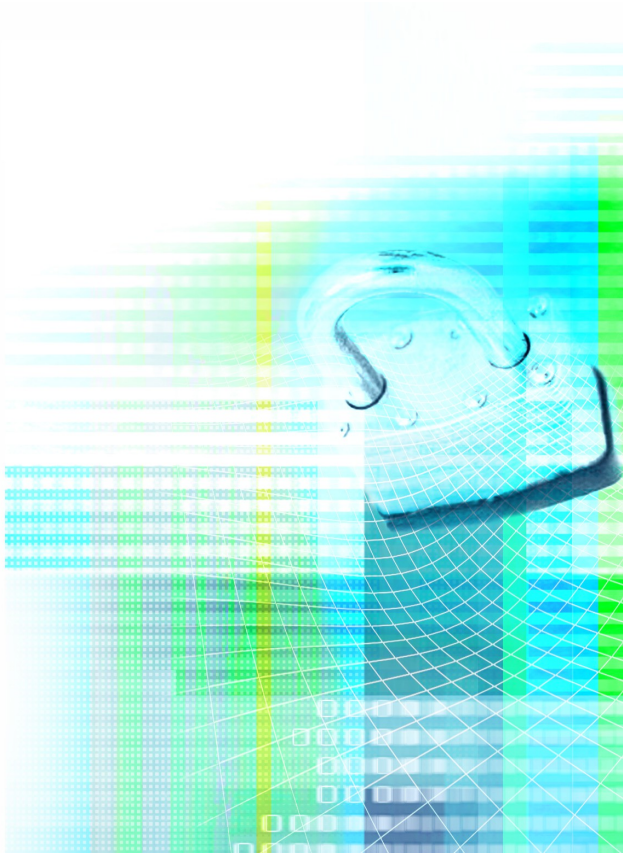
Wie sicher bin ich eigentlich? Security Management mit OCTAVE

Regensburg / 22. Mai 2012

DFN-CERT Services GmbH
Dr. Klaus-Peter Kossakowski
kossakowski@dfn-cert.de



Agenda

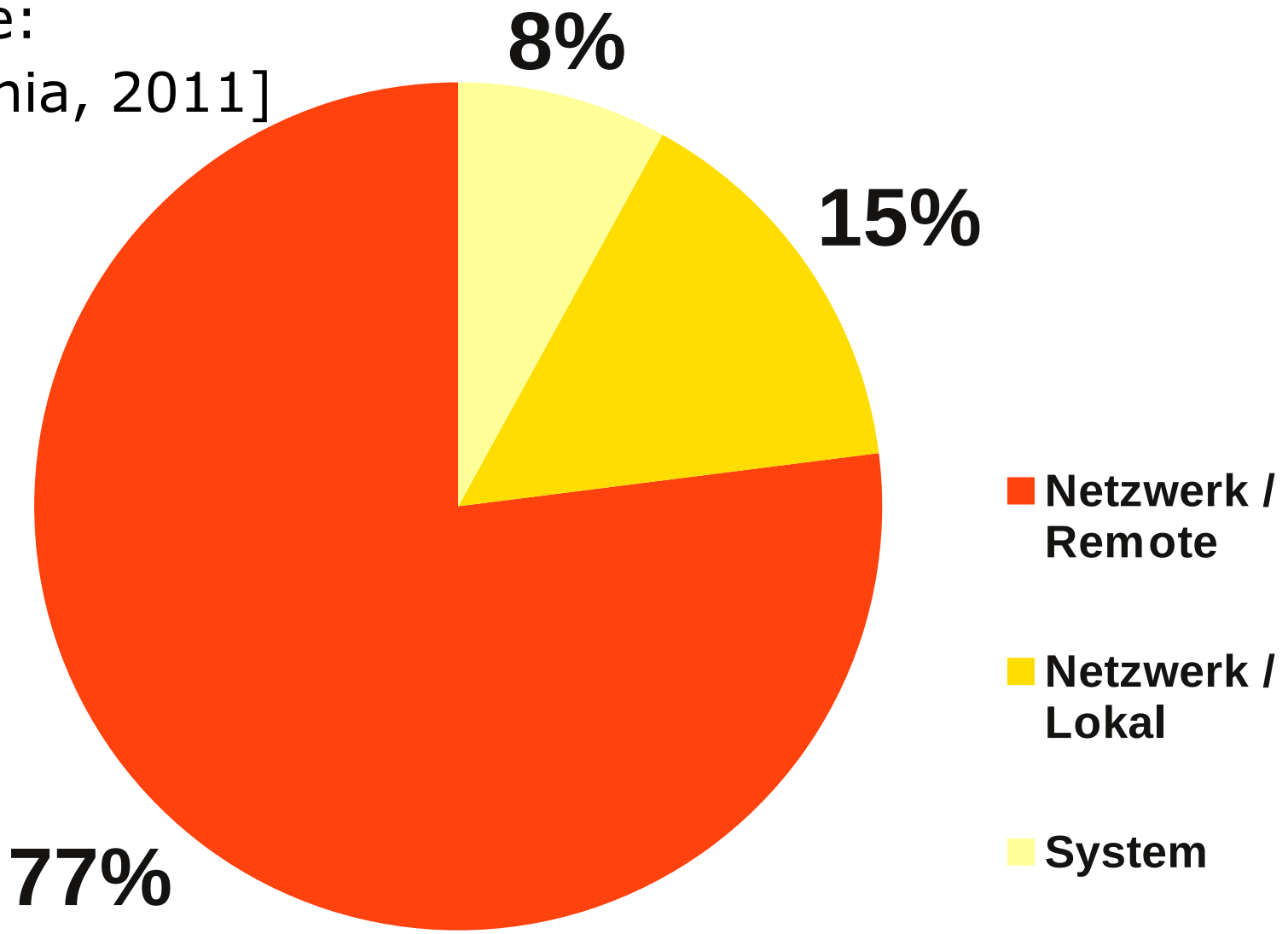
- **Bedrohungen der IuK-Sicherheit**
  - **durch alte und neue Schwachstellen**
  - **durch neue Konvergenzen**
  - **auch ohne Sicherheitslücken**
- **Bewertung der eigenen Sicherheit**
- **Was ist zu tun?**

Schwachstellen

- **Auch die großen Anbieter (Adobe, Apple, Google, Microsoft, Skype) konnten die Zahl der Schwach-stellen nicht wirksam verringern.**
  - **Auch wenig verbreitete Software hat Lücken, die ausgenützt werden.**
- **Je mehr Software läuft, desto höher ist das Angriffspotential.**
  - **Fast jede Software bringt eigene Update-Mechanismen mit sich.**

Schwachstellen (2)

[Quelle:
Secunia, 2011]



Schwachstellen (3)

- **Quartalspatchday im April 2012:**
  - **Insgesamt 88 Schwachstellen**
  - **Darunter auch für das „Flagschiff“, die Oracle-Datenbanklösung**
- **Eine der Schwachstellen wurde bereits 2008 gemeldet**
  - **Der damalige Entdecker veröffentlicht Details zur Erkennung / Überprüfung**

… und dann stellt sich raus, dass der Patch nicht wirkt !

Schwachstellen (4)

- **Reaktion im April 2012:**
  - **Eine dynamische Funktion abstellen**
  - **Ein teures Zusatzpaket – das sowieso grundsätzlich zu empfehlen ist – nachkaufen**

… und dann mehrere Monate auf einen richtigen Patch warten !

Schwachstellen (5)

- **Entgegenkommen im Mai 2012:**
  - **Das sonst teure Zusatzpaket – das sowieso grundsätzlich zu empfehlen ist – kann ohne Kosten eingesetzt werden**

… aber ob jetzt der Patch noch kommt?

[http://www.heise.de/security/meldung/Oracle-Datenbanken-anfaellig-fuer-eingeschleuste-Lauscher-1563022.html]

[http://www.heise.de/security/meldung/Oracle-aendert-Lizenzmodell-wegen-verplapperter-Sicherheitsluecke-1564995.html]

Schwachstellen (6)

- **Flash: Malware**
  - **Erhalt einer Email mit infiziertem Anhang**
  - **Wird der Anhang geöffnet, wird die Malware aktiv und macht den Rechner aus dem Internet erreichbar**

[http://www.heise.de/security/meldung/Adobe-schliesst-kritische-Flash-Luecke-nach-Angriffen-1568649.html]

Neue Konvergenzen

- **Heute (oder in naher Zukunft) wird alles ans Internet angeschlossen!**
- **Wichtige Themen für alle:**
  - **Smartphones**
  - **Netzwerkdrucker**
  - **Facility Management**
- **Selbst bei etablierten Sicherheits-konzepten bleibt Handlungsbedarf!**

Neue Konvergenzen (2)

- **Smartphone am PC**
  - **Mitgebracht werden Filme, Musik, ...**
  - **Aber evtl. ist schon eine Malware drauf**
- **Gilt in gleicher Form für USB-Sticks, Wechselplatten, ...**
- **Allerdings kann ein Smartphone auch mehr**
  - **Verbindung zum Internet via UMTS**
  - **Neuer Zugang zum internen Netz an der Firewall vorbei?**

Neue Konvergenzen (3)

- **Bei Sicherheitsanalysen gefunden:**
  - **Netzwerkdrucker reagieren auf die Portabfragen aus dem Internet**
  - **Erkannt wird ein Web-Server**
- **Auf Nachfrage kam heraus:**
  - **Die IT-Abteilung war nicht für Drucker verantwortlich!**
    - Sicherheitsupdates gab es bisher nicht
  - **Die Nutzer wussten nichts von den vielfältigen Möglichkeiten!**

Auch ohne Lücken

- **Selbst wenn es keine Schwach-stellen oder offene Flanken gibt, sind Angriffe effektiv möglich!**
- **Die Ansatzpunkte der Angreifer sind dabei unterschiedlich:**
  - **Unschuldige Personen, die manipuliert werden, um Zugang zu erreichen**
  - **Öffentlich erreichbare Dienste, um diese zu stören**

Nutzer-Manipulation

- **Die Menschen haben kritische Informationen und Zugänge!**
- **Gelingt es dem Angreifer, die Identität des Nutzers vorzutäuschen**
  - **stehen ihm viele Möglichkeiten offen**
  - **können bestehende Schranken umgangen werden**
- **Vielfältige Beispiele:**
  - **Phishing, Malware, Drive-by-Exploits**

Nutzer-Manipulation (2)

- **Android: Drive-by**
  - **Besuch einer infizierten Seite startet automatisch den Download einer Installationsdatei Update.apk**
  - **Wird der Installer dann vom Nutzer gestartet, wird ein Sicherheitsupdate "com.Security.Update" präsentiert**

[http://www.heise.de/security/meldung/Android-Malware-oeffnet-Hintertuer-ins-Intranet-1566356.html]

Überlast bei Diensten

- Der Zugang zu Diensten stellt die Nutzung sicher und erlaubt erst eine Wertschöpfung!
- Gelingt es dem Angreifer, diesen Zugang zu blockieren
  - ist dies im Internet üblicherweise auch für Dritte sichtbar
  - können legitime Nutzer nicht arbeiten
- Vielfältige Beispiele:
  - DDoS, Flash Crowds, Slash-Dot Effect

Agenda

- Bedrohungen der IuK-Sicherheit
- Bewertung der eigenen Sicherheit
  - Schwierigkeit der eigenen Situation
  - Vorteile von OCTAVE
  - Vorgehen mit OCTAVE
  - Erfahrungen beim Einsatz
- Was ist zu tun?

Wo stehe ich ???

- **Wie sicher wir sind, ist nur schwer einschätzbar!**
  - **Welche Bedrohungen existieren?**
  - **Welche davon betreffen mich?**
  - **Reichen meine Schutzmaßnahmen aus?**
  - **Erfülle ich alle rechtlichen und vertraglichen Vorgaben?**
  - **In welchen Bereichen muss ich nachbessern?**
  - **Und wo fange ich an?**

Womit fange ich an???

- Durchführung einer Risikoanalyse?
  - Beratungsunternehmen mit eigenen Verfahren
  - Grundschutz gemäß BSI
- Aufbau und Betrieb eines Information Security Management Systems (ISMS)?
  - ISO 27001 mit oder ohne BSI
- Besser alles in ITIL integrieren?

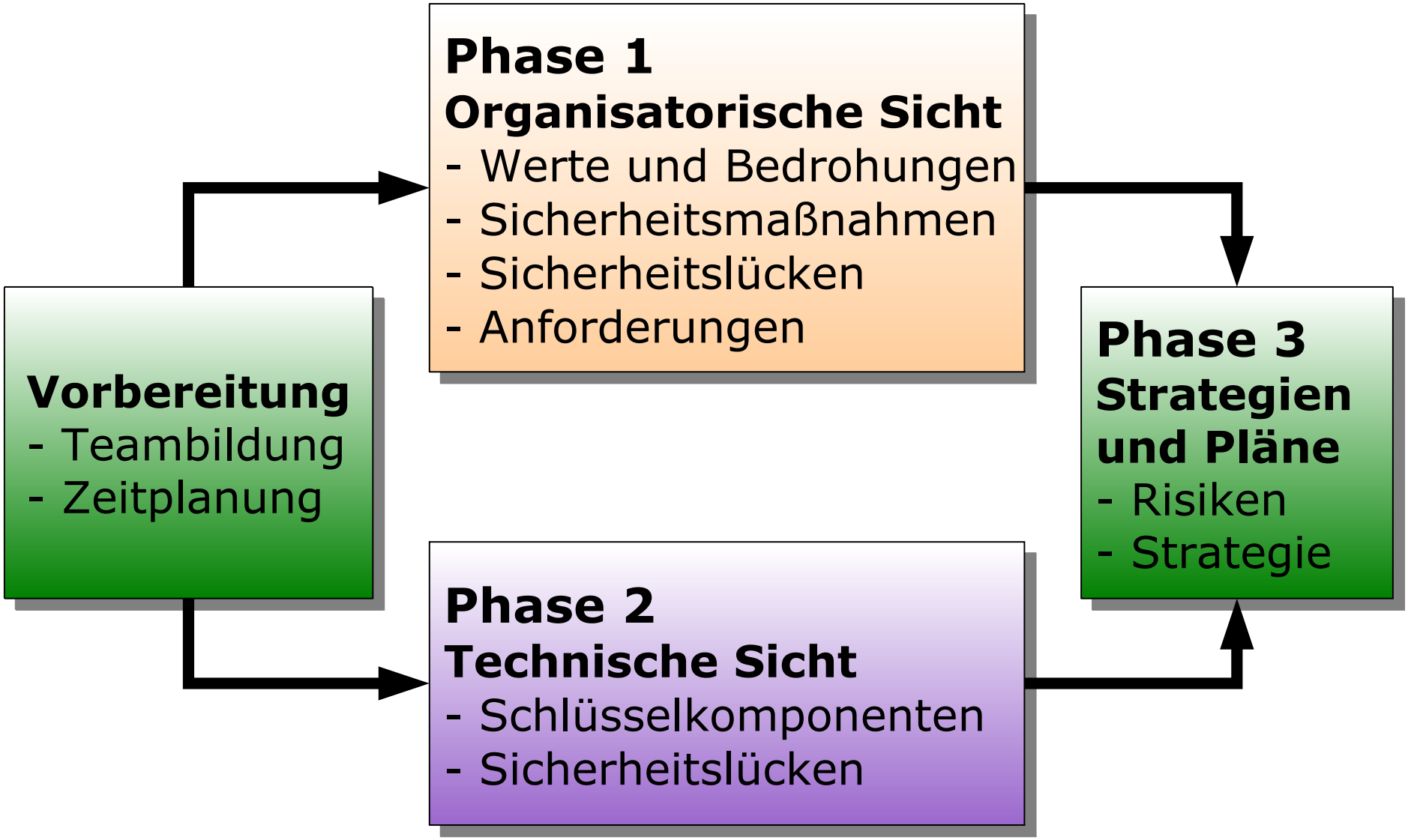
Aber nicht so einfach!

- **Maßnahmenkataloge (wie Grundschutz) häufig zu umfangreich!**
  - **Außerdem wenig Unterstützung bei eigener Durchführung solcher Analyse!**
- **Externe Sicherheitsexperten ohne Einbeziehung eigener Fachkräfte!**
  - **Keine Nachhaltigkeit gegeben!**
- **Konzentration auf die Technik!**
  - **Keine Sicht auf Geschäftsprozesse!**

Unser Ansatz: OCTAVE

- **Hilfe zur Selbsthilfe:**
  - **Leitfäden und Werkzeuge auf Deutsch**
  - **ISO2700x kompatibele Fachbegriffe und Kategorien**
- **Kombination von Verfahren und Technik:**
  - **Einbeziehung der Anwender**
- **Iterative Vorgehensweisen:**
  - **Auswahl der nächsten Schritte**
  - **Dokumentation fürs nächste Mal**

OCTAVE-Phasen



Vorbereitung

- **Auswahl der Teammitglieder**
  - **Mitglieder sowohl aus dem IT-Bereich**
  - **als auch aus den Organisations-**
  - **und Anwendungsbereichen**
- **Projektleiter für die Organisation und Vorbereitungen der Workshops**
- **Planung einzelner Workshops mit unterschiedlichen Teams**

Phase 1: Werte

- **Identifizierung wichtiger Werte in der Organisation**
  - **Informationen**
  - **IT-Systeme**
  - **Anwendungen**
  - **Prozesse**
  - **Personen**
- **Typische Fragen:**
  - **Welche Anwendungen und Dienste werden benötigt, damit die Arbeit verrichtet werden kann?**

Phase 1: Kritische Werte

- **Auswahl der kritischen Werte: Entsteht ein schwerwiegender Schaden falls etwas ...**
  - **in den Besitz nicht-autorisierter Personen gelangt?**
  - **manipuliert wird?**
  - **verloren geht oder zerstört wird?**
  - **nicht mehr erreichbar ist?**

Phase 1: Maßnahmen

- **Was ist bereits vorhanden?**
  - **Rot: Nicht vorhanden, kritisch**
  - **Gelb: Vorhanden, zu verbessern**
  - **Grün: Vorhanden, gut**
- **Beispiel Zugangskontrolle:**
  - **Ein Schlüsselmanagement ist vorhanden!**
  - **Ein Passwortmanagement ist vorhanden!**
  - **Ein Identity-Management fehlt!**

Phase 2: Technische Sicht

- **Identifizierung von Schwachstellen:**
  - **Wie greifen Mitarbeiter auf die kritischen Werte zu?**
  - **Welche Komponenten der IT-Infrastruktur sind den kritischen Werten zuzuordnen?**
  - **Welche technischen Schwachstellen sind vorhanden?**
    - Systeme
    - IT-Infrastruktur

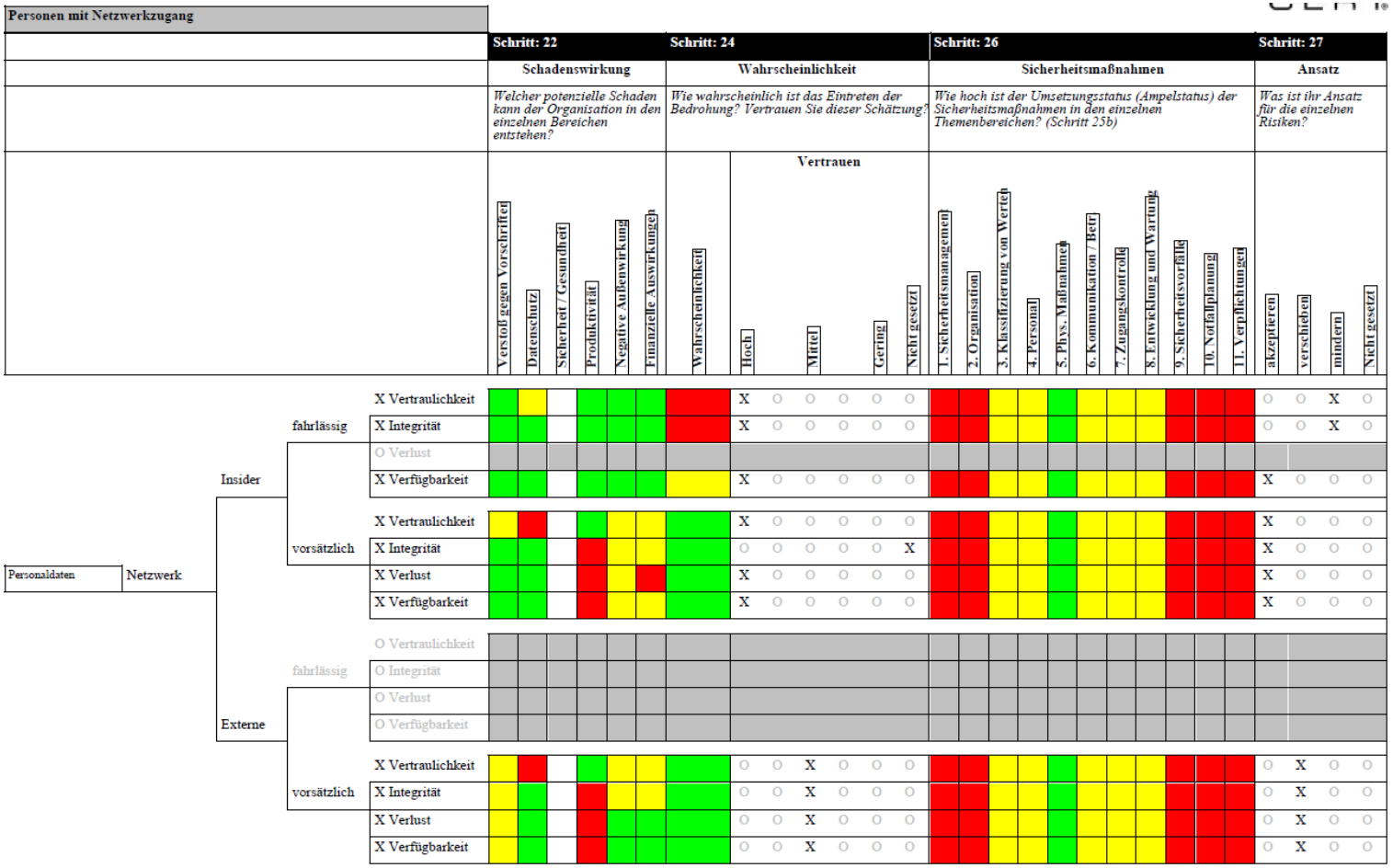
Alles im Überblick!

Themengebiet	Ampelstatus
Informationssicherheitsmanagement und Informationssicherheitspolitik	
Organisation	
Klassifizierung und Kontrolle von Werten	
Personal	
Physische Sicherheit	
Kommunikation und Betrieb	
Zugangs- und Zugriffskontrolle	
Entwicklung und Wartung	
Behandlung von Sicherheitsvorfällen	
Notfallplanung - Business Continuity	
Einhaltung von Verpflichtungen	

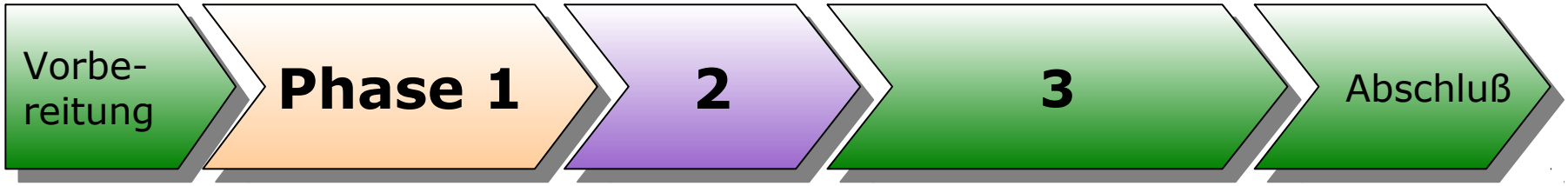
Phase 3: Strategie

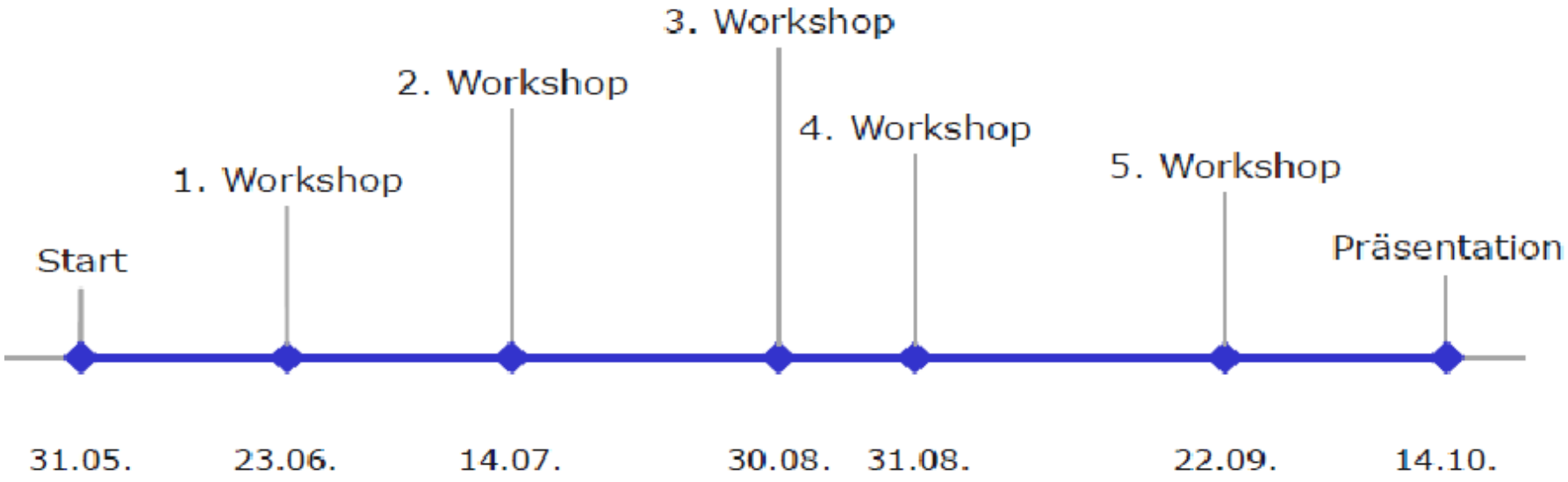
- **(Weiter-) Entwickelung einer Sicherheitsstrategie:**
  - **Wie bekommen wir die Auswirkungen im Schadensfall in den Griff?**
  - **Welche Schutzmaßnahmen brauchen wir noch? Und wie dringend?**
  - **Welche Verfahrensanweisungen und Zusicherungen brauchen wir noch?**
  - **Wie bekommen wir ein kontinuierliches Sicherheitsmanagement hin?**

Phase 3: Übersichtsblatt



Projekt an der Uni Leipzig





Projekt an der Uni Leipzig

Zu verbessernde Themenbereiche

Übergeordnete Bereiche

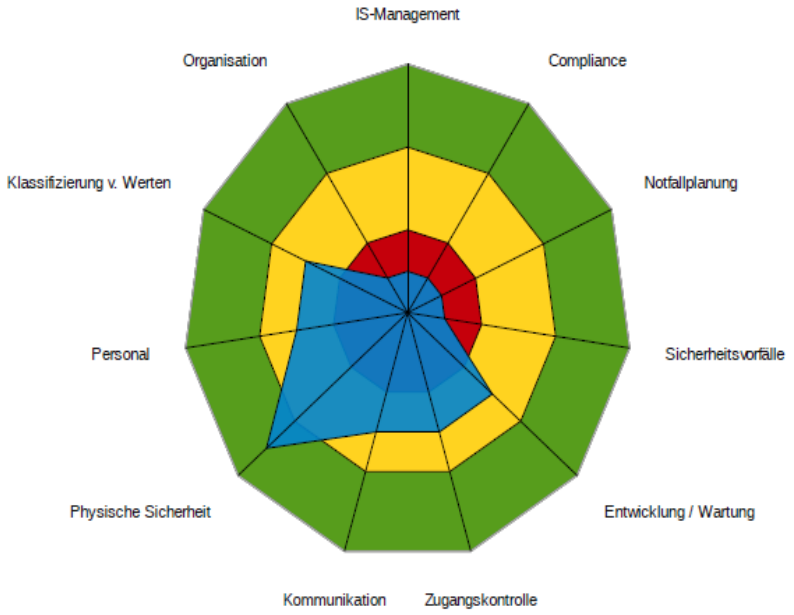
- Informationssicherheitsmanagement
- Organisation
- Behandlung von Sicherheitsvorfällen

Verwaltungsbezogene Bereiche

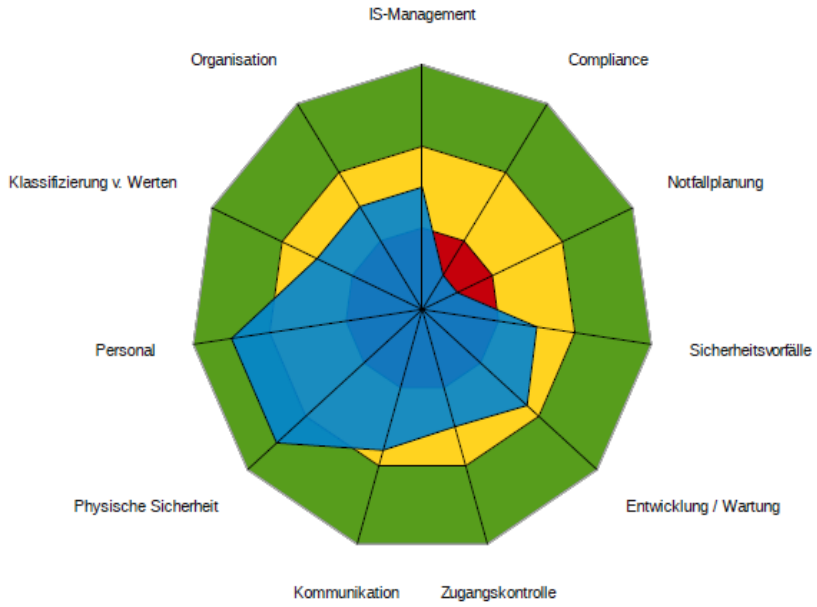
- Personelle Sicherheit
- Kommunikation und Betrieb
- Entwicklung und Wartung

Projekt an der Uni Leipzig

Sicherheitsstatus aktuell



Sicherheitsstatus – Soll



Und danach?

- Zunächst identifizierte Projekte abschließen!
- Danach neue Iteration, aber:
  - Vorherige Daten über die eigene Situation sind bereits verfügbar
  - Projektleiter kennt das Verfahren
  - Ablauf ist bereits eingeübt
- Audits oder Zertifizierung nötig?
  - Richtige Terminologie
  - Daten bereits verfügbar

Agenda

- Bedrohungen der IuK-Sicherheit
- Bewertung der eigenen Sicherheit
- Was ist zu tun?

Nicht ob, sondern wie!

- **IuK-Sicherheit zu erreichen ist primär kein technisches Problem!**
  - **Vorgaben, Verfahren, Prozesse**
  - **Menschen, Menschen, Menschen**
- **IuK-Sicherheit ist kein Selbstzweck sondern eine Grundanforderung**
  - **Qualitätsmerkmal der Infrastruktur**
  - **Fehlende IuK-Sicherheit schadet allen**
- **IuK-Sicherheit wird eingefordert!**

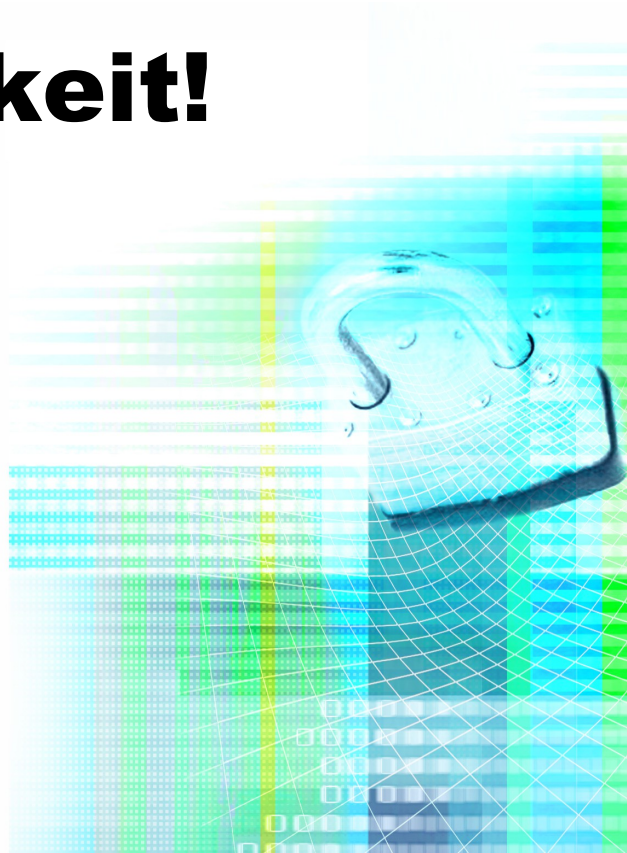
Was ist zu tun?

- **Eigene Strategien entwickeln**
  - **Sicherheitslinien nutzen**
  - **Risiken identifizieren und angehen**
  - **z.B. mit OCTAVE**

    https://www.dfn-cert.de/kooperationen/octave.html
- **Eigenes Sicherheitsmanagement ausbauen**
  - **z.B. neue Prozeßbausteine des DFN-Vereins einbauen**

Danke für
Ihre Aufmerksamkeit!

DFN-CERT Services GmbH
Dr. Klaus-Peter Kossakowski
kossakowski@dfn-cert.de



DFN CERT®

Ultimate Excellence lies
not in winning
every battle but
in defeating the enemy
without ever fighting!

Sun Tzu