# Wenn nichts mehr geht: Forensik nach Ransomware-Angriffen

Nürnberg Digital Festival

HiSolutions AG

Lisa Lobmeyer

# Lisa Lobmeyer
# Team Managerin

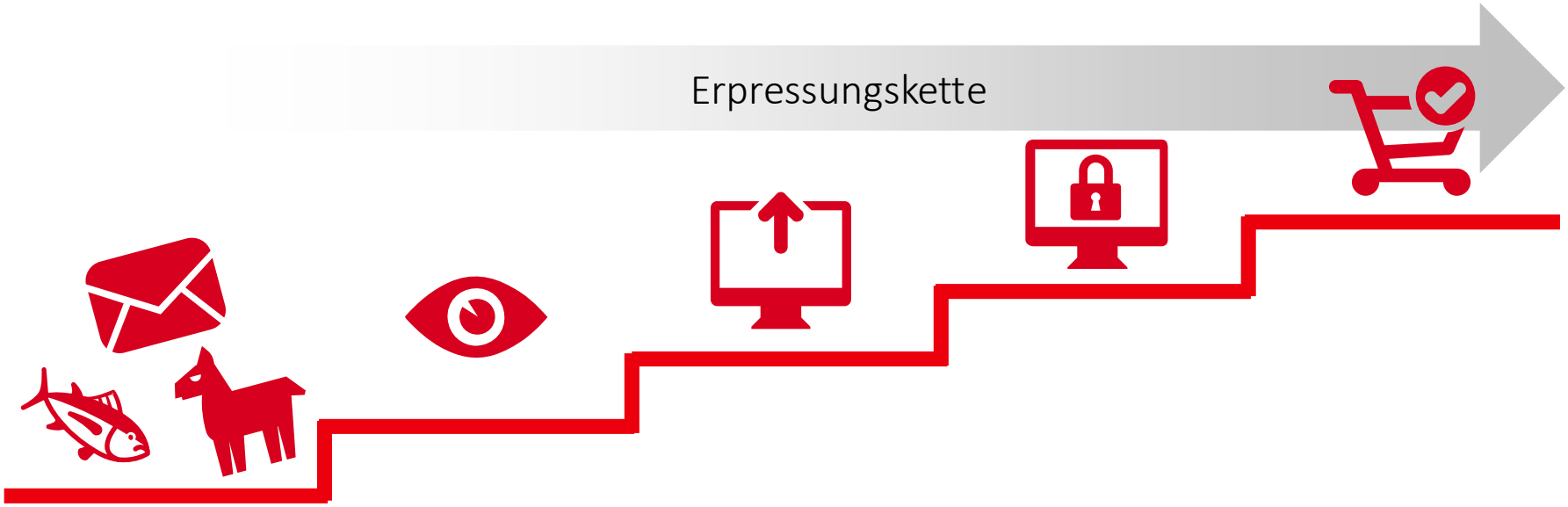
- Expertin für Incident Response
- Koordinierung des Incident Response-Geschäfts
- Einsatzleitung von IT-Sicherheitsvorfällen
  - Forensische Beweissicherung und Analyse
  - Krisenmanagement
  - Incident Koordinierung
- Themenverantwortliche IT-Forensik
- Schulung und Sensibilisierungen von Fachkräften und Leitung

# Agenda

1. Was ist Ransomware?
2. Ziele der (IT-)Forensik
3. Durchführung und Vorbereitung einer IT-forensischen Analyse

# Was ist Ransomware?

# Das Geschäftsmodell: Ransomware as a Service

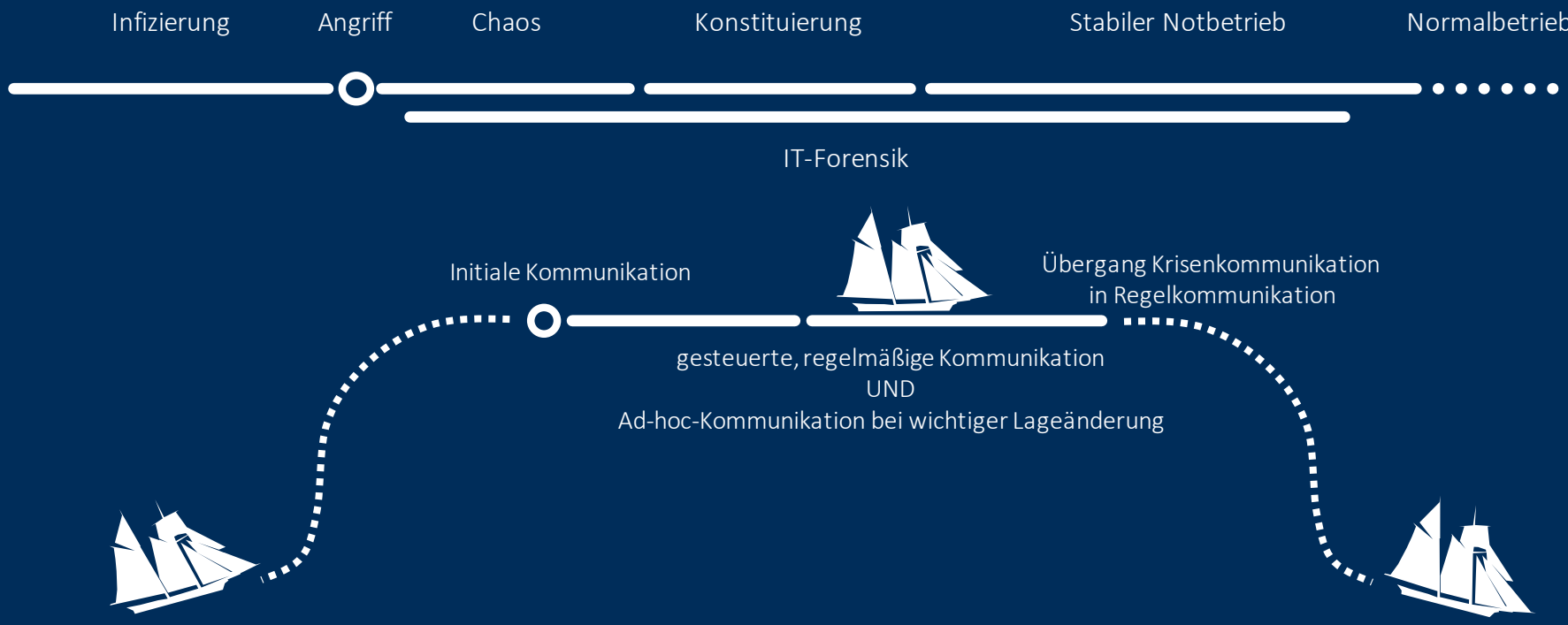



| Initialer Zugriff | Auskundschaften des Ziels | Datenabzug | Verschlüsselung | Daten-veröffentlichung/ -verkauf |
|---|---|---|---|---|

# Phasen der Vorfallbewältigung

# Ziele der Forensik

# Phasen der Vorfallbewältigung



> Überall dort, wo er geht, was er berührt,
> was er hinterlässt, auch unbewusst,
> all das dient als stummer Zeuge gegen ihn.

Edmond Locard

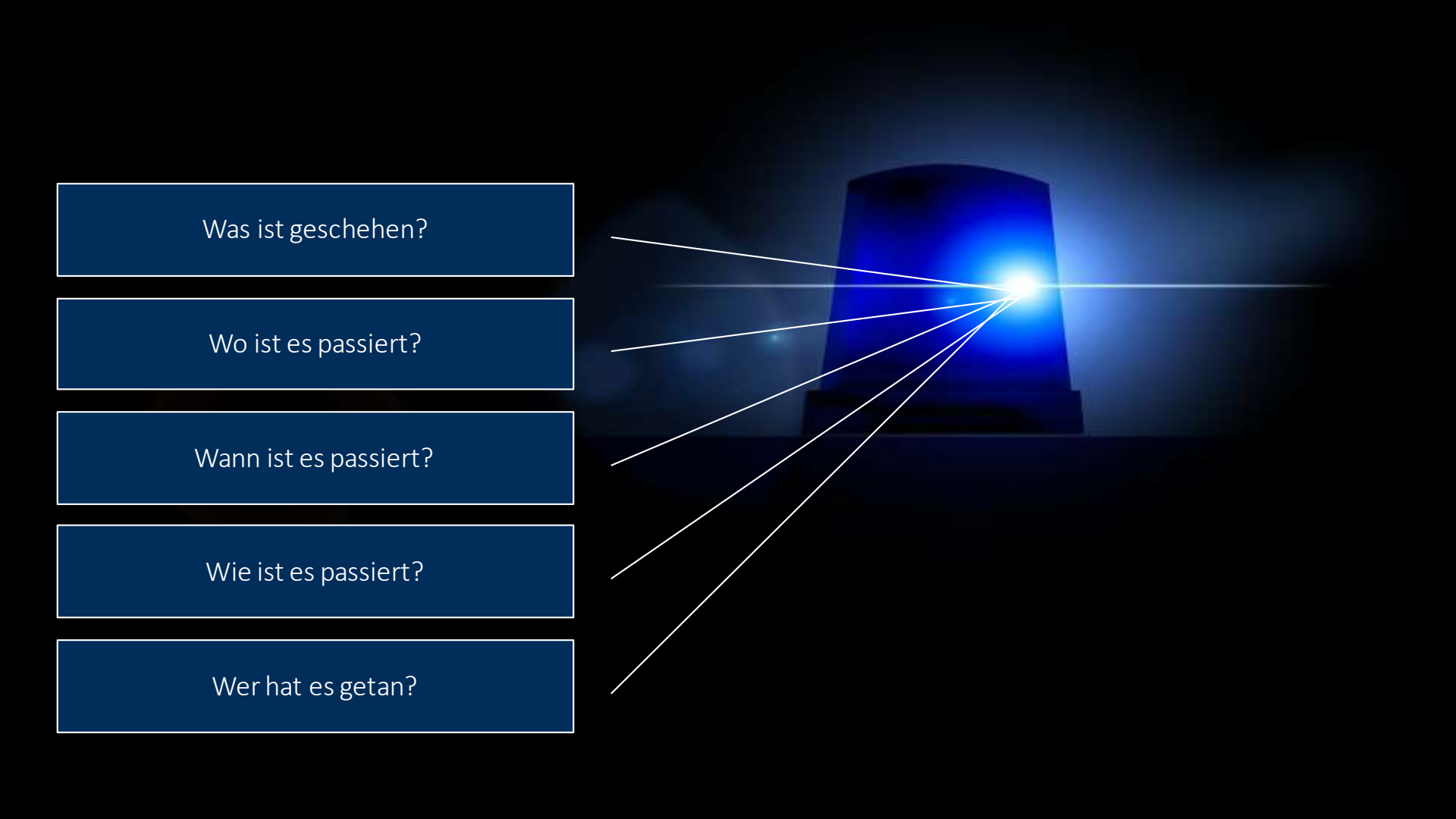
Was ist geschehen?

Wo ist es passiert?

Wann ist es passiert?

Wie ist es passiert?

Wer hat es getan?



# Erkenntnisse in der IT-Forensik

| | | |
|---|---|---|
| Was ist geschehen? | ——— | Kill Chain/Kompromittierung |
| Wo ist es passiert? | ——— | Betroffene Systeme |
| Wann ist es passiert? | ——— | Angriffszeitpunkt |
| Wie ist es passiert? | ——— | Einfallsvektor |
| Wer hat es getan? | ——— | Attributierung |

# Anforderungen an eine forensische Analyse

Akzeptanz

Integrität

Glaubwürdigkeit

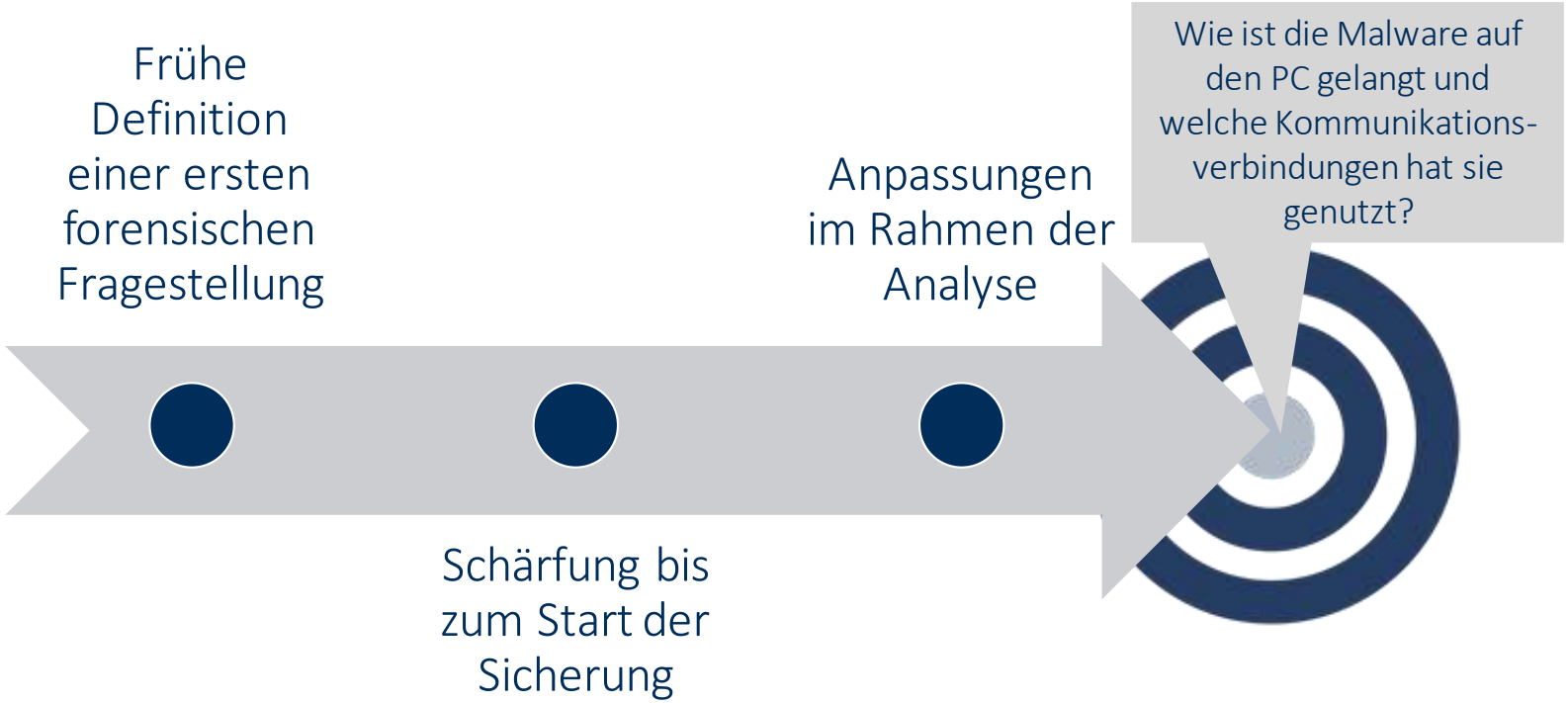
Ursache und Auswirkungen

Wiederholbarkeit

Dokumentation

# Durchführung und Vorbereitung einer IT-forensischen Analyse

# Definition einer forensischen Fragestellung



# Ablauf einer forensischen Analyse

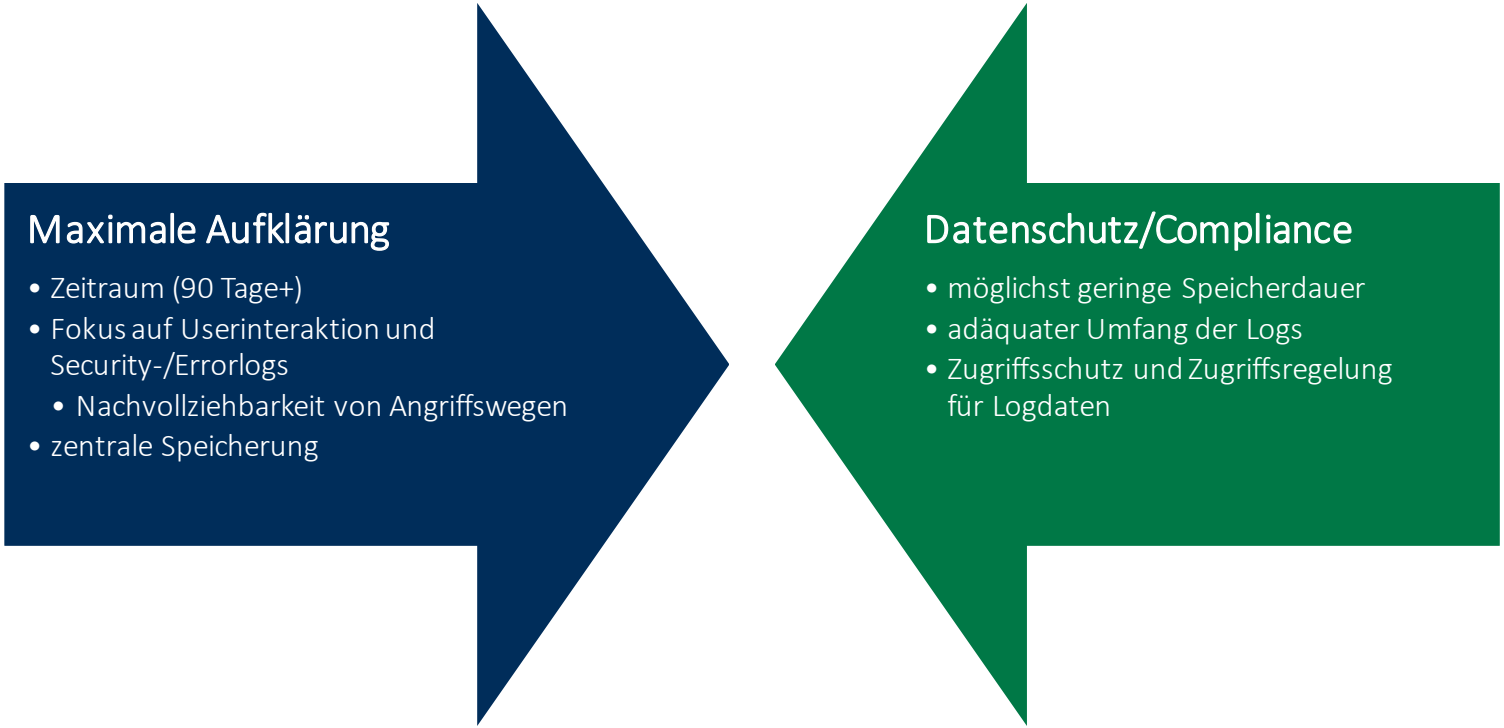
# Vorbereitung für den Fall der Fälle?

# Wie es nicht sein sollte: IT-Forensik-Edition


Quelle


Quelle

# Logging: ein konstantes Spannungsfeld



# Was sollte geloggt werden?

- „~~Es kommt drauf an.~~“

- Baseline-Logging:
  - OWASP-Logging-Cheat-Sheet
  - Microsoft Audit Policy Recommendations
  - Logging Recommendations for Internet-Facing Servers (RFC6302)
  - Draft: DSGVO-Konformität RFC6302
  - BSI: Configuration Recommendations for Windows 10 Logging

> You can have data without information,
> but you cannot have information without data.

Daniel Keys Moran

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com