intersoft consulting

Datenschutz, IT-Sicherheit und IT-Forensik: Wir halten Sie auf Kurs.

# Reaktion im Ernstfall - strukturierte Incident Response

Schnelle Erkennung, Eindämmung und Wiederherstellung zur Minimierung von Schäden

**Joanna Lang-Recht**
Director IT Forensics

# Agenda

1. Was ist Incident Response?
2. Rolle der IT-Forensik
3. Incident Response Prozess
4. Tools und Techniken
5. Best Practices
6. Herausforderungen & Risiken
7. Fazit

# Was ist Incident Response?




- Strukturierter Prozess zur Erkennung, Analyse und Behebung von IT-Sicherheitsvorfällen
- **Ziel**: (schnellstmögliche) Minimierung des Schadens, Sicherung der Beweise und Wiederherstellung des Normalbetriebs

Weiterführende Informationen zum Team, den Laboren und den Leistungen unter

www.it-forensik.de

# Agenda

1 Was ist Incident Response?

➔ 2 Rolle der IT-Forensik

3 Incident Response Prozess

4 Tools und Techniken

5 Best Practices

6 Herausforderungen & Risiken

7 Fazit

# Rolle der IT-Forensik

## Kernkompetenz IT-Forensik

- IT-forensische Analysen
  - Endgeräte
  - Server
  - E-Mails
  - Logfiles
  - Malware

## Ergänzend

- Optimierung von IT-Infrastrukturen im Sinne der “Forensic Readiness”
- Finden und Schließen von Sicherheitslücken

# Rolle der IT-Forensik



## Sachkundige und gerichtsverwertbare Analyse

- Gerichtsfeste Identifizierung, Sicherung und Analyse von Beweisen
- Aufklärung eines Vorfalls und bestenfalls Überführen des Täters bzw. der Tätergruppe
- Erstellung eines ggf. gerichtsfesten Gutachtens
- Erkennen, Eindämmen und Rekonstruktion eines Angriffs
- Identifizieren der ausgenutzten Schwachstellen
- Lessons Learned: Maßnahmenempfehlungen, Beratung zur IT-Sicherheit, um neue Vorfälle zu verhindern

# Agenda

1 Was ist Incident Response?

2 Rolle der IT-Forensik

➔ 3 Incident Response Prozess

4 Tools und Techniken

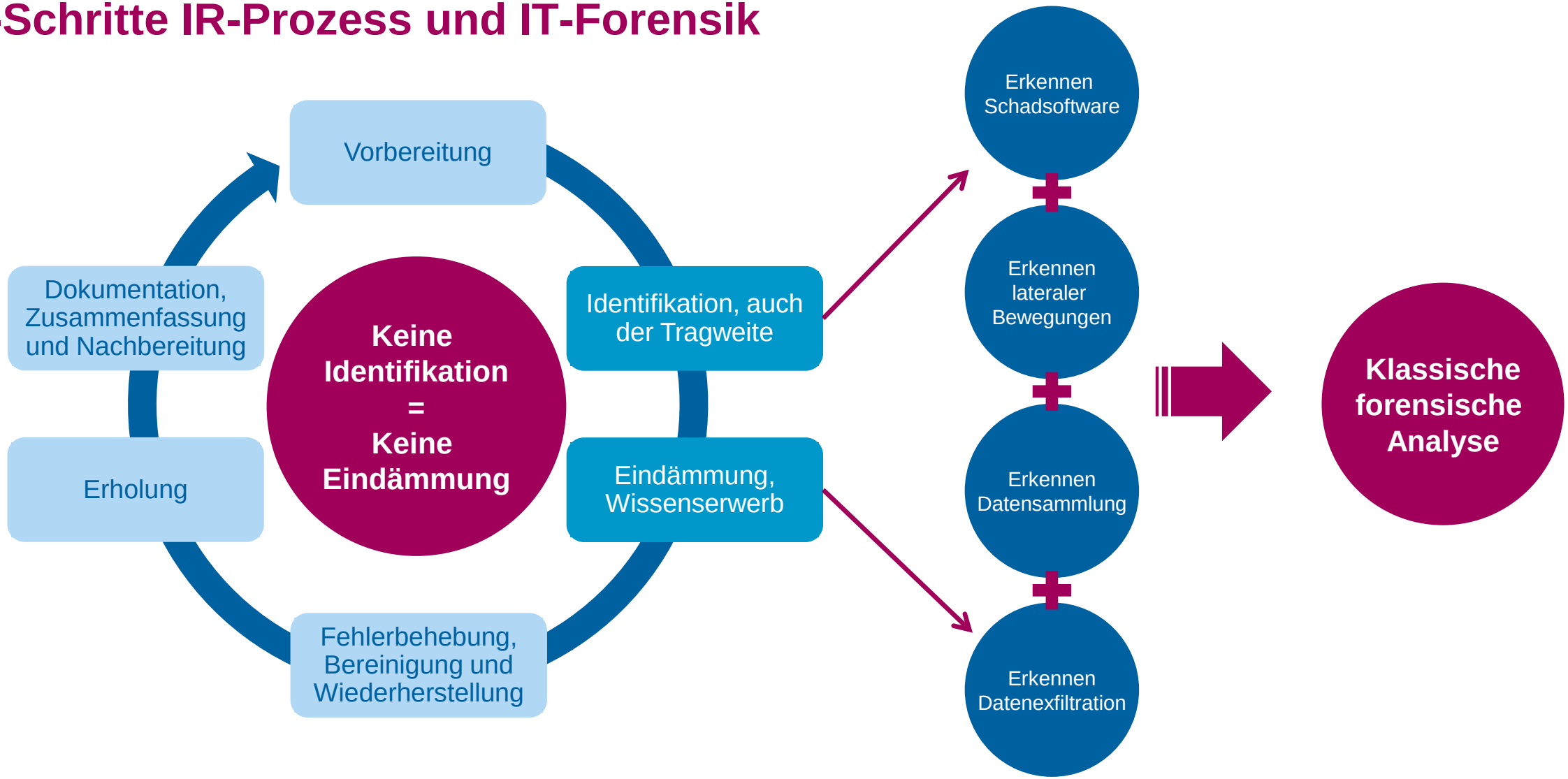
5 Best Practices

6 Herausforderungen & Risiken

7 Fazit

# Incident Response Prozess

## 6-Schritte IR-Prozess und IT-Forensik



# Agenda

1 Was ist Incident Response?

2 Rolle der IT-Forensik

3 Incident Response Prozess

➔ 4 Tools und Techniken

5 Best Practices

6 Herausforderungen & Risiken

7 Fazit

# IT-Forensik Tools und Techniken (Auswahl)

## Tools

- FTK / Imager
- Wireshark
- Velociraptor

## Techniken

- Imageerstellung
- Analyse des Netzwerkverkehrs
- Parallele, automatisierte Spurensuche auf Vielzahl von Geräten

Integrität der Beweise durch dokumentierte Chain of Custody

# Agenda

1 Was ist Incident Response?

2 Rolle der IT-Forensik

3 Incident Response Prozess

4 Tools und Techniken

➔ 5 Best Practices

6 Herausforderungen & Risiken

7 Fazit

# Best Practices



- Incident Response Pläne zur gesteigerten Reaktionsfähigkeit
- Eindeutige Rollenverteilung für Sicherheitsvorfall
- Lückenlose Dokumentation bei Vorfällen
- Regelmäßige Notfallübungen und Schwachstellenanalysen / Pentests

# Agenda

1 Was ist Incident Response?

2 Rolle der IT-Forensik

3 Incident Response Prozess

4 Tools und Techniken

5 Best Practices

➔ 6 Herausforderungen & Risiken

7 Fazit

# Herausforderungen & Risiken

- Zeitdruck beim aktiven Vorfall
- Mangelnde Ressourcen / Spuren

- Datenschutz und Meldepflicht
- Krisenkommunikation
  - Verhandlung zur Tätergruppe
  - Ermittlungsbehörden
  - Presse

# Agenda

1 Was ist Incident Response?

2 Rolle der IT-Forensik

3 Incident Response Prozess

4 Tools und Techniken

5 Best Practices

6 Herausforderungen & Risiken

➔ 7 Fazit

# Fazit

- Ein gut strukturierter und vorbereiteter IncidentResponse Prozess minimiert den möglichen Schaden
- IT-Forensik ist entscheidend für Aufklärung und nachfolgende Prävention (Lessons Learned)
- Regelmäßige Schulungen, Vorbereitungen und auch Nachbereitungen sind unverzichtbar

# D.E.V.I.L

# Digital Evidence Validation & Investigation Lab

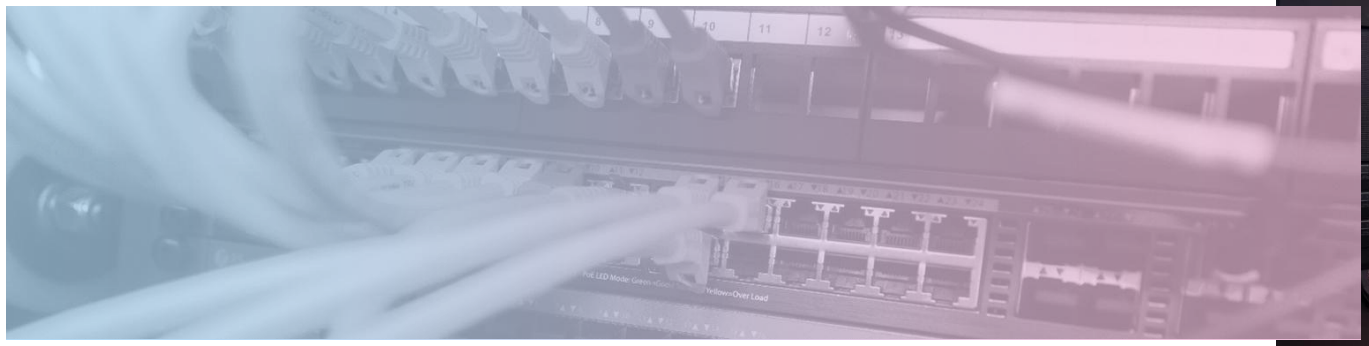
# DEVIL – Facts

- Mobiles IT-Forensik Labor
- 6 Tonnen
- Luftfederung
- Hydraulik Stützen
- Überwachungskamera

# DEVIL – Facts

## Forensik-Labor

- Storage Server System
- 3 Analyse-Rechner für 3 Arbeitsplätze
- Gesamtspeicher: ca. 1,2 Petabyte –
  davon über 300 Terabyte mobil verfügbar



## Mehrere Internetanschlüsse

- Autarke Netze
  (Glasfaser, Satellit, Ethernet RJ45)

# Fragen & Antworten

# Vielen Dank für Ihre Aufmerksamkeit.

Gern stehe ich Ihnen für Fragen zur Verfügung.

**Joanna Lang-Recht**
Director IT Forensics