Maritime Cyber Risk Management

Seeschifffahrtssicherheitskonferenz 2017

Christian Hemminghaus
Fraunhofer FKIE
Cyber Analysis & Defense

08. November 2017

© iStock/zmeel

© iStock

Fraunhofer FKIE

Fraunhofer FKIE

Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie

Fraunhofer FKIE erforscht und entwickelt Modelle, Methoden und Werkzeuge für Kontroll- und Steueraufgaben in vernetzten Systemen (»Vernetzte Operationsführung«).

Forschungsgebiete

- Sensordatenfusion
- Kommunikationssysteme
- Human Factors
- Mensch-Maschine-Systeme
- Systemergonomie
- Informationstechnik für Führungssysteme
- Kognitive Mobile Systeme
- Cyber Analysis & Defense
- Cyber Security
- Usable Security and Privacy
- Privacy and Security in Ubiquitous Computing

Standorte	Wachtberg und Bonn
Gegründet	1963
Fraunhofer	seit August 2009
Mitarbeiter	> 400
Budget	> 30 Mio €
Institutsleiter	Prof. Dr. Peter Martini
Website	www.fkie.fraunhofer.de

© Uwe Bellhäuser

Cyber Analysis & Defense

Forschungsabteilung

»Wir erforschen Möglichkeiten,
um existenzbedrohende Risiken im Cyber- und Informationsraum frühzeitig zu erkennen, zu minimieren und beherrschbar zu machen.«

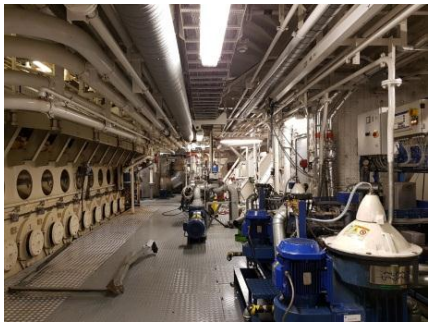
- Schutz kritischer Systeme und Infrastrukturen vor Cyber-Angriffen durch
  - Analyse verwundbarer Systeme
  - Absicherung eigener Systeme und Infrastrukturen
  - Analyse von Cyber-Angriffen, Täterwerkzeugen und Akteuren

- Schutz vor
  - Cyber-Kriminalität
  - Cyber-Spionage
  - Cyber-Sabotage

➢ Wahrnehmung einer gesellschaftlichen Verantwortung durch Beitrag zur Sicherheit im Cyber- und Informationsraum

Das Risiko des digitalen Fortschritts

Systeme und Gefährdungen

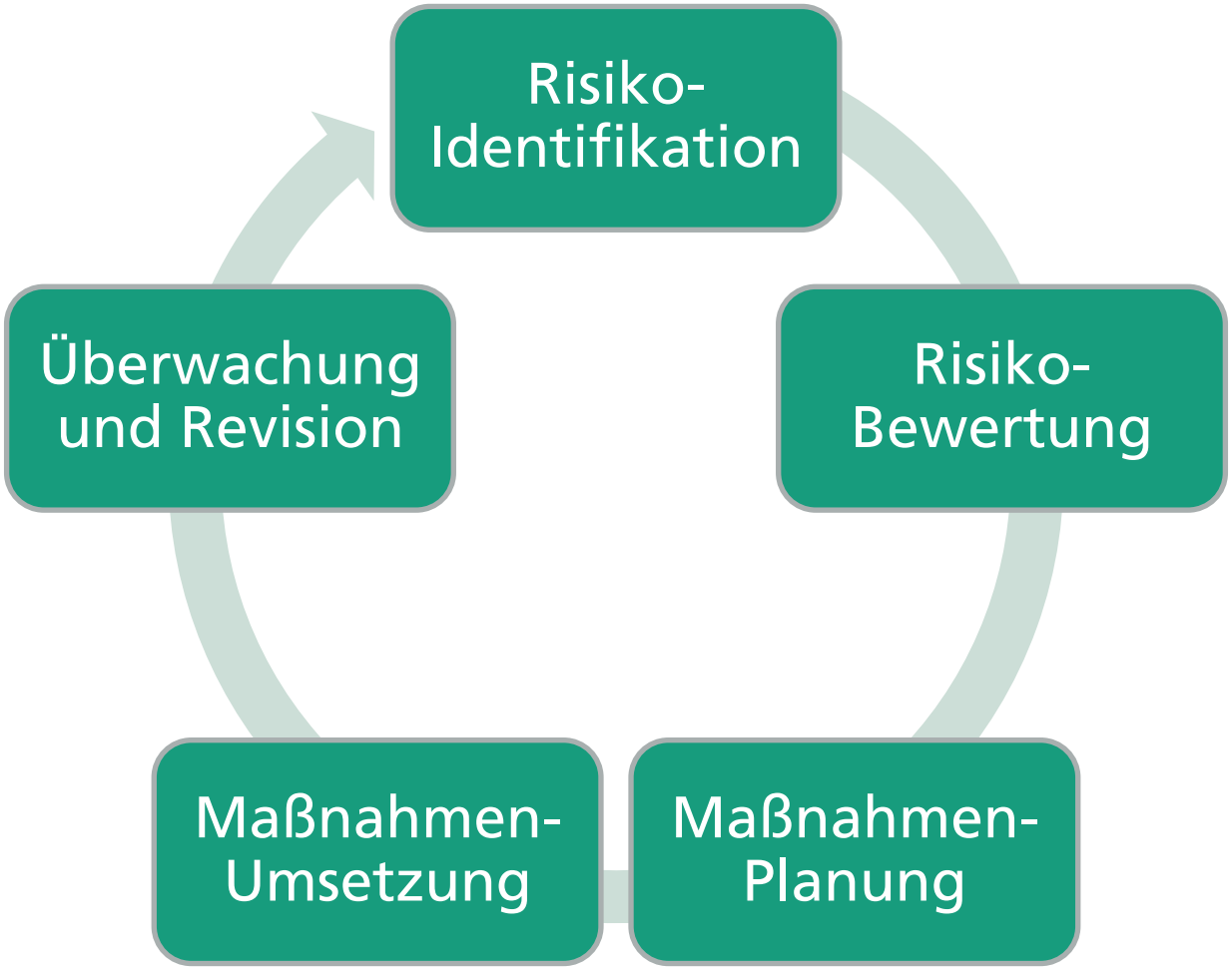



- Akute Gefährdungen
  - Komplizierte Fehlerdiagnose durch verzahnte Systeme
  - Schadsoftware (Logger, Ransomware, Backdoors, …)
  - Spionage digitaler Daten
  - Gezielter Eingriff in Schiffssysteme

- Mögliche Auswirkungen
  - Wirtschaftliche Konsequenzen
  - Rechtliche Konsequenzen
  - Schlechte Reputation und Imageverlust
  - Menschenleben sind in Gefahr

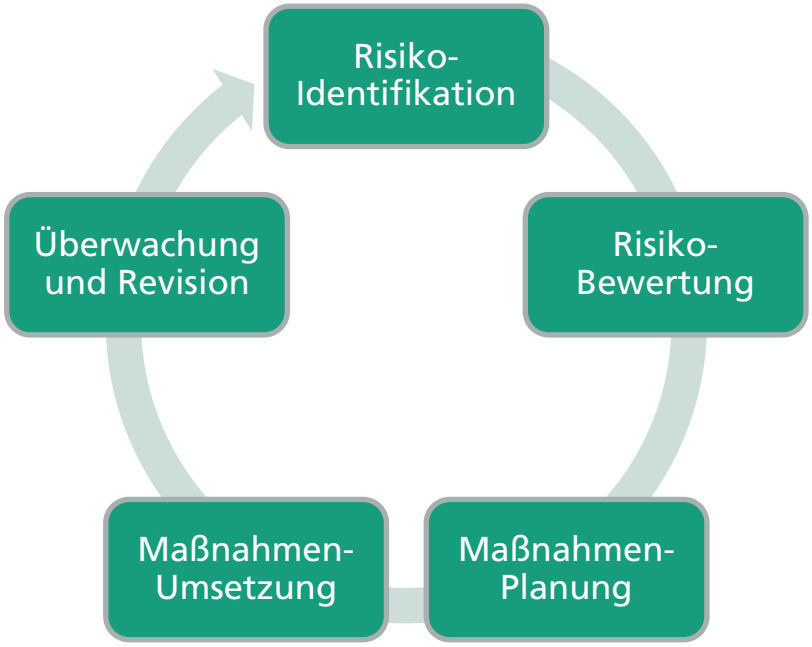
Risk Management

Der zentrale Prozess



Cyber Risk Management

Umsetzung für digitale Technologien

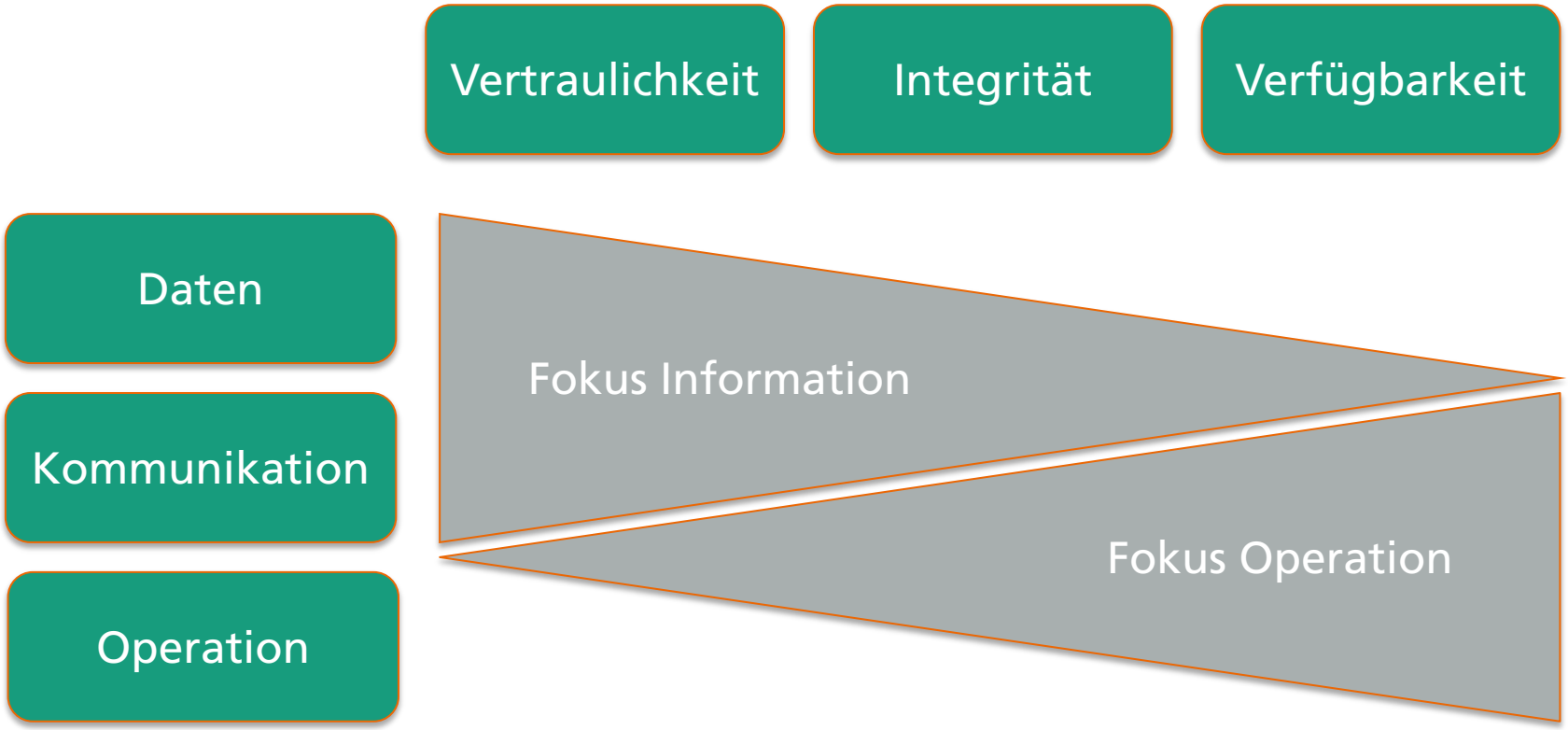


Identifikation

- Digitale Assets identifizieren
- Schutzbedarfsfeststellung (Schutzziele)
- Risiken sind Gefährdungen der Schutzziele

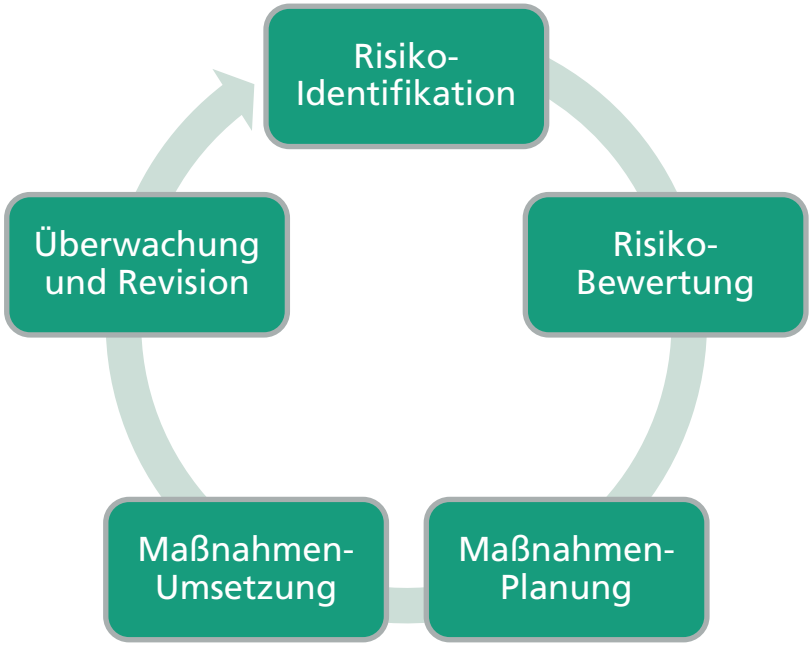
Schutzobjekte und Schutzziele

Information vs. Operation



Cyber Risk Management

Umsetzung für digitale Technologien



Identifikation

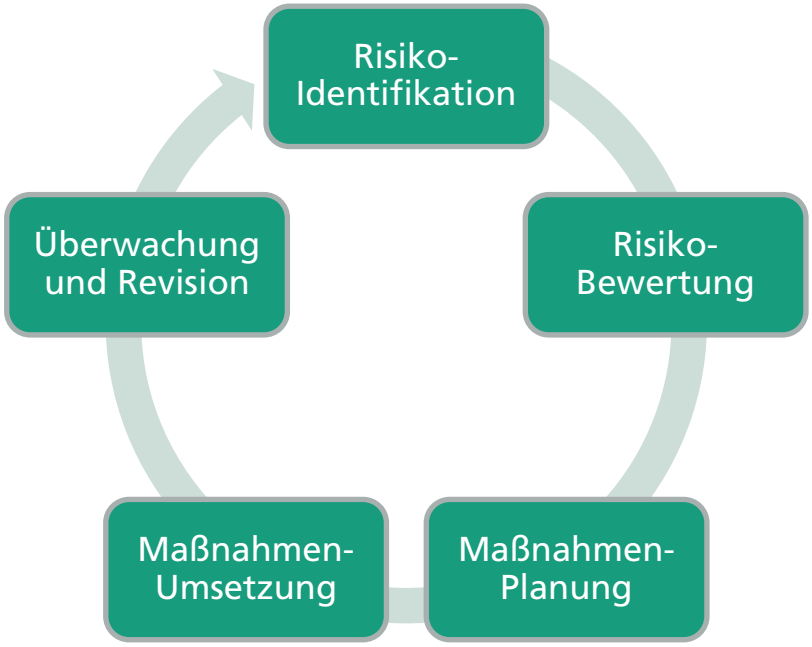
- Digitale Assets identifizieren
- Schutzbedarfsfeststellung (Schutzziele)
- Risiken sind Gefährdungen der Schutzziele

Bewertung

- Risiko = Wahrscheinlichkeit x Auswirkungen
- Angreifermodell
- Meist nur qualitativ möglich

Cyber Risk Management

Umsetzung für digitale Technologien



Identifikation

- Digitale Assets identifizieren
- Schutzbedarfsfeststellung (Schutzziele)
- Risiken sind Gefährdungen der Schutzziele

Bewertung

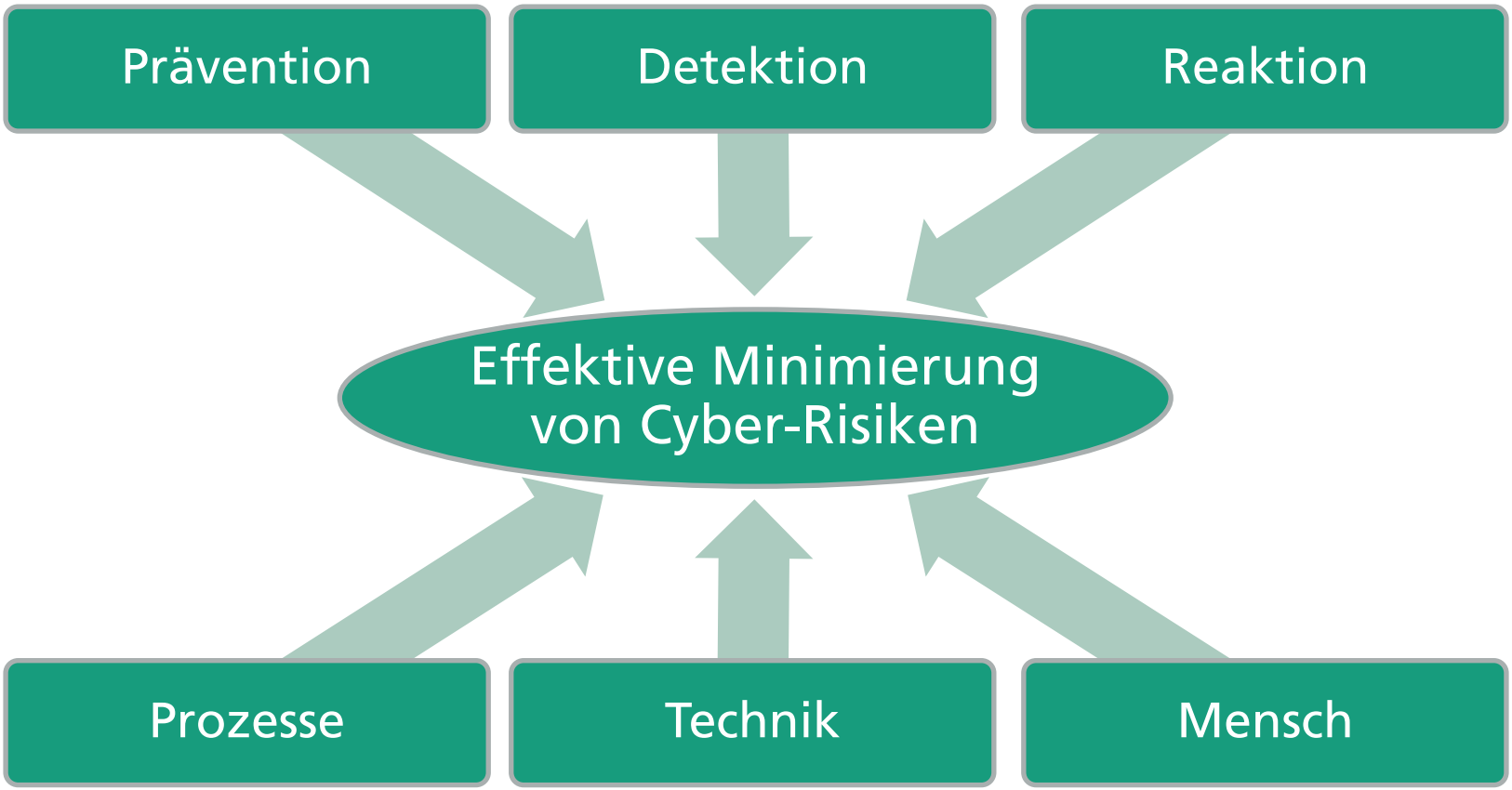
- Risiko = Wahrscheinlichkeit x Auswirkungen
- Angreifermodell
- Meist nur qualitativ möglich

Maßnahmen

- möglichst flächendeckend
- Security in Depth
- Prävention, Detektion, Reaktion
- Prozesse, Technik, Mensch

Sicherheitsmaßnahmen

Faktoren auf verschiedenen Ebenen



Cyber-Systeme im maritimen Bereich

Spezielle Anforderungen

Systeme an Land

- Größtenteils vergleichbar mit herkömmlichen IT-Systemen (z.B. Büro-IT)
- Vereinzelt Automation

Systeme auf See

- Heterogene Cyber-physische Systeme
- Operation steht im Vordergrund
- Autonomie ist wichtiger Faktor
- Vergleichbar mit ICS oder Automotive-Branche

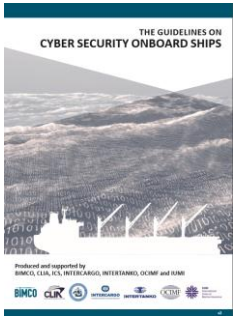
Kommunikation

- Häufig niedrige Bandbreite
- Teils keine Kommunikation möglich
- (noch) keine einheitliche Infrastruktur
- Experten im Zweifel nicht erreichbar

Guidelines und Standards

Referenzen und Dokumente

- Guidelines
  - IMO – Guidelines on Maritime Cyber Risk Management
  - BIMCO et al. – The Guidelines on Cyber Security onboard Ships
  - DNVGL - Recommended Practice – Cyber security resilience management
  - DfT Code of Practice - Cyber Security for Ships
  - CSC - Cyber Security Case Study



- Standards
  - ISO/IEC 27001
  - BSI IT-Grundschutz
  - NIST Framework
  - Technisch: IEC 61162-460 (bisher nur für Navigationssysteme)

Wie geht es weiter? Was ist zu tun?

Cyber Risiken gemeinsam begegnen

- Cyber Sicherheit ist ein Prozess!
- Bewerten Sie Ihre Risiken!
- Ausbau mehrerer Faktoren von Schutzmaßnahmen

- Branchenspezifische Sicherheitsmechanismen!

- Bleiben Sie im Austausch!
- Fördern Sie Austausch!

- DGON AG „Maritime Cyber Risk Management“

Vielen Dank
für Ihre Aufmerksamkeit