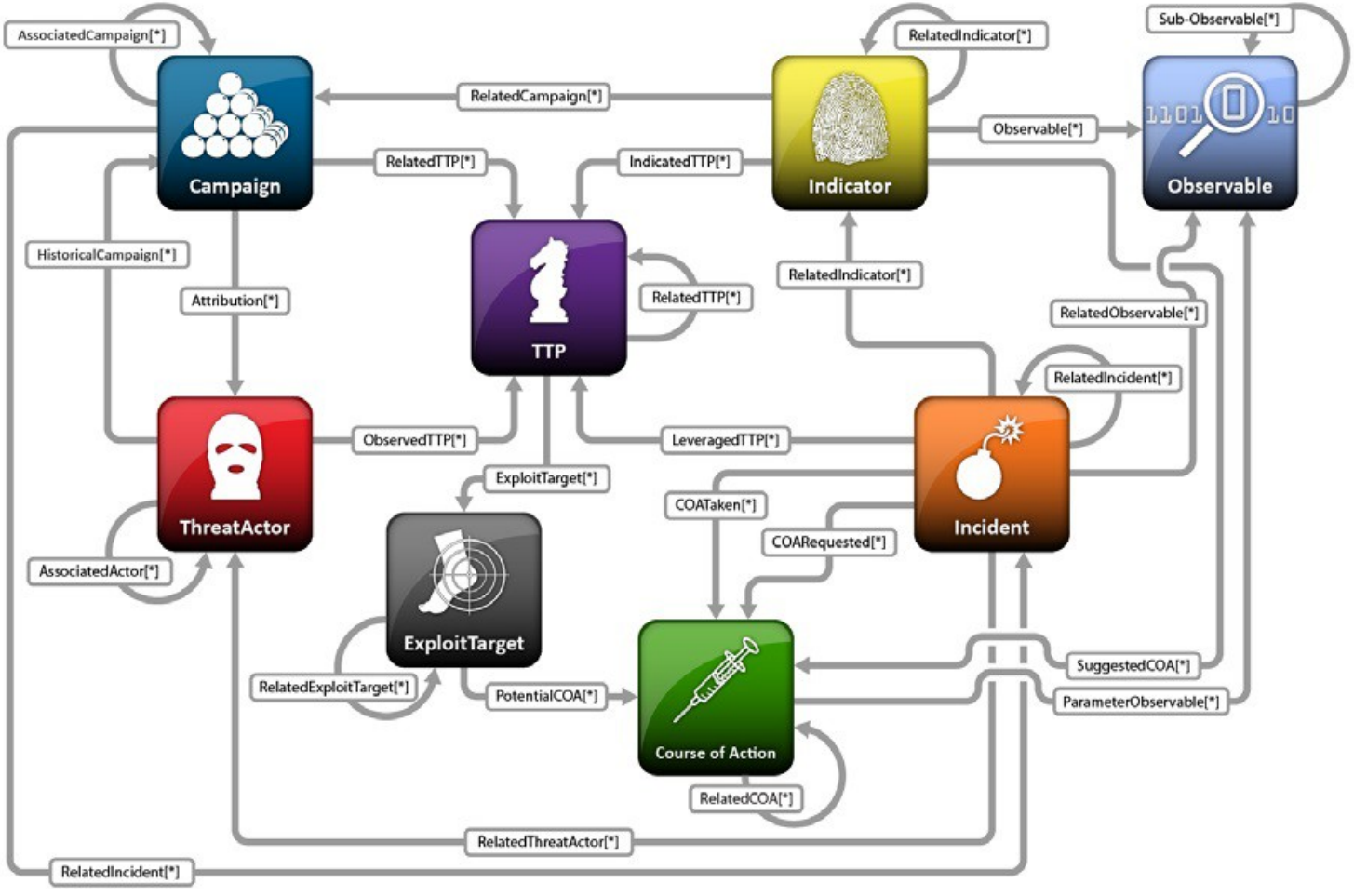
© 2017 by Klaus-Peter Kossakowski, Germany

Meine Antwort bleibt ...

- Schwache und/oder Klartext-Passworte
- Systeme mit Sicherheitslücken ohne angemessene Gegenmaßnahmen
- Viele ~~kreative~~ Benutzer, denen ihre gesetzlichen Möglichkeiten nicht ausreichen
- „Privateers“, die unter dem Schutz oder mit Förderung von Nationalstaaten die wirtschaftlichen und gesellschaftlichen Entwicklungen negativ beeinflussen

© 2017 by Klaus-Peter Kossakowski, Germany

Komplexität betrifft alle!



© 2017 by Klaus-Peter Kossakowski, Germany

Irgendwie klappt was nicht!

- **Eigentlich nimmt die Anzahl von Security Policies (u.ä.) immer weiter zu …**
  - Doch fehlende oder falsche Umsetzungen schließen nicht alle Lücken, die für Angriffe genutzt werden!

© 2017 by Klaus-Peter Kossakowski, Germany

Weiterhin viel zu viele Vorfälle!

- **Eigentlich nimmt die Anzahl von Security Policies (u.ä.) immer weiter zu …**
  - Doch fehlende oder falsche Umsetzungen schließen nicht alle Lücken, die für Angriffe genutzt werden!
- **Eigentlich sollte sich die Code-Qualität deutlich verbessert haben ...**
  - Aber weiterhin beruhen die meisten Exploits auf vermeidbaren Programmierfehlern!
  - „Plug-and-Pray“ verschärft die Problematik

© 2017 by Klaus-Peter Kossakowski, Germany

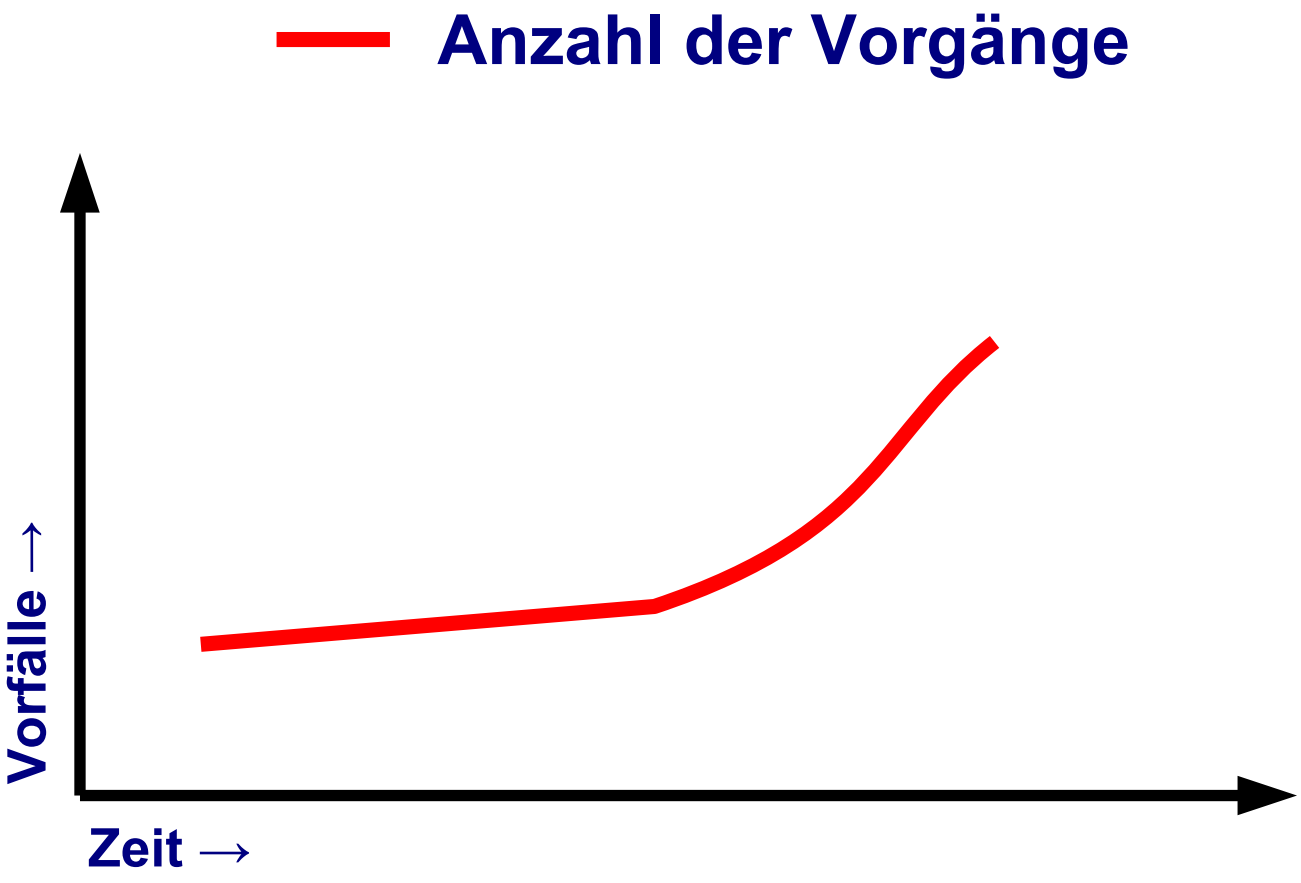
Und die Erkennung klappt auch nicht!

- Ungeachtet aller Monitoring- und Audit-Aktivitäten vergehen Tage, Wochen oder Monate, bis signifikante Vorfälle aufgedeckt werden!
- Und selbst dann fällt es selbst vorbereiteten Teams schwer
  - schnell (genug) und
  - effektiv

  darauf zu reagieren, weil wesentliche Informationen (z.B. Logs) fehlen

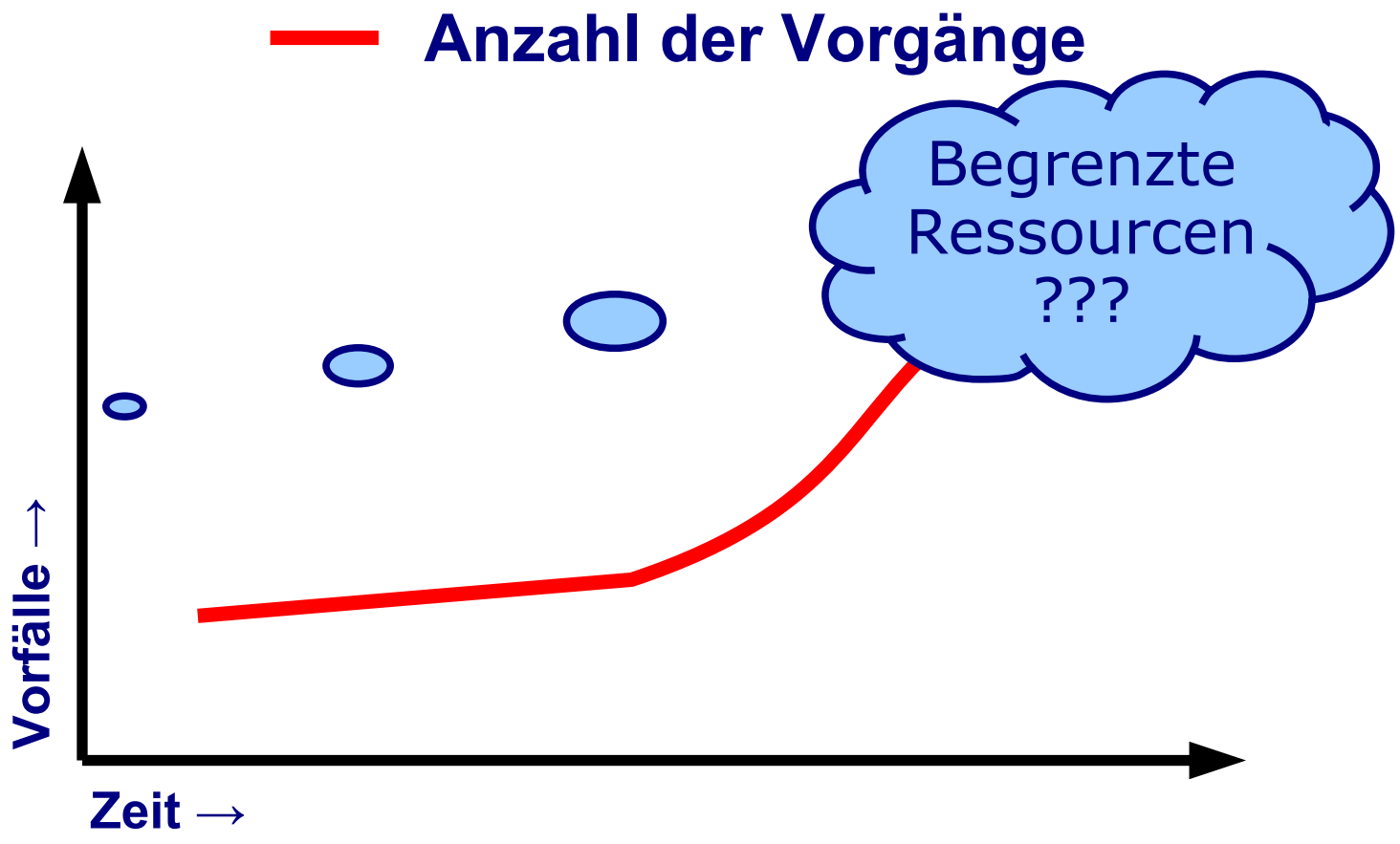
© 2017 by Klaus-Peter Kossakowski, Germany

Die Anzahl der Vorfälle / Vorgänge steigt



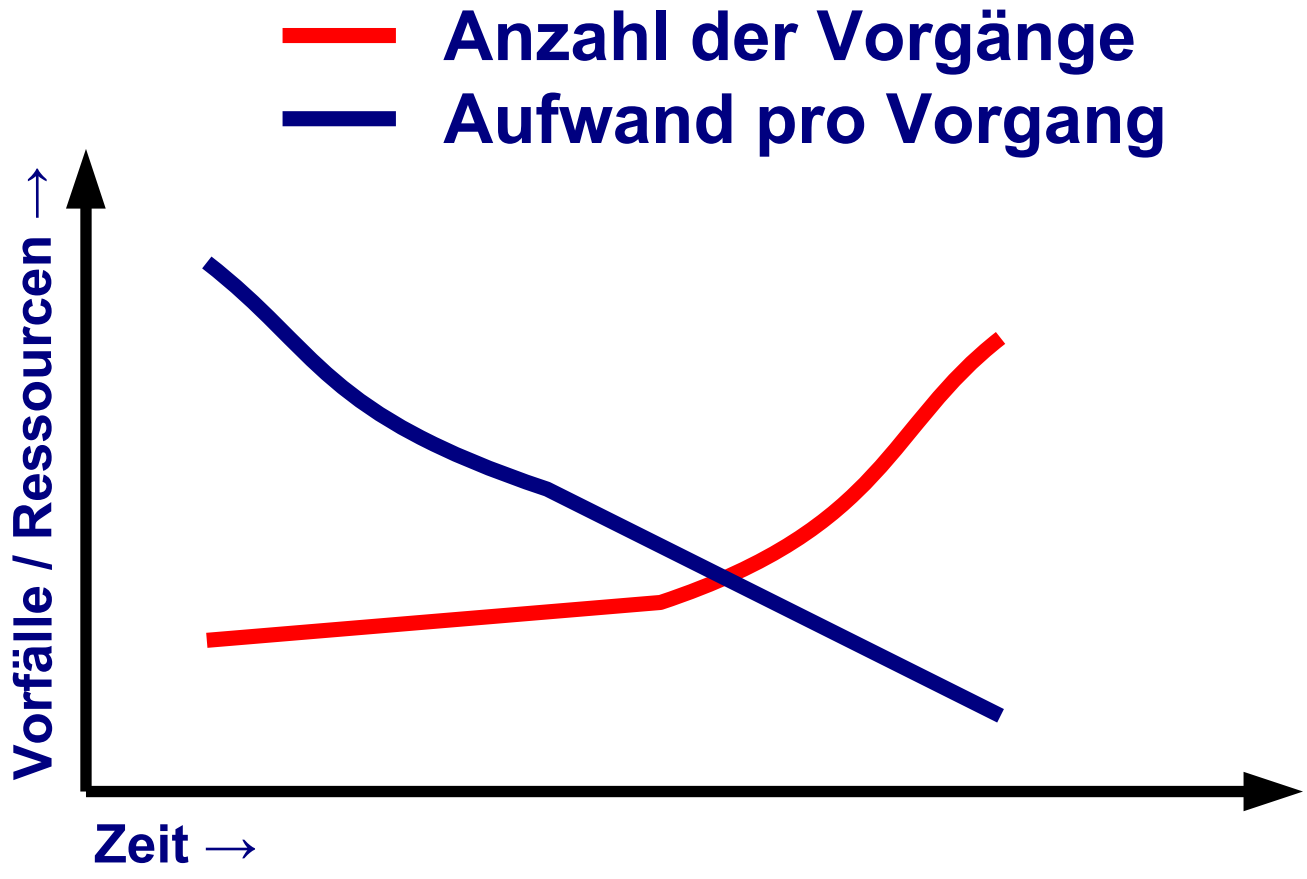
© 2017 by Klaus-Peter Kossakowski, Germany

Die Anzahl der Vorfälle / Vorgänge steigt



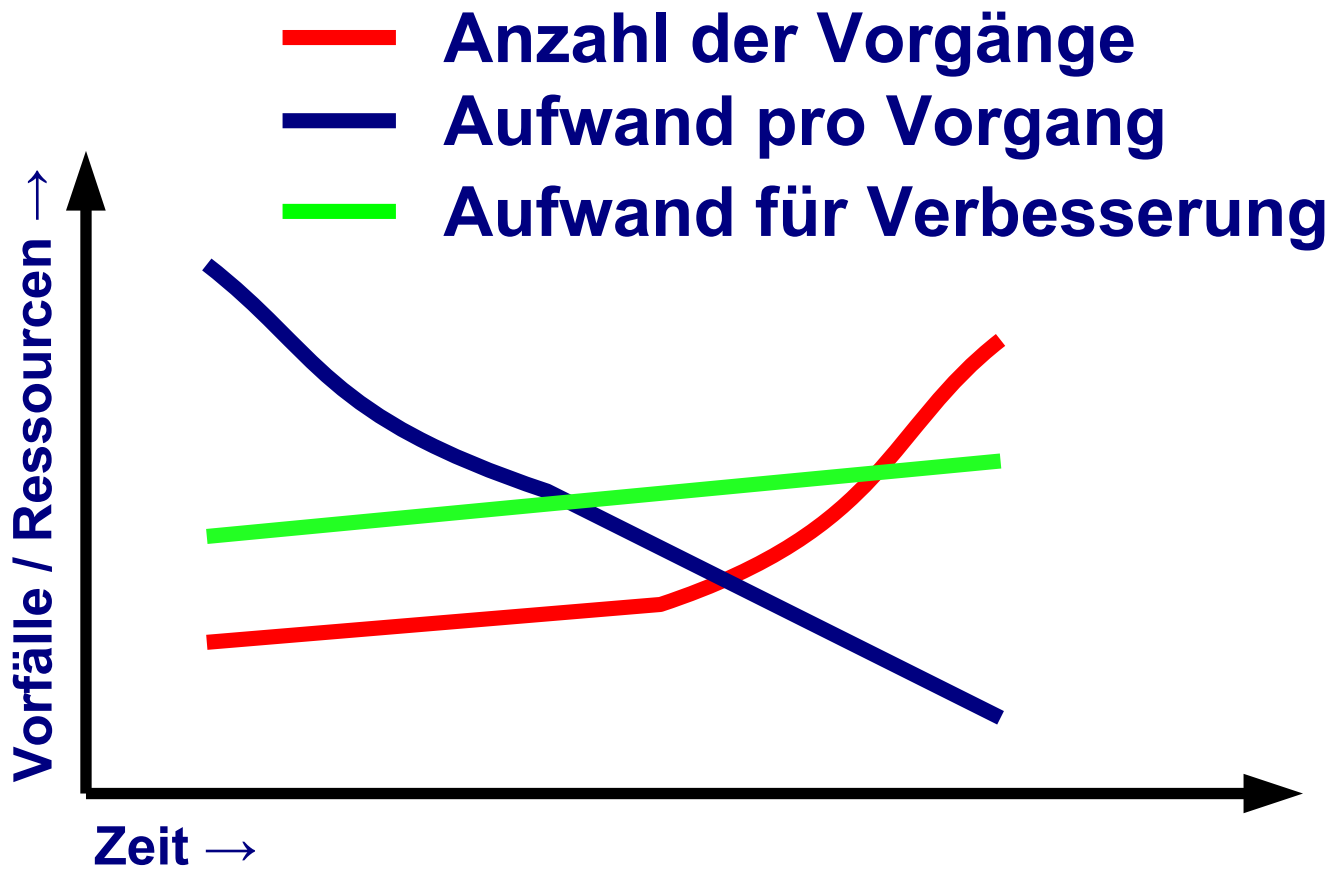
© 2017 by Klaus-Peter Kossakowski, Germany

Es ist wie bei einer guten Ärztin ...



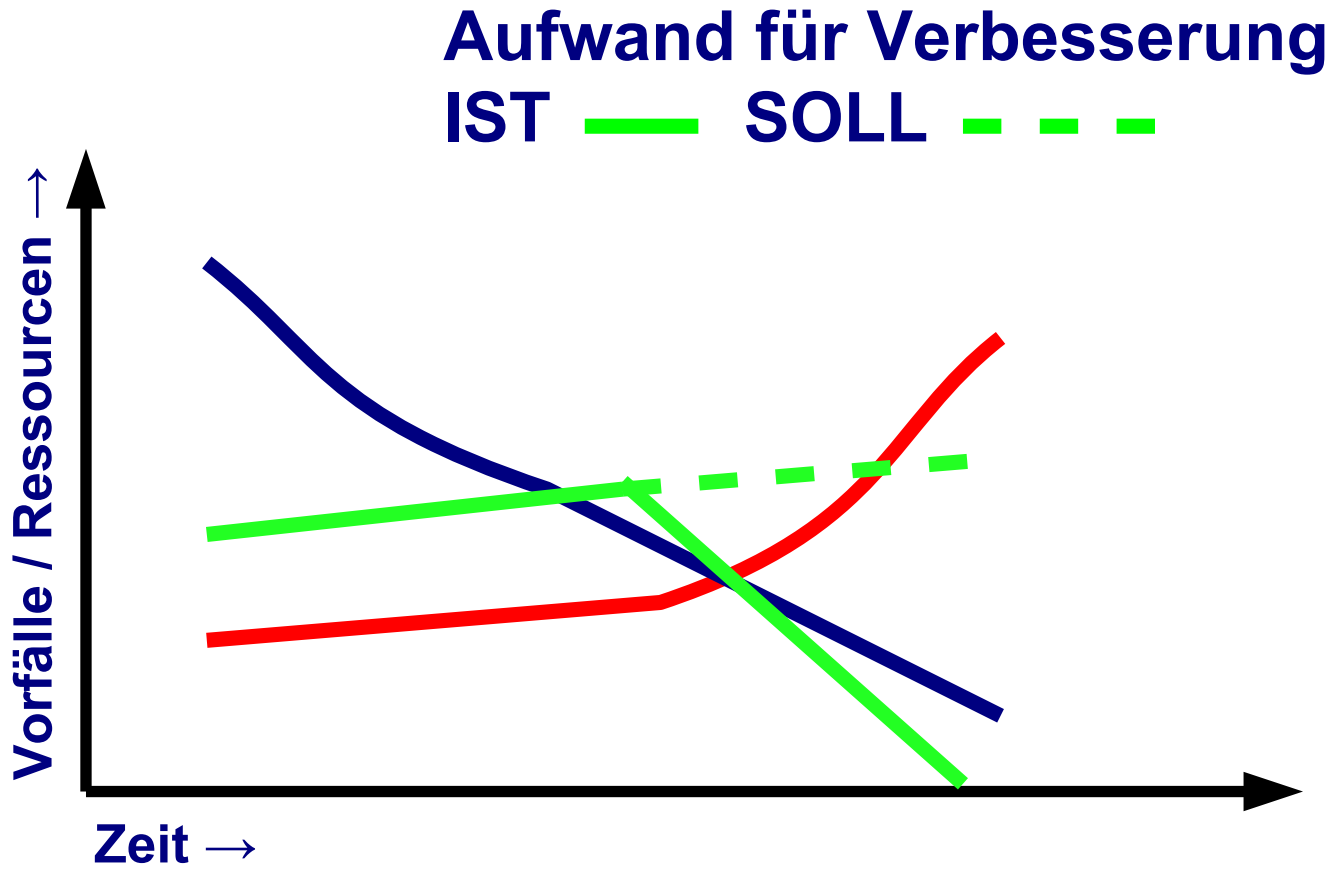
© 2017 by Klaus-Peter Kossakowski, Germany

Raum für Verbesserung muss her!



© 2017 by Klaus-Peter Kossakowski, Germany

Raum für Verbesserung muss her?



© 2017 by Klaus-Peter Kossakowski, Germany

Mehr Personal löst das Problem!

About the only common attributes between existing […] teams are that they are under-funded, under-staffed, and over-worked.

– Danny Smith, AUSCERT, 1994

© 2017 by Klaus-Peter Kossakowski, Germany

Unterstützung und stetige Verbesserung

- **Das strategische Ziel des CERT@VDE ist Stabilität und Mehrwert!**
  - Nachhaltige Service-Güte für möglichst viele der Zielgruppe!

    … und damit eine bessere Sicherheit für Kunden und auch alle Bürgerinnen/er
- **Ressourcen für Verbesserungen schaffen und erhalten!**
- **Feedback und Adaption basierend auf dem „Need to Share“**

© 2017 by Klaus-Peter Kossakowski, Germany

Kontakt

Prof. Dr. Klaus-Peter Kossakowski

Email: klaus-peter.kossakowski @haw-hamburg.de

Mobil: (+49) 0171 / 5767010

https://users.informatik.haw-hamburg.de/~kpk/

© 2017 by Klaus-Peter Kossakowski, Germany