T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting 2013
Berlin, 04. - 05.11.2013

Werte- und prozessorientierte Risikoanalyse mit OCTAVE

Christian Aust
.consecco

Dr. Christian Paulsen
DFN-CERT

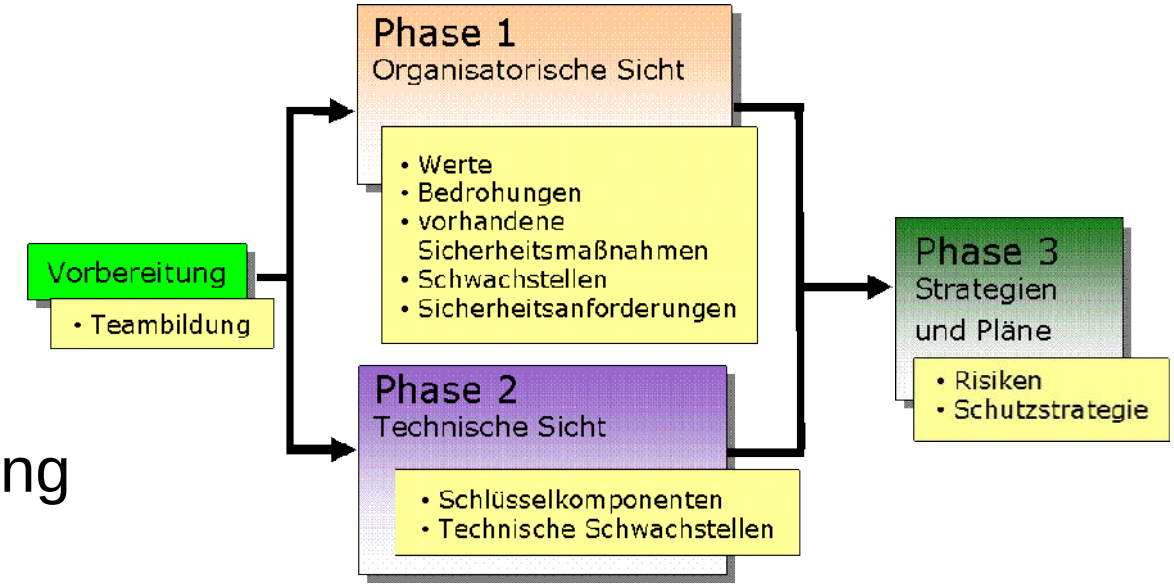
Was Sie erwartet…

- Vorstellung von OCTAVE:
  Methodik, Phasen, Aktivitäten
- Toolunterstützung bei OCTAVE

Was ist OCTAVE?

- **Operationally Critical Threat, Asset and Vulnerability Evaluation**
- Anschauliche Methode zur wertebezogenen Analyse von Risiken und Sicherheitsprozessen
- Entwickelt vom CERT/CC der Carnegie Mellon University
- Unterstützung der Anwender durch ausführliche Anleitungen, Formblätter, Checklisten, Moderationspläne
- Vom DFN-CERT ins Deutsche übersetzt, gekürzt und an ISO 27001 angepasst
- Toolunterstützung durch DFN-CERT möglich

OCTAVE-Ablauf: die Struktur



- **3 Phasen** plus Vorbereitung
- **5 Prozesse S1 bis S5**
  - P1, S1: Bewertungskriterien, Werte, vorhandene Maßnahmen
  - P1, S2: Auswahl kritischer Werte mit Anforderungen und Bedrohungen
  - P2, S3: Erfassung der IT-Infrastruktur und ihrer Schwachstellen
  - P3, S4: Risikoanalyse und Sicherheitsstrategie
  - P3, S5: Schutzstrategie und Risiko-Behandlungsplan
- **16 Aktivitäten**

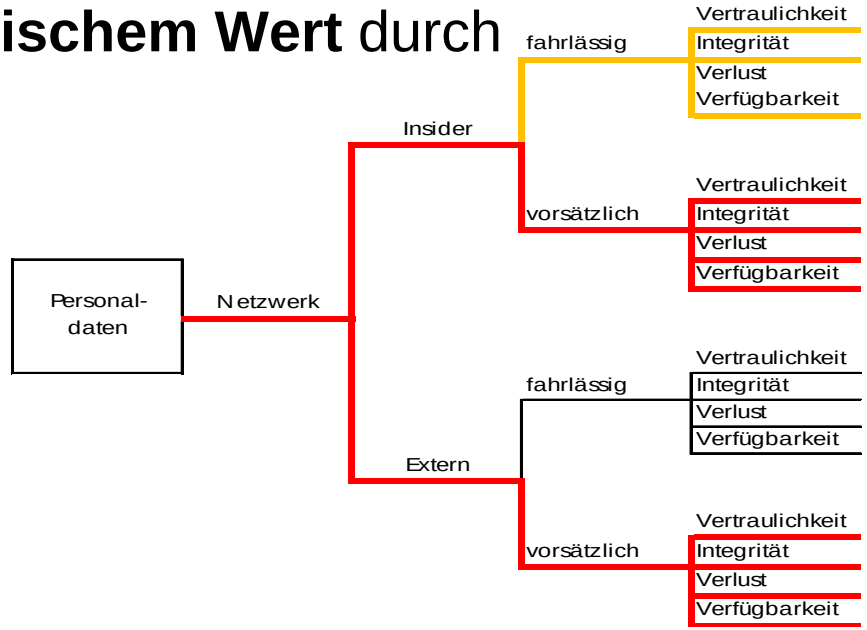
Phase 1: Organisatorische Sicht (1/2)

- **Prozess S1: Kritische Werte und Ist-Analyse**
  - ***Wie können Schadensauswirkungen bewertet werden?***
    - Aufstellen einer Metrik für die Schadenshöhe (“niedrig”, “mittel”, “hoch”) bezogen auf Schadenskategorien
  - ***Welche kritischen Werte sind vorhanden?***
    - Prozesse, Informationen, IT-Systeme, Anwendungen, Personen
  - ***Welches aktuelle Niveau haben die Sicherheitsmaßnahmen?***
    - Ermittlung des Ampelstatus für die Themenbereiche der ISO 27001
      - Rot: Nicht vorhanden, kritisch!
      - Gelb: Vorhanden mit Verbesserungspotential
      - Grün: Ausreichend vorhanden

Phase 1: Organisatorische Sicht (2/2)

- **Prozess S2: Definition von Bedrohungsprofilen**
  - **Auswahl und Analyse der zu betrachtenden kritischen Werte**
    - *Warum ist dieser Wert kritisch?*
    - *Wer verwendet diesen Wert? Wer trägt die Verantwortung für ihn?*
    - *Welche weiteren Werte haben einen Bezug zu diesem Wert?*
    - *Welche Sicherheitsanforderungen hat dieser Wert?*
  - **Analyse der Bedrohungen pro kritischem Wert** durch
    - Personen mit Netzzugang
    - Personen mit physischem Zugang
    - Technische Probleme
    - Weitere Problemfelder

→ **Bedrohungsprofil**



Phase 2: Technische Sicht
Prozess S3

- **Identifizierung von Schwachstellen in der IT-Infrastruktur**
  - **Ermittlung der Zugangswege zu den kritischen Werten**
    (aus Sicht der kritischen Werte)
    - *Wie greifen Mitarbeiter auf die kritischen Werte zu?*
      Welche IT-Systeme sind daran beteiligt?
      → Identifzierung relevanter Zugriffspfade
    - *Welche Komponenten der IT-Infrastruktur sind den kritischen Werten zuzuordnen? Wie sind diese vernetzt?*
  - **Analyse der technischen Prozesse**
    (aus Sicht der IT-Infrastruktur)
    - *Welche IT-Komponenten haben einen Bezug zu kritischen Werten?*
    - *Wer ist für diese Komponenten verantwortlich?*
    - *Wie stark wird Sicherheit bei Aufbau und Betrieb dieser IT-Komponenten berücksichtigt?*

Phase 3: Strategien und Pläne
Prozess S4

- **Identifizierung und Analyse der Risiken**
  - **Abschätzung der Schadenswirkung auf Basis der identifizierten Bedrohungen**
    Welcher potentielle Schaden kann für das Unternehmen entstehen, wenn ein Ereignis vorliegt?
  - **Festlegung von Kriterien für die Eintrittswahrscheinlichkeiten**
    Was bedeutet eine Eintrittswahrscheinlichkeit niedrig, mittel, hoch?
  - **Abschätzung der Eintrittswahrscheinlichkeit für jedes identifizierte Bedrohungsszenario**

  → **Vollständige Risikoanalyse für jede identifizierte Bedrohung, bezogen auf einen kritischen Wert**

Phase 3: Strategien und Pläne (1/2)
Prozess S5

- **Schutzstrategie und Plan zur Risikominimierung**
  - **Beschreibung der aktuell umgesetzten Sicherheitsmaßnahmen für die einzelnen Themenbereiche der ISO 27001**
    (Konkretisierung bzw. Verifikation der Ist-Analyse)
    - W*elche Maßnahmenpakete wurden in den einzelnen Themenbereichen bereits ausreichend umgesetzt? Wie ist der Ampelstatus?"*
  - **Übertragung des Ampelstatus auf die Risikoanalyse**
    - *Welche Risiken haben die höchste Dringlichkeit bei der Umsetzung?*
    - *Welche Themenbereiche sollten bei der Auswahl risiko-reduzierender Maßnahmen vorrangig berücksichtigt werden?*
  - **Identifikation notwendiger Sicherheitsmaßnahmen zur Risikominimierung und Umsetzungsplanung**
    Was kann getan werden, um die Risiken mit dem höchsten Schadenspotential zu minimieren?

Phase 3: Strategien und Pläne (2/2)
Prozess S5

- **Entwicklung einer Schutzstrategie und eines Plans zur Risikominimierung**
  - **Überprüfung, ob durch die Risikominimierung vorhandene Richtlinien / die Sicherheitspolitik modifiziert werden müssen**
    - *Sind die geplanten Sicherheitsmaßnahmen durch die aktuellen Richtlinien abgedeckt oder muss eine Veränderung erfolgen?*
  - **Darstellung der Ergebnisse**
    - *Was muss das Management 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 Werte betrachtet werden?”*

Vorteile von OCTAVE

- Anwendung einer strukturierten und skalierbaren Methode
- Maßgebliche Beteiligung aller Verantwortlichen, auch des Managements
- Berücksichtigung betriebswirtschaftlicher Aspekte
- Systematische Anleitung des Analyseteams durch Erläuterungen und Arbeitsblätter
- Klare Trennung zwischen dringenden und kontinuierlichen Maßnahmen
- Schärfung des Sicherheitsbewusstseins der Mitarbeiter
- Grundlage für ein ISMS und eine Zertifizierung nach ISO 27001 bzw. BSI-Grundschutz
- Investitionen für Informationssicherheit leichter argumentierbar

Toolunterstützung bei OCTAVE

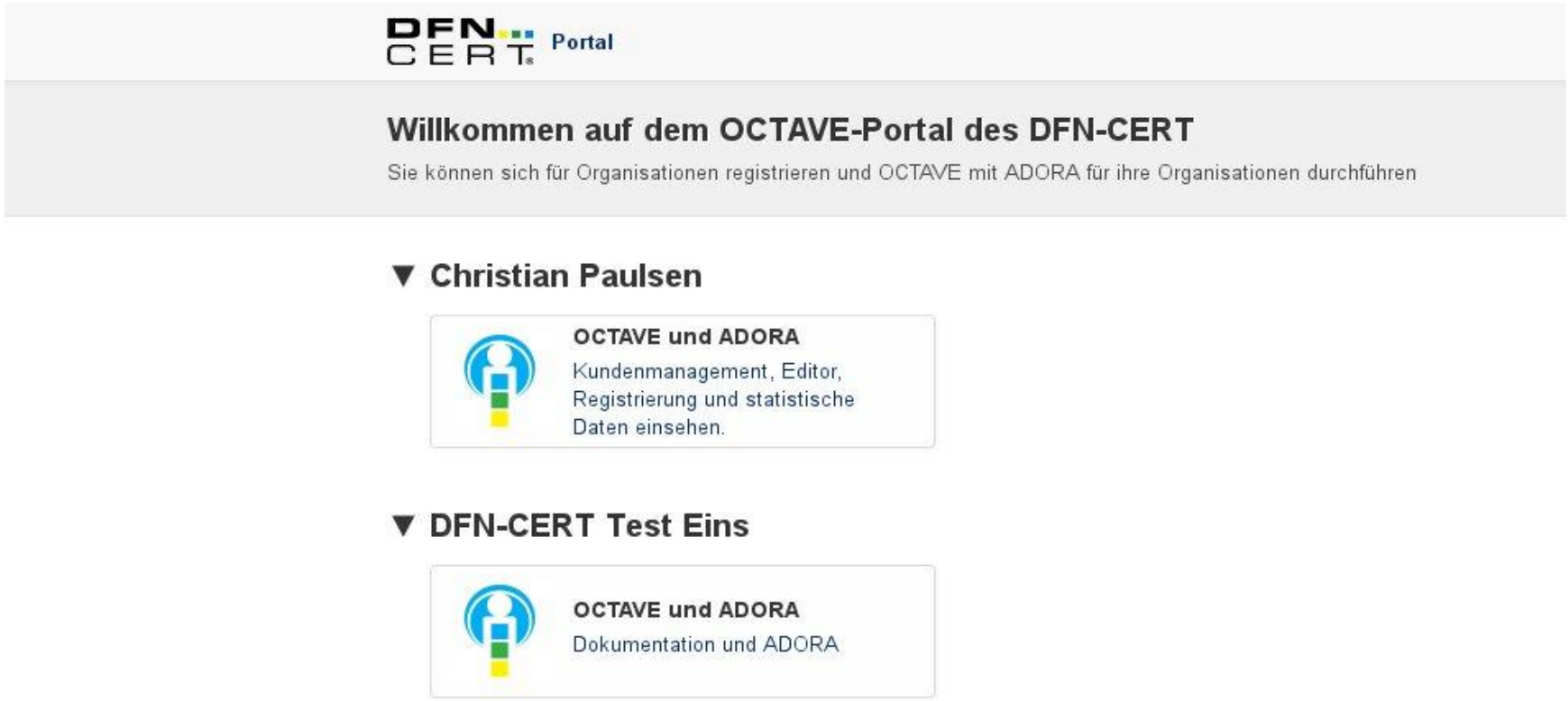
- OCTAVE-Anwender fragten vermehrt nach einem Tool
- Planung und Entwicklung im Rahmen einer Diplomarbeit in 2011
- Kontinuierliche Weiterentwicklung

- ADORA: Assistent zur Durchführung einer OCTAVE Risikoanalyse
- Ersetzt das Ausfüllen von Papierarbeitsblättern
- Unterstützung des Workflows – Schritt für Schritt
- Mehrere Assistenten:
  - Exportfunktionen (PDF, Diagramme)
  - Risikoberechnung

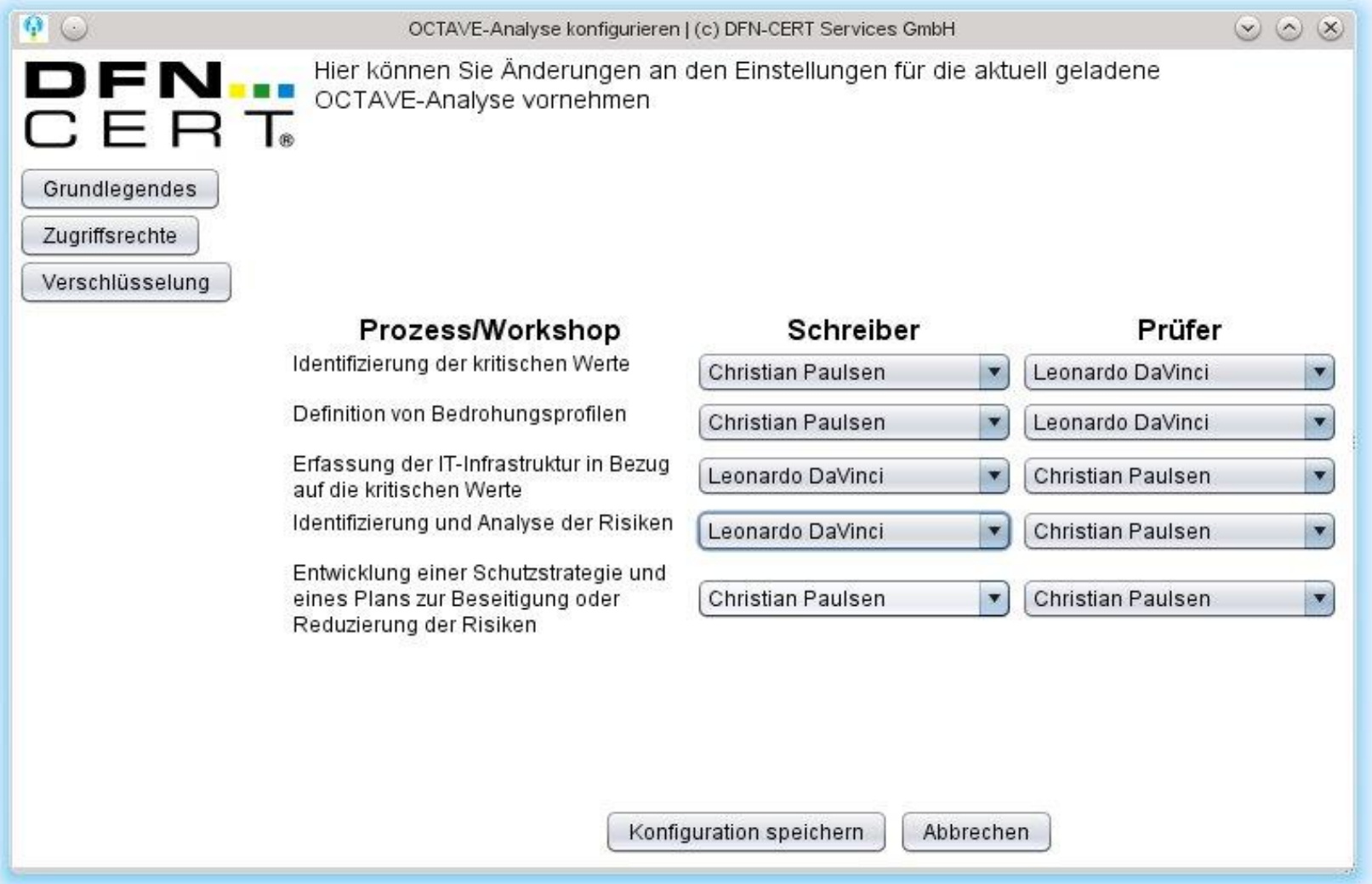
Eigenschaften von ADORA

- Client-Server Modell
- Zertifikatsbasierter Zugang über ein Webportal
- Abruf der aktuellen Arbeitsblätter bei jedem Start
- Datenhaltung als XML-Datei beim Client →
- Daten werden nicht beim DFN-CERT gespeichert
- Freiwillige Weitergabe von Ergebnissen zu statistischen Zwecken:
  - Wo stehe ich im Vergleich zu anderen Organisationen?
- Unterstützt 4-Augen-Prinzip

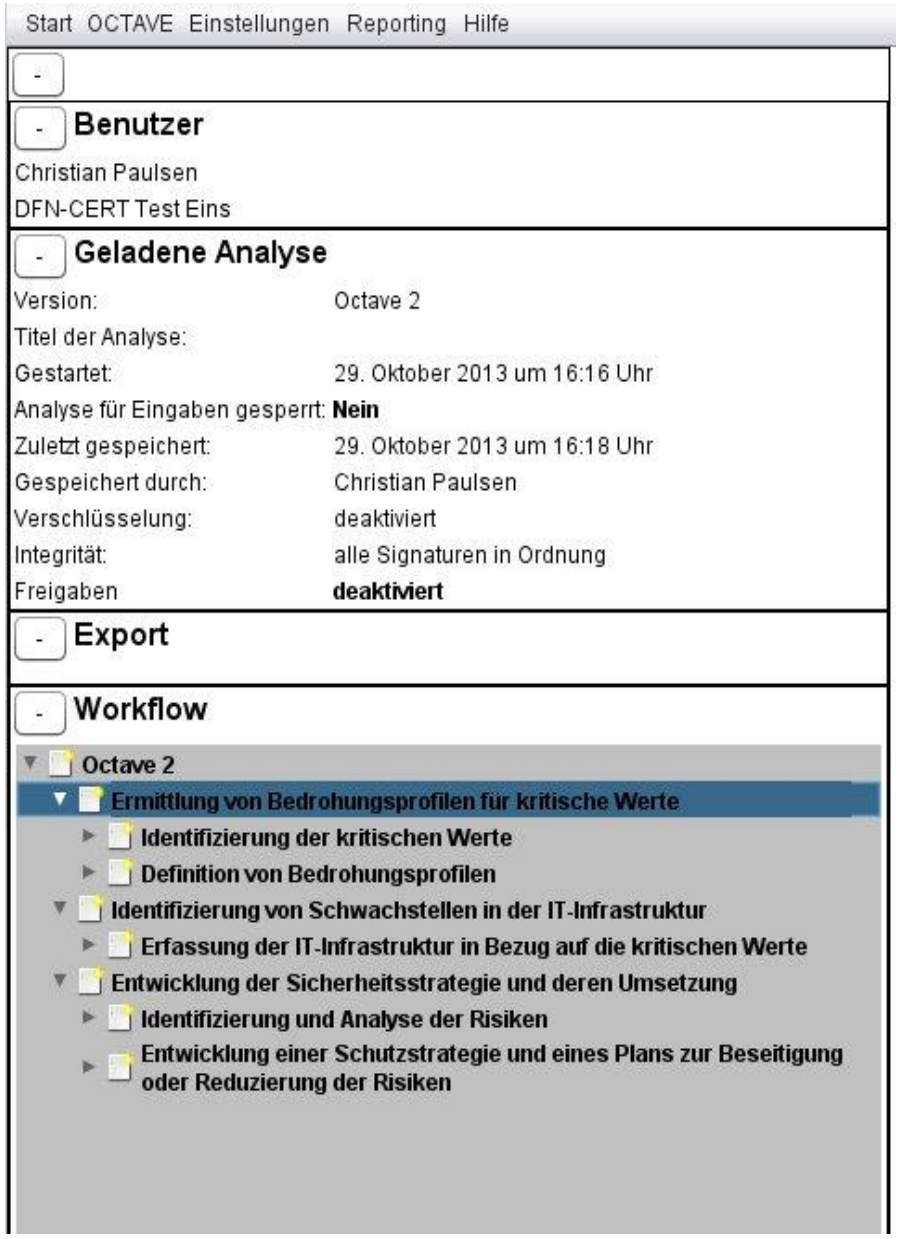
ADORA: Webportal



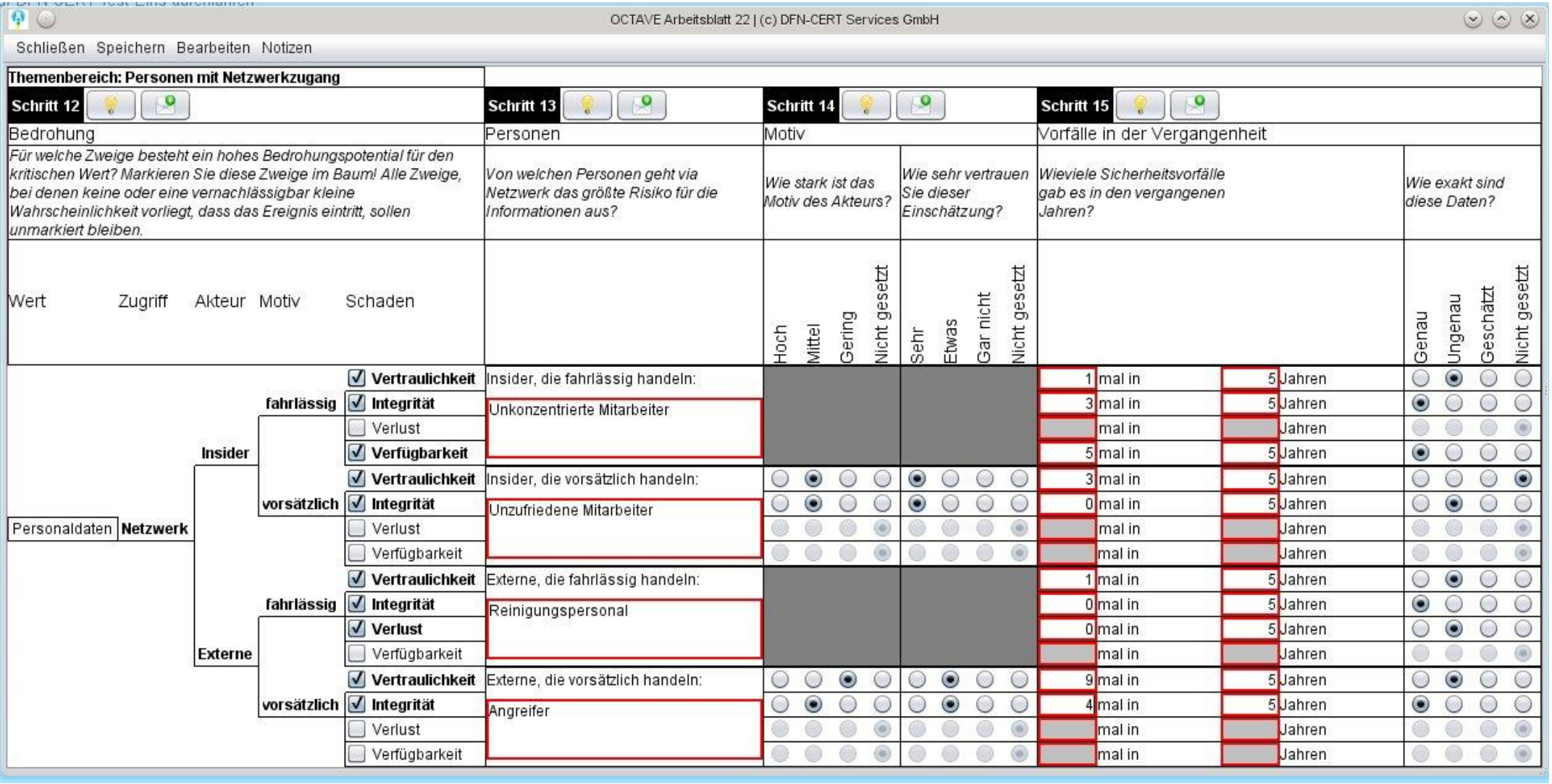
ADORA: Rechteverwaltung



ADORA: Übersichtsseite



ADORA: Risikoanalyse Übersichtsblatt 1



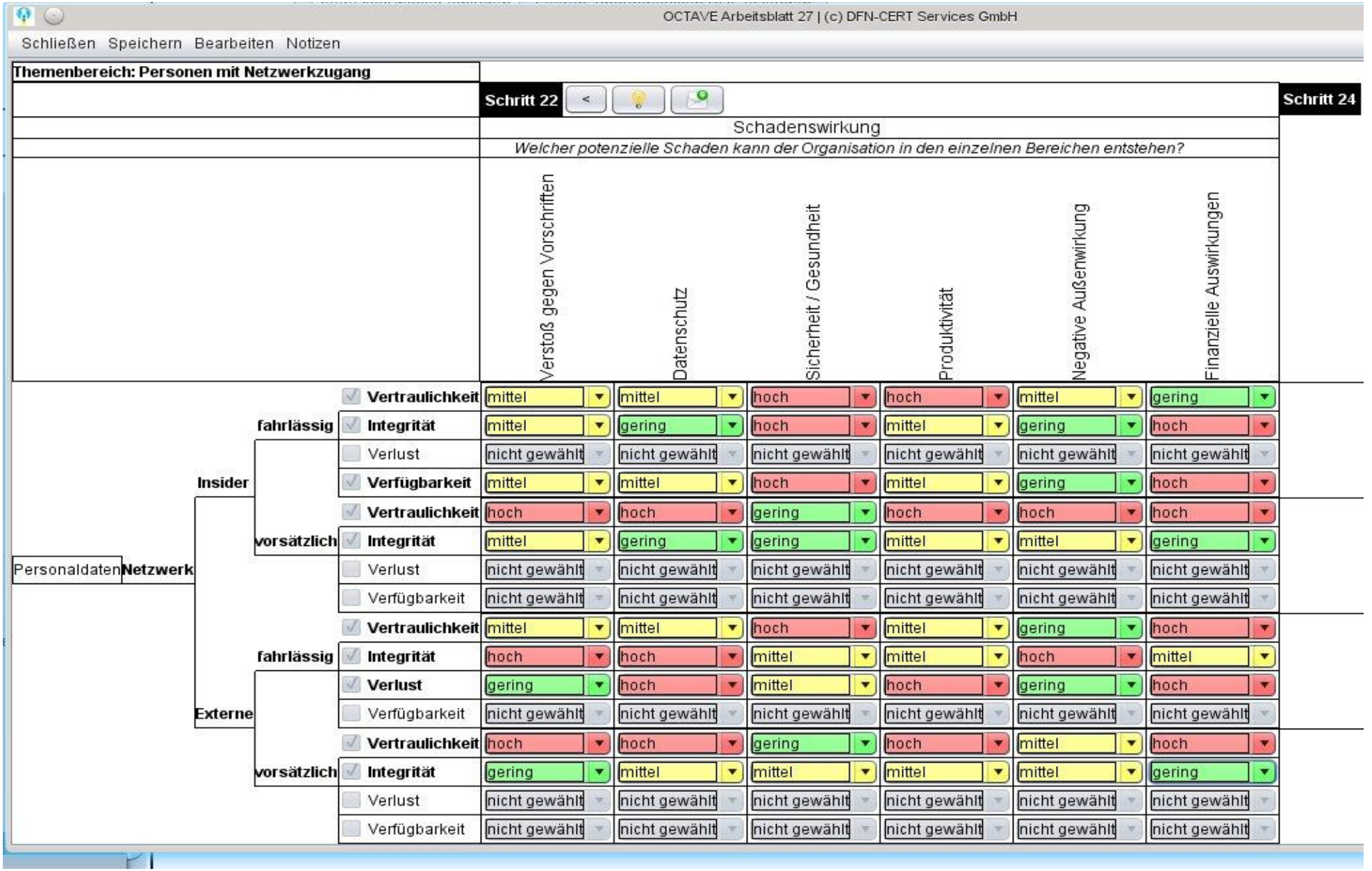
OCTAVE Arbeitsblatt 22 | (c) DFN-CERT Services GmbH

Schließen Speichern Bearbeiten Notizen

Themenbereich: Personen mit Netzwerkzugang

Schritt 12					**Schritt 13**	**Schritt 14**							**Schritt 15**								
Bedrohung					Personen	Motiv							Vorfälle in der Vergangenheit								
Für welche Zweige besteht ein hohes Bedrohungspotential für den kritischen Wert? Markieren Sie diese Zweige im Baum! Alle Zweige, bei denen keine oder eine vernachlässigbar kleine Wahrscheinlichkeit vorliegt, dass das Ereignis eintritt, sollen unmarkiert bleiben.					*Von welchen Personen geht via Netzwerk das größte Risiko für die Informationen aus?*	*Wie stark ist das Motiv des Akteurs?*				*Wie sehr vertrauen Sie dieser Einschätzung?*				*Wieviele Sicherheitsvorfälle gab es in den vergangenen Jahren?*						*Wie exakt sind diese Daten?*		
Wert	Zugriff	Akteur	Motiv	Schaden		Hoch	Mittel	Gering	Nicht gesetzt	Sehr	Etwas	Gar nicht	Nicht gesetzt						Genau	Ungenau	Geschätzt	Nicht gesetzt
Personaldaten	Netzwerk	Insider	fahrlässig	☑ **Vertraulichkeit**	Insider, die fahrlässig handeln:									1	mal in	5	Jahren		○	◉	○	○
				☑ **Integrität**	Unkonzentrierte Mitarbeiter									3	mal in	5	Jahren		◉	○	○	○
				☐ Verlust											mal in		Jahren		○	○	○	○
			vorsätzlich	☑ **Verfügbarkeit**										5	mal in	5	Jahren		◉	○	○	○
				☑ **Vertraulichkeit**	Insider, die vorsätzlich handeln:	○	◉	○	○	◉	○	○	○	3	mal in	5	Jahren		○	○	○	◉
				☑ **Integrität**	Unzufriedene Mitarbeiter	○	◉	○	○	◉	○	○	○	0	mal in	5	Jahren		○	◉	○	○
				☐ Verlust		○	○	○	○	○	○	○	○		mal in		Jahren		○	○	○	○
				☐ Verfügbarkeit		○	○	○	○	○	○	○	○		mal in		Jahren		○	○	○	○
		Externe	fahrlässig	☑ **Vertraulichkeit**	Externe, die fahrlässig handeln:									1	mal in	5	Jahren		○	◉	○	○
				☑ **Integrität**	Reinigungspersonal									0	mal in	5	Jahren		◉	○	○	○
				☑ **Verlust**										0	mal in	5	Jahren		○	◉	○	○
				☐ Verfügbarkeit											mal in		Jahren		○	○	○	○
			vorsätzlich	☑ **Vertraulichkeit**	Externe, die vorsätzlich handeln:	○	○	◉	○	○	◉	○	○	9	mal in	5	Jahren		○	◉	○	○
				☑ **Integrität**	Angreifer	○	◉	○	○	○	◉	○	○	4	mal in	5	Jahren		◉	○	○	○
				☐ Verlust		○	○	○	○	○	○	○	○		mal in		Jahren		○	○	○	○
				☐ Verfügbarkeit		○	○	○	○	○	○	○	○		mal in		Jahren		○	○	○	○

ADORA: Risikoanalyse Übersichtsblatt 2



OCTAVE Arbeitsblatt 27 | (c) DFN-CERT Services GmbH

Schließen Speichern Bearbeiten Notizen

Themenbereich: Personen mit Netzwerkzugang

Schritt 22 < **Schritt 24**

Schadenswirkung

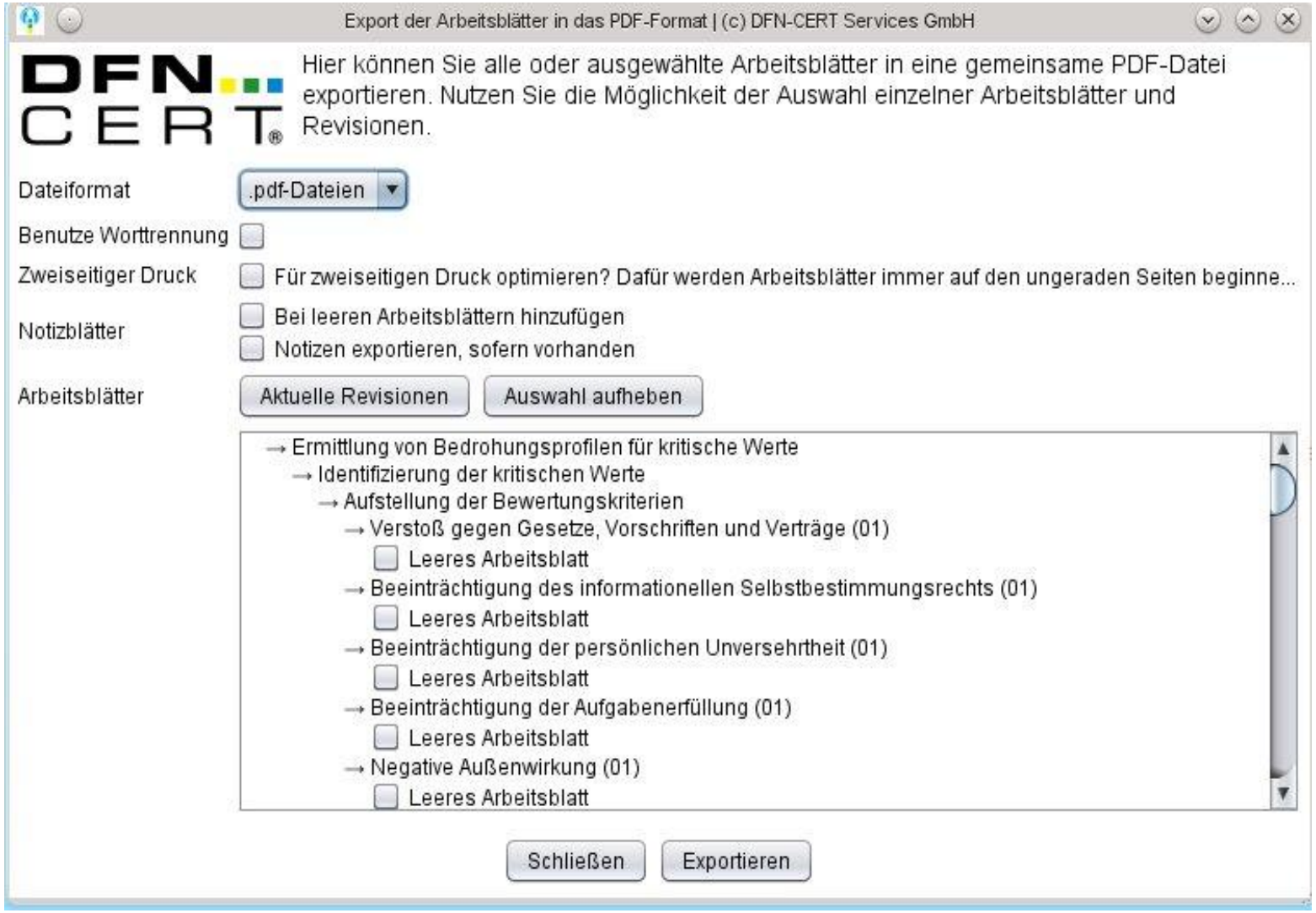
Welcher potenzielle Schaden kann der Organisation in den einzelnen Bereichen entstehen?

					Verstoß gegen Vorschriften	Datenschutz	Sicherheit / Gesundheit	Produktivität	Negative Außenwirkung	Finanzielle Auswirkungen
Personaldaten	Netzwerk	Insider	fahrlässig	Vertraulichkeit	mittel	mittel	hoch	hoch	mittel	gering
				Integrität	mittel	gering	hoch	mittel	gering	hoch
				Verlust	nicht gewählt	nicht gewählt	nicht gewählt	nicht gewählt	nicht gewählt	nicht gewählt
				Verfügbarkeit	mittel	mittel	hoch	mittel	gering	hoch
			vorsätzlich	**Vertraulichkeit**	hoch	hoch	gering	hoch	hoch	hoch
				Integrität	mittel	gering	gering	mittel	mittel	gering
				Verlust	nicht gewählt	nicht gewählt	nicht gewählt	nicht gewählt	nicht gewählt	nicht gewählt
				Verfügbarkeit	nicht gewählt	nicht gewählt	nicht gewählt	nicht gewählt	nicht gewählt	nicht gewählt
		Externe	fahrlässig	**Vertraulichkeit**	mittel	mittel	hoch	mittel	gering	hoch
				Integrität	hoch	hoch	mittel	mittel	hoch	mittel
				Verlust	gering	hoch	mittel	hoch	gering	hoch
				Verfügbarkeit	nicht gewählt	nicht gewählt	nicht gewählt	nicht gewählt	nicht gewählt	nicht gewählt
			vorsätzlich	**Vertraulichkeit**	hoch	hoch	gering	hoch	mittel	hoch
				Integrität	gering	mittel	mittel	mittel	mittel	gering
				Verlust	nicht gewählt	nicht gewählt	nicht gewählt	nicht gewählt	nicht gewählt	nicht gewählt
				Verfügbarkeit	nicht gewählt	nicht gewählt	nicht gewählt	nicht gewählt	nicht gewählt	nicht gewählt

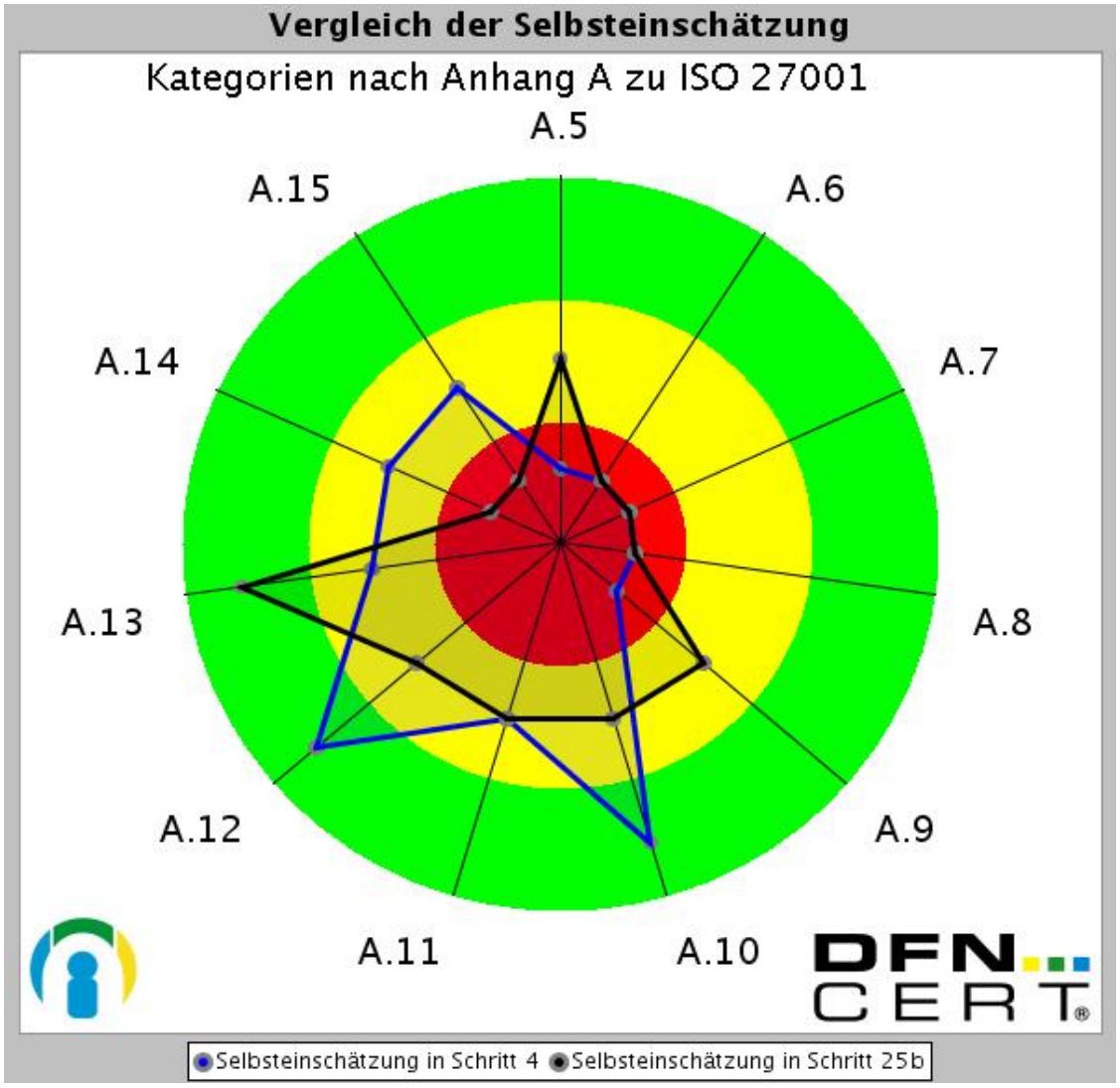
ADORA: Risikoanalyse Übersichtsblatt 3

	Schritt: 22						Schritt: 24						Schritt: 26											Schritt: 27				
	Schadenswirkung						Wahrscheinlichkeit						Sicherheitsmaßnahmen											Ansatz				
	Welcher potenzielle Schaden kann der Organisation in den einzelnen Bereichen entstehen?						*Wie wahrscheinlich ist das Eintreten der Bedrohung? Vertrauen Sie dieser Schätzung?*						*Wie hoch ist der Umsetzungsstatus (Ampelstatus) der Sicherheitsmaßnahmen in den einzelnen Themenbereichen? (Schritt 25b)*											*Was ist ihr Ansatz für die einzelnen Risiken?*				
	Verstoß gegen Vorschriften	Datenschutz	Sicherheit / Gesundheit	Produktivität	Negative Außenwirkung	Finanzielle Auswirkungen	Wahrscheinlichkeit	Vertrauen: Hoch	Vertrauen: Mittel	Vertrauen: Gering	Vertrauen: Nicht gesetzt		Sicherheitsmanagement	Organisation	Klassifizierung von Werten	Personal	Phys. Maßnahmen	Kommunikation / Betr.	Zugangskontrolle	Entwicklung und Wartung	Sicherheitsvorfälle	Notfallplanung	Verpflichtungen	Risikobewertung	akzeptieren	verschieben	mindern	Nicht gesetzt
Vertraulichkeit																												
✓ Integrität								○	○	○	○	⊗												54	○	○	○	⊗
✓ Verlust								○	⊗	○	○	○												60	○	⊗	○	○
Verfügbarkeit																												
Vertraulichkeit																												
✓ Integrität								○	○	⊗	○	○												90	○	⊗	○	○
Verlust																												
✓ Verfügbarkeit								○	○	⊗	○	○												16	⊗	○	○	○

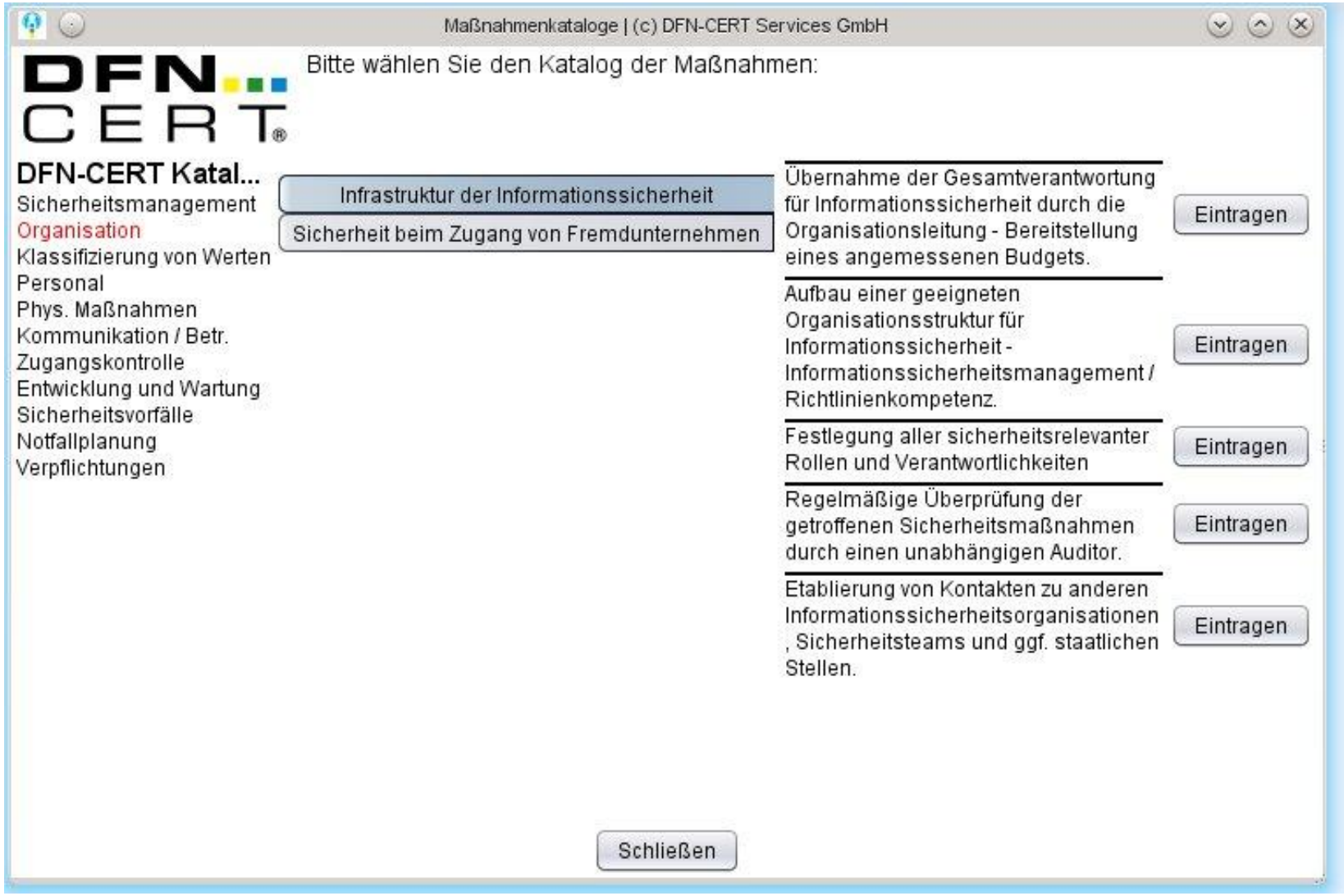
ADORA: PDF-Export



ADORA: Spiderwebdiagramme



ADORA: Maßnahmenauswahl



ADORA: Hilfe und Support / Kontakt

- Hilfetexte für jeden Schritt
- Softwarehandbuch als PDF
- OCTAVE-Leitfaden als PDF
- Buttons für inhaltlichen und für technischen Support vorhanden

Weitere Informationen unter:

- http://www.dfn-cert.de/leistungen/octave.html
- octave@dfn-cert.de

Christian Aust
christian.aust@consecco.de

Dr. Christian Paulsen
paulsen@dfn-cert.de