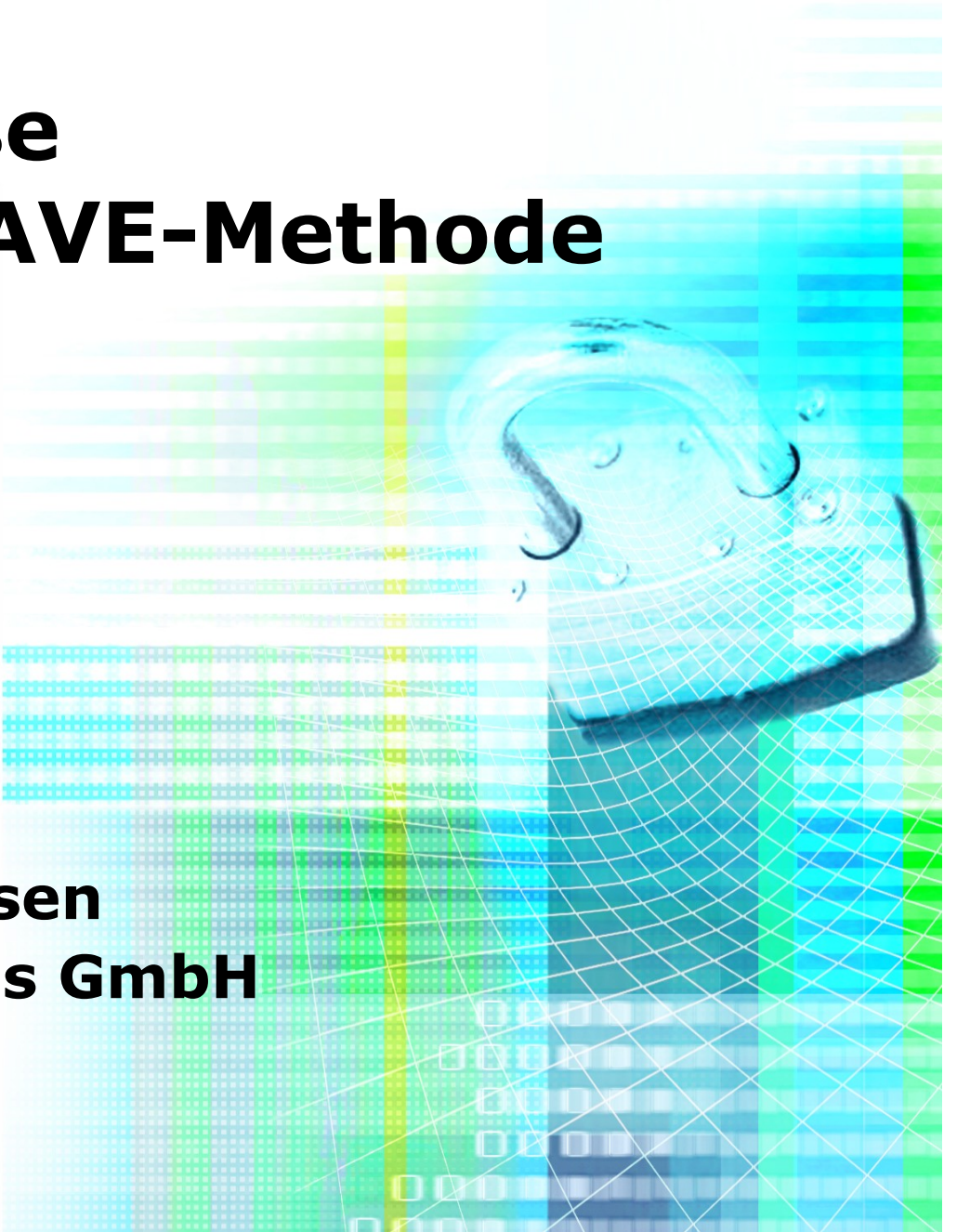
Risikoanalyse mit der OCTAVE-Methode



07.05.2013

Dr. Christian Paulsen
DFN-CERT Services GmbH

Bedrohungslage

Trends der Informationssicherheit:

- Hauptmotivation der Angreifer: Geld, Informationen
- Automatisierte Angriffe
- Social Engineering Angriffe, Phishing
- Ausnutzung von Schwachstellen in Software
- Drive-by Infektionen
- Mobile Datenträger
- Moderne Kriegsführung (Cyberwar)

Ausgangssituation

- **Problem:** Aktueller Stand hinsichtlich Informationssicherheit schwer einschätzbar

- Offene Fragen:
  - Welche Bedrohungen existieren?
  - Sind meine Schutzmaßnahmen ausreichend?
  - Erfülle ich alle rechtlichen und vertraglichen Vorgaben?
  - In welchen Bereichen muss ich nachbessern? Wo am dringendsten?

Ausgangssituation

- **Problem:** Aktueller Stand hinsichtlich Informationssicherheit schwer einschätzbar

- Offene Fragen:
  - Welche Bedrohungen existieren?
  - Sind meine Schutzmaßnahmen ausreichend?
  - Erfülle ich alle rechtlichen und vertraglichen Vorgaben?
  - In welchen Bereichen muss ich nachbessern? Wo am dringendsten?

Ausgangssituation

Lösungsmöglichkeiten:

- Durchführung einer Risikoanalyse
- Aufbau und Betrieb eines Informationssicherheitsmanagement-systems (ISMS)
- Informationssicherheit als Prozess verstehen
- Orientierung an Standards:
  - ISO 27001, IT Grundschutz, ITIL...
- Aber: Einstieg oft sehr schwierig!

Nachteile vorhandener Risikoanalyseverfahren

- Maßnahmenkataloge häufig zu umfangreich
- Wenig Unterstützung bei konkreter Durchführung der Analyse
- Häufig externe Expertisen ohne Einbeziehung der eigenen Mitarbeiter
- Nachhaltigkeit häufig nicht gegeben
- Schwerpunkt liegt zumeist auf technischen Prozessen --> betriebswirtschaftliche Sicht wird vernachlässigt!

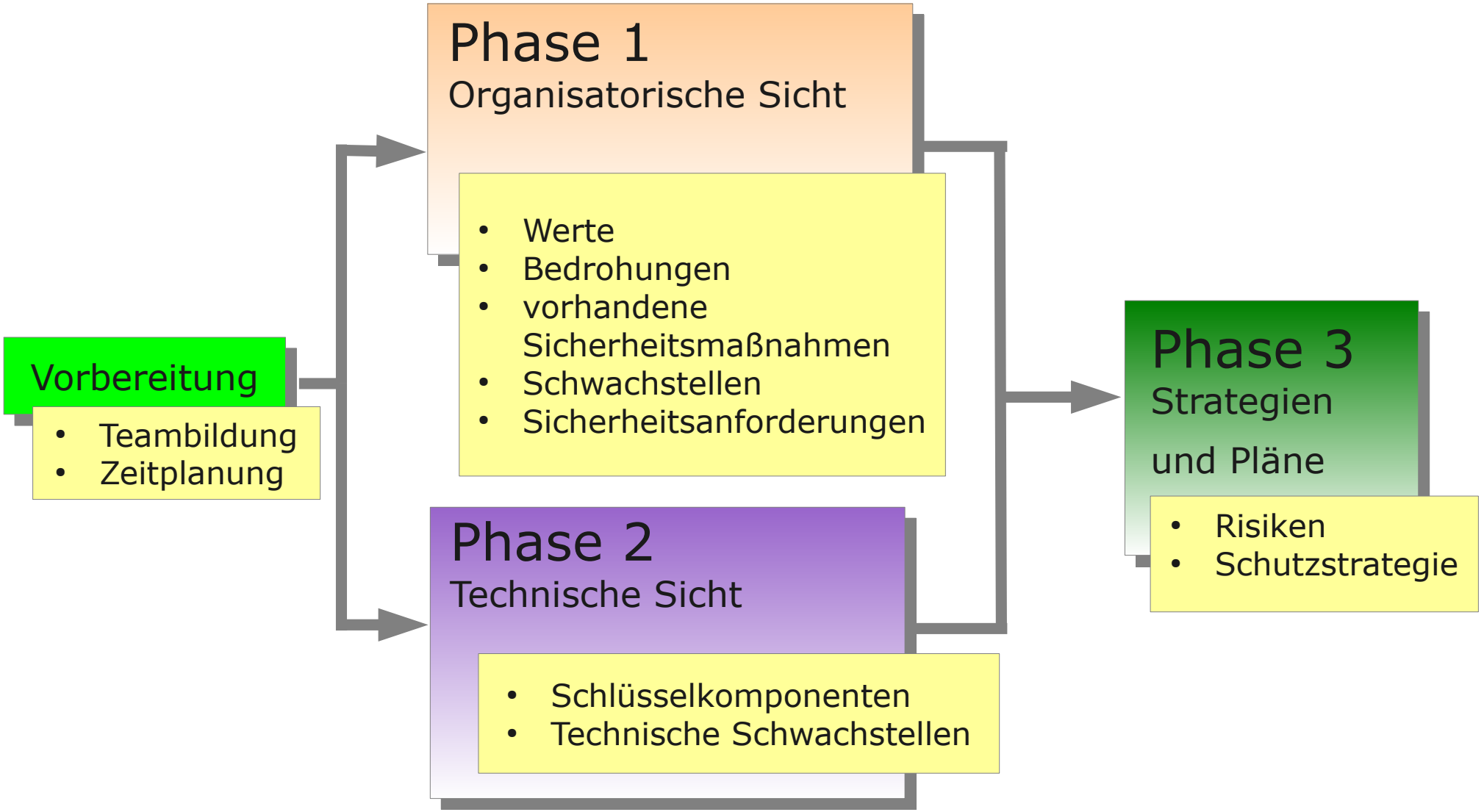
Was ist OCTAVE?

- **OCTAVE** =
  Operationally Critical Threat, Asset and Vulnerability Evaluation
- Entwickelt vom CERT/CC der Carnegie Mellon University
- Unterstützt den Anwender mit Formblättern, Checklisten, Moderationsplänen
- **Schwerpunkt: wertebezogene Analyse der Risiken und Sicherheitsprozesse**

Vorteile von OCTAVE

- Anwendung einer einheitlichen und transparenten Methode
- Maßgebliche Beteiligung aller Verantwortlichen (auch Leitungsebene)
- Berücksichtigung betriebswirtschaftlicher Aspekte
- Arbeitsblätter führen das Analyseteam durch die gesamte Evaluation
- Auswahl und Priorisierung geeigneter Schutzmaßnahmen

OCTAVE-Phasen



Auswahl der Teammitglieder

- Mitglieder sowohl aus dem IT-Bereich als auch aus den Organisations- und Anwendungsbereichen
- Planung einzelner Workshops mit unterschiedlichen Teams
- Ein Projektleiter für den Gesamtüberblick (optional: Unterstützung durch das DFN-CERT)

Phase 1 - Werte

- Identifizierung wichtiger Werte in der Organisation (Informationen, IT-Systeme, Anwendungen, Personen)

- Beispiel: Anwendungen / Dienste
  - Welche Anwendungen und Dienste benötigen die Mitarbeiter in Ihrem Unternehmen, um ihre Arbeit zu verrichten?

Phase 1 – Status Quo

- Welche Sicherheitsmaßnahmen sind bereits vorhanden?
- Jeweiligen Ampelstatus festlegen:

  - Rot: Nicht vorhanden, kritisch
  - Gelb: Vorhanden, verbesserungswürdig
  - Grün: Optimal
- Beispiel Zugangskontrolle:
  - Ein Schlüssel- und Passwortmanagement ist vorhanden?
  - Ja/z.T./Nein/nicht bekannt

Phase 1 – Kritische Werte

Auswahl der kritischen Werte:

- Welche Werte sind kritisch, d.h. es würde ein schwerwiegender Schaden entstehen, falls sie
  - nicht-autorisierten Personen in die Hände fallen?
  - ohne Berechtigung modifiziert werden?
  - verloren gehen oder zerstört werden?
  - nicht mehr erreichbar wären?

Phase 2

Identifizierung von Schwachstellen:

- Wie greifen Mitarbeiter auf die kritischen Werte zu?
- Welche Komponenten der IT-Infrastruktur sind den kritischen Vermögenswerten zuzuordnen?
- Welche technischen Schwachstellen sind vorhanden?

Phase 3

Entwickeln einer Sicherheitsstrategie:

- Was sind die Auswirkungen im Schadensfall?
- Welche Gegenmaßnahmen sind nötig?
- Welche Maßnahmen müssen kurzfristig/mittelfristig/langfristig umgesetzt werden?
- Welche Veränderungen sind für ein kontinuierliches Sicherheitsmanagement erforderlich?

Etablierte Best Practice Ansätze

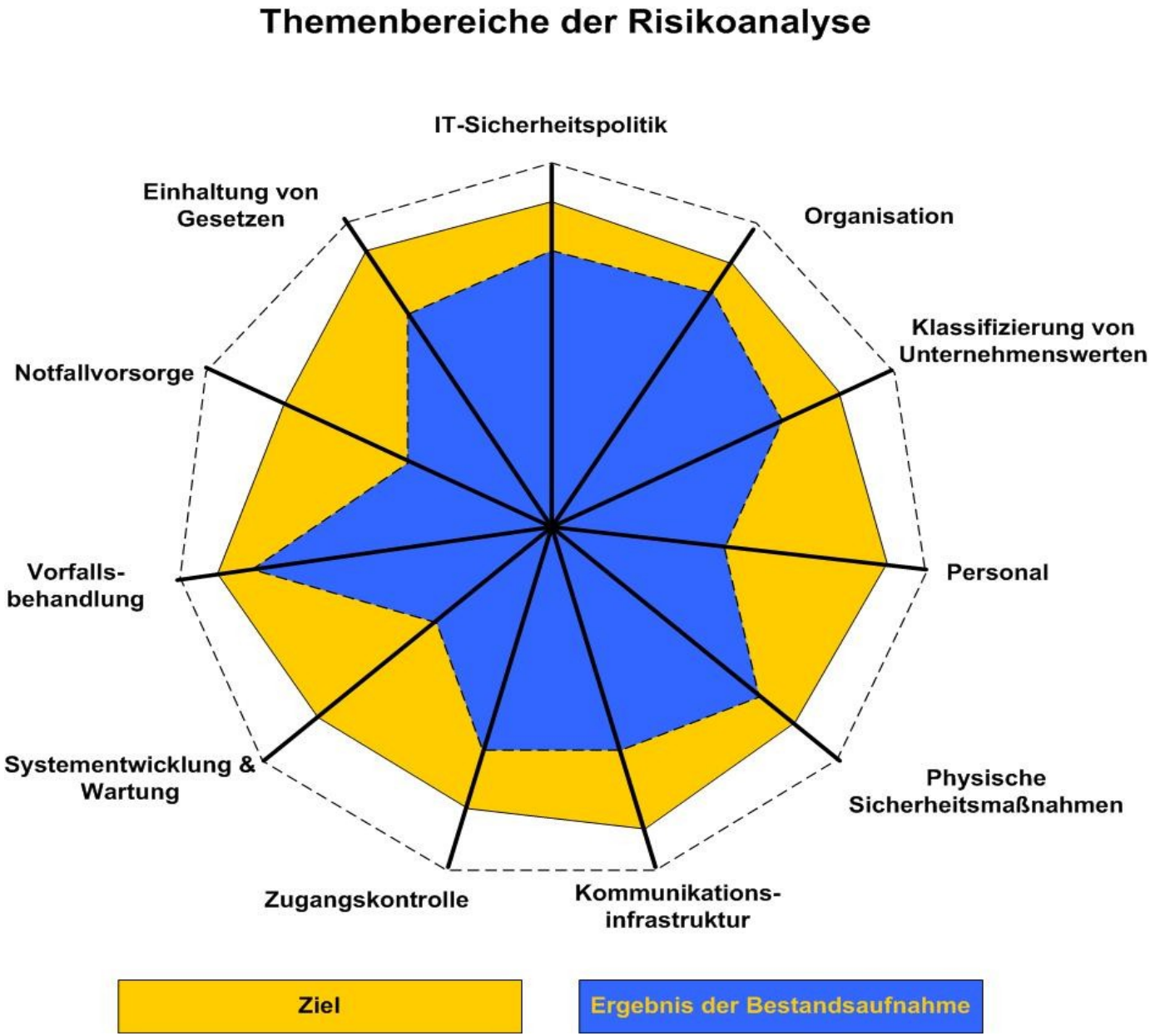
2. Organisation der Informationssicherheit	
Maßnahmenziele	**Leitfaden zur Umsetzung / potenzielle Maßnahmen**
Infrastruktur der Informations-sicherheit	Übernahme der Gesamtverantwortung für Informationssicherheit durch die Organisationsleitung – Betreitstellung eines angemessenen Budgets
	Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit – Informationssicherheitsmanagement / Richtlinienkompetenz
	Festlegung aller sicherheitsrelevanter Rollen und Verantwortlichkeiten
	Regelmäßige Überprüfung der getroffenen Sicherheitsmaßnahmen durch einen unabhängigen Auditor
	Etablierung von Kontakten zu anderen Informationssicherheitsorganisationen, Sicherheitsteams und ggf. staatlichen Stellen

Darstellung der Untersuchungsergebnisse

Fragestellungen:

- Was muss die Leitungsebene unternehmen, um eine erfolgreiche Umsetzung zu unterstützen?
- Wie kann die Umsetzung der Maßnahmen kontrolliert werden?
- Wann erfolgt die nächste Iteration der Analyse?
- Müssen weitere kritische Vermögenswerte betrachtet werden?

Weitere Schritte



Weitere Optionen

- OCTAVE ist nicht nur für die Erstellung von Risikoanalysen geeignet
- Weitere Anwendungsoptionen:
  - Dokumentation von Werten und Prozessen
  - Sicherheitsbewusstsein erhöhen
  - Schwachstellenanalyse (Status Quo), um den Handlungsdruck zu erhöhen
  - Analyse unterschiedlicher Organisationsbereiche (Skalierbarkeit)
  - Vorbereitung einer ISO 27001-Zertifizierung

Risikoanalyse mit OCTAVE

- Arbeitsunterlagen
  - Arbeitsblätter
  - Leitfaden zur Umsetzung
- Tutorien
  - 1-2 pro Jahr
  - Individuell vor Ort
- Begleitung der Analyse
  - Drei Leistungspakete
- OCTAVE-Tool „ADORA“

DFN CERT®

Vielen Dank
für die Aufmerksamkeit!

Fragen?

Dr. Christian Paulsen
https://www.dfn-cert.de/
octave@dfn-cert.de