Erfahrungen bei der Risikoanalyse von Kritischen Infrastrukturen von KMUs

Clemens Teichmann, Roman Maczkowsky

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Projektträger:
VDI|VDE|IT

Agenda

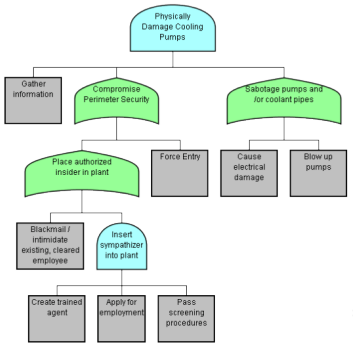
- Ausgangspunkt und Annahmen
- Risikoanalysen bei Betreibern Kritischer Infrastrukturen
- Erfahrungen und Herausforderungen
- Lösungsansatz

Ausgangspunkt

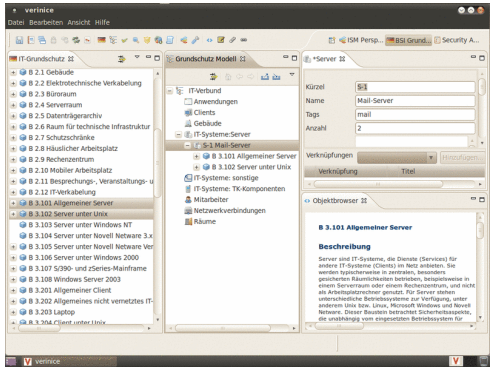
- Kritische Infrastrukturen
  - sind zunehmend von IKT durchdrungen
  - werden oft von kleinen und kommunalen Organisationen betrieben
  - weisen sehr heterogenes Sicherheitsniveau auf

Quelle: MEDIA CONSULTA Deutschland GmbH

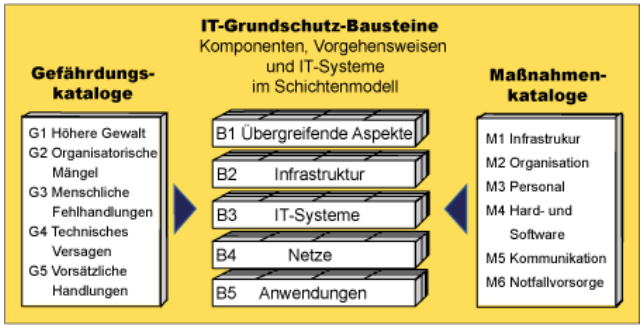
- Risikoanalyse und Bewertung des Sicherheitsniveaus
  - Voraussetzung für effiziente und effektive Maßnahmenauswahl
  - I.d.R. mit generischen Methoden und Werkzeugen
  - Aufwändig und großer Zeitversatz



Quelle: Amenaza



Quelle: verinice



Quelle: BSI IT-Grundschutz

Annahmen

- Heutige Methoden sind
  - sehr aufwändig in Personal und Zeit
  - zu generisch für einfache Anwendbarkeit
  - zu abstrakt in der Abschätzung von Risiken

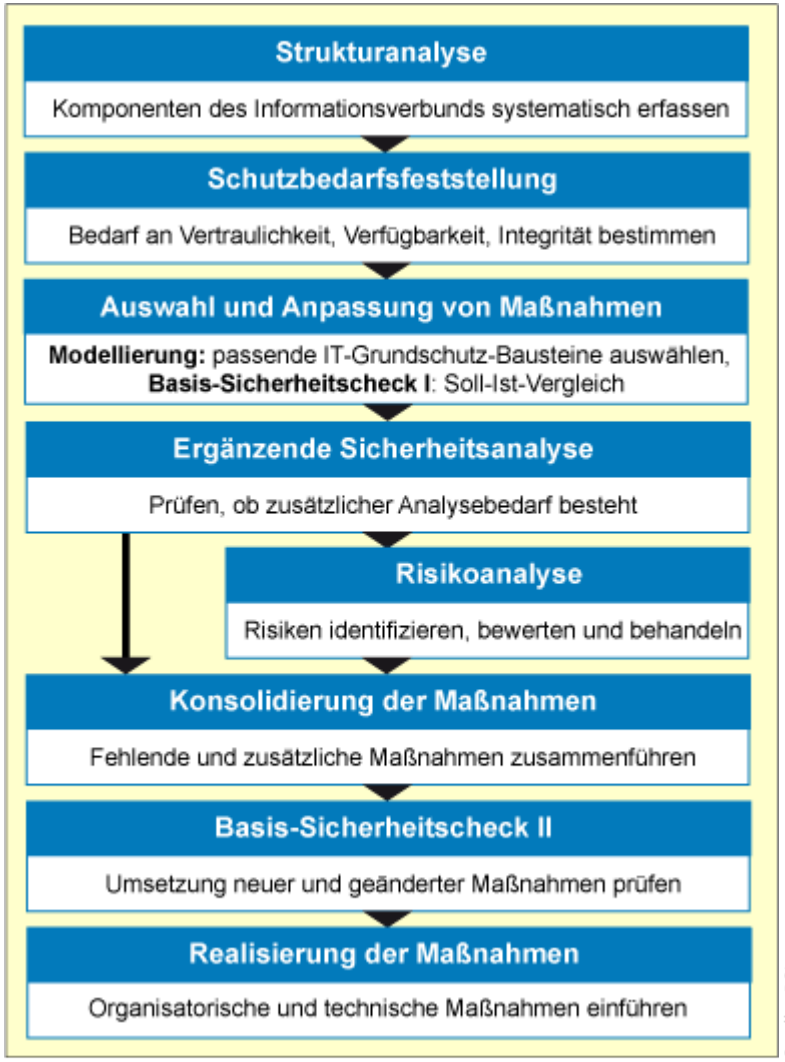
- und die dazugehörigen Werkzeuge sind
  - nicht auf die Untersuchungsbereiche Kritische Infrastruktur angepasst
  - mit wenig Hilfestellung für die Anwender ausgestattet
  - schwer in bestehende Werkzeugketten einzubinden
  - nicht an mögliche Sensoren angebunden.

Zentrale Rettungsleitstelle Gera

- Zentrale Aufgaben der Rettungsleitstelle
  - Alarmieren und Führen des Rettungsdienstes und der Feuerwehren
  - Vermittlung des Ärztlichen Notdienste, Auskünfte über Bereitschaftsdienste
- Infrastruktur
  - 5 Leitstellenarbeitsplätze
  - 6 digitale Leitungen Notrufentgegennahme
  - Direkte Drahtverbindung zur Polizei
  - 8 Relaisfunkstellen im Leitstellengebiet
  - Server für Karten- und Einsatz-leitsystem
  - Internetzugang

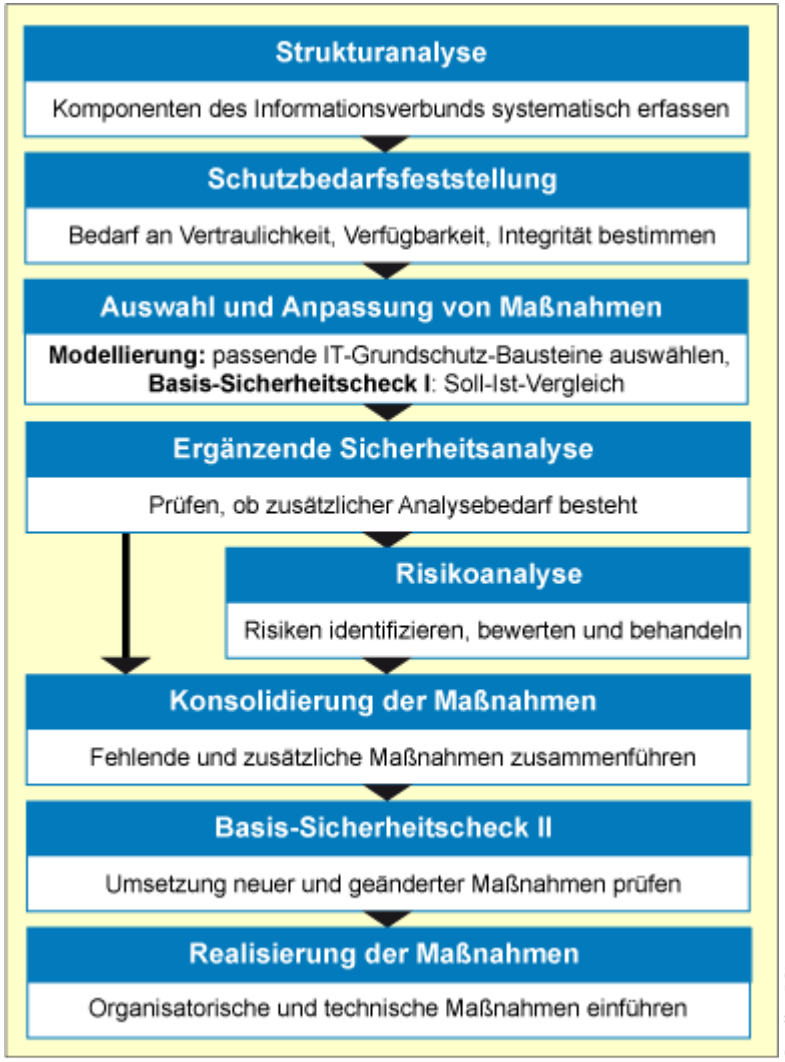
Risikoanalyse mittels BSI IT-Grundschutz

- Vorgehen
  1. Infrastruktur analysieren
  2. Schutzbedarfsfeststellung
  3. Maßnahmenauswahl
  4. Ergänzende Sicherheitsanalyse
- Bewertung
  - Gefährdung über BadUSB, Schadprogramm (Viren) und Eindringen
  - Festlegung von Wirkungs- und Verhaltensindikatoren
  - Größtes Risiko ist die Nichtverfügbarkeit der Notrufentgegennahme durch alle drei Gefährdungen



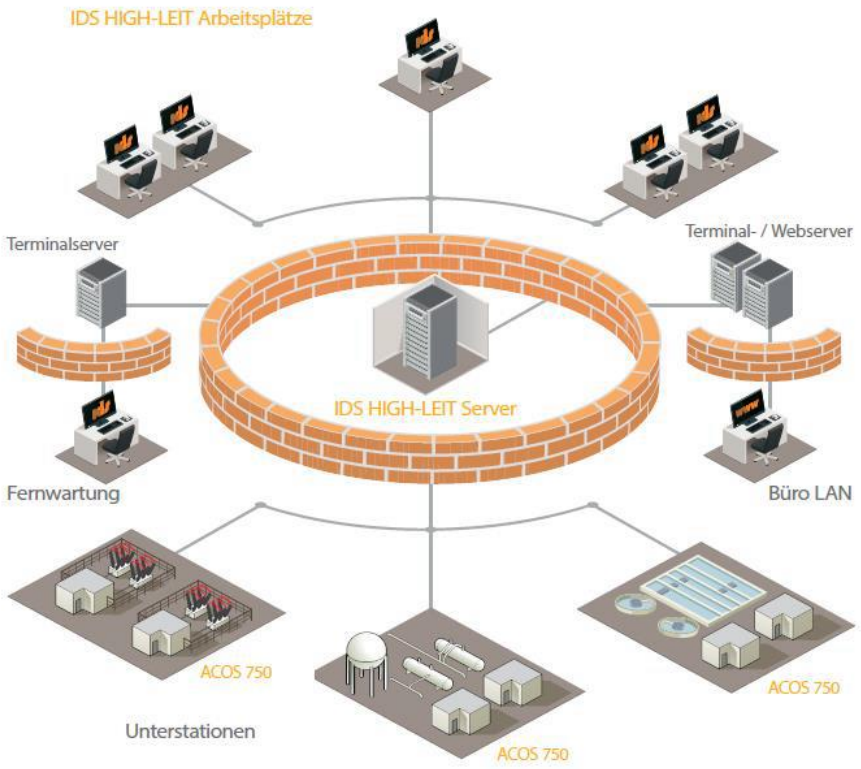
Risikoanalyse mittels BSI IT-Grundschutz

- Vorgehen
  1. Infrastruktur analysieren
  2. Schutzbedarfsfeststellung
  3. Maßnahmenauswahl
  4. Ergänzende Sicherheitsanalyse
- Erfahrung
  - ⊕ Hohe Akzeptanz
  - ⊕ Breite Abdeckung
  - ⊖ Arbeitsintensiv
  - ⊕ Erprobte Vorgehensweise
  - ⊖ Statische Sicht



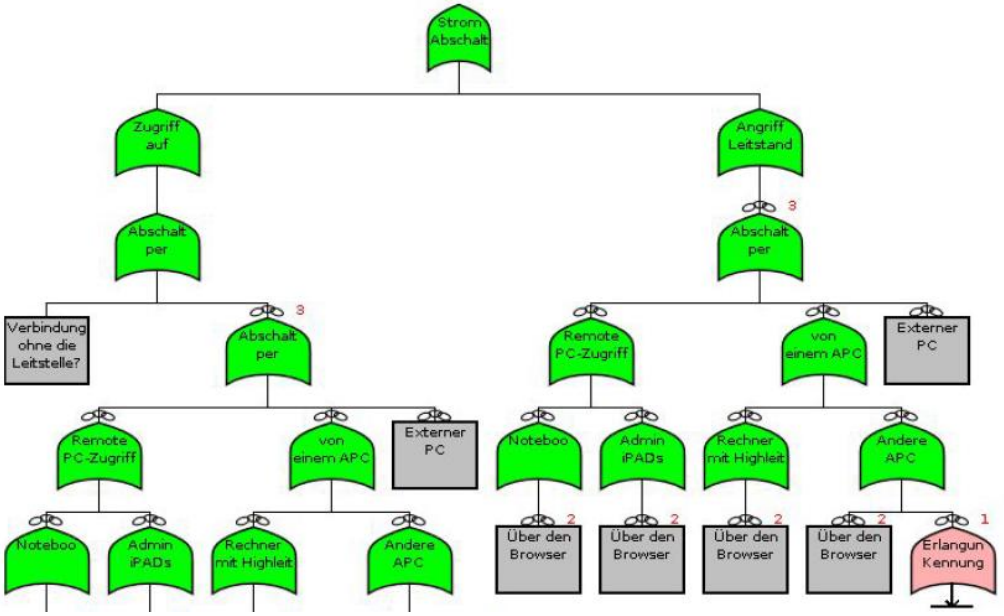
Stadtwerk Haßfurt GmbH

- Zentrale Aufgaben
  - Mehrspartenversorger für Strom, Erdgas, Wasser
  - Erzeugung regenerativer Energien
  - Administration der Netze
- Infrastruktur
  - Netzleitstelle mit Steuerungssoftware
  - Internes Rechenzentrum
  - Verbindung zu externen Erzeugungs-anlagen
  - Internetzugang



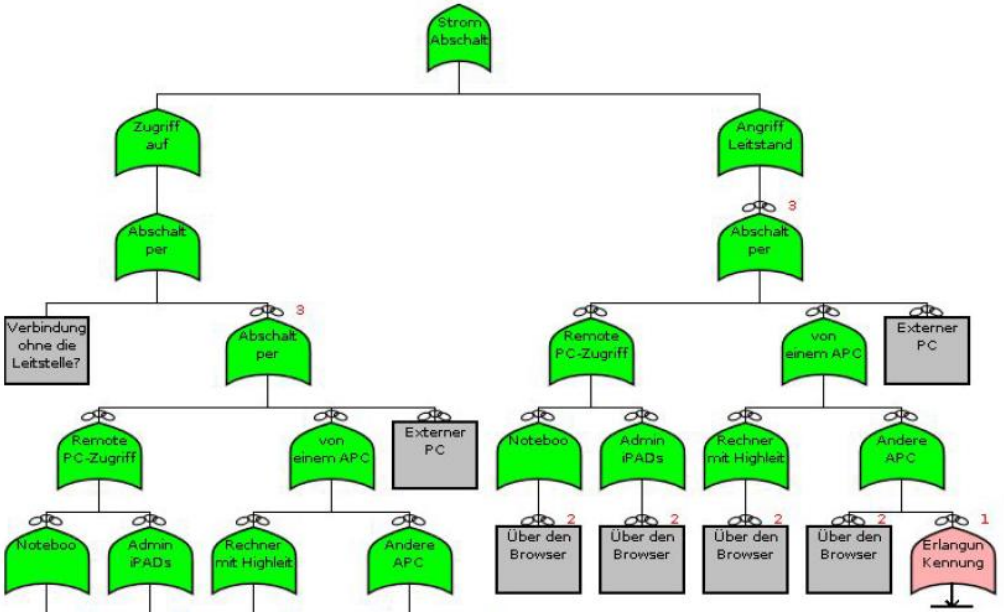
Risikoanalyse mittels Attack Trees

- Vorgehen
  1. Angriffsziele identifizieren und bewerten
  2. Angriffsschritte und Unterschritte zu den Zielen identifizieren und bewerten
  3. Aggregation der Blattwerte
- Bewertung
  - Hauptziel: Abschaltung der Stromversorgung
  - Definition von Bedrohungs-agenten
  - Ziel vollständig nur über physisch gesicherten Zugriff zu erreichen



Risikoanalyse mittels Attack Trees

- Vorgehen
  1. Angriffsziele identifizieren und bewerten
  2. Angriffsschritte und Unterschritte zu den Zielen identifizieren und bewerten
  3. Aggregation der Blattwerte
- Erfahrungen



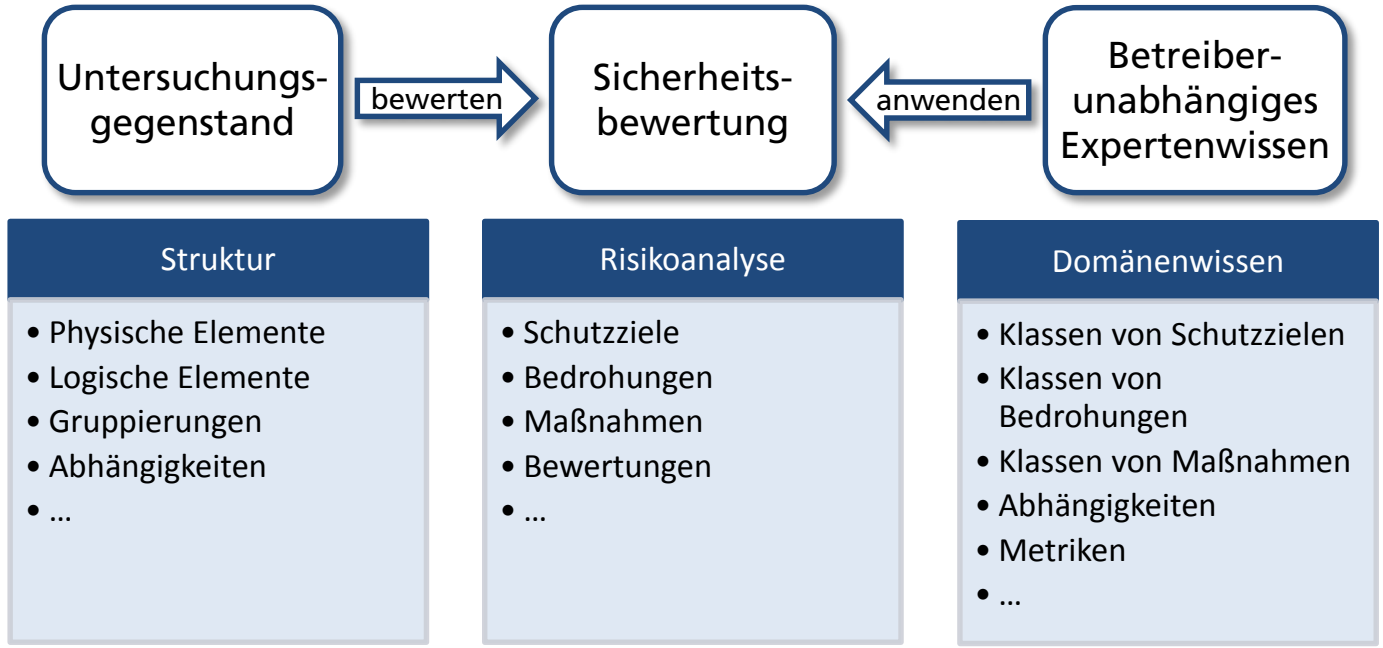
Erfahrungen und Herausforderungen

- Komplexität der Untersuchungsbereiche und vorhandene Ressourcen sehr unterschiedlich
- Ausgewählte Methoden bestimmen Ergebnisse (in Aufwand und Tiefe)
- Schutzbedarfsfeststellung und Angreiferbeschreibungen gut einzuschätzen

- Hoher Ressourcenaufwand bei der Strukturanalyse (trotz Werkzeugunterstützung)
- Mangelhafte oder fehlende Dokumentation der Infrastruktur
- Analyse der Abhängigkeiten zwischen Prozessen und Infrastruktur notwendig
- Notwendige Kommunikation des Expertenwissens
- Schwierige Maßnahmenauswahl in wandelnder Infrastruktur

Lösungsansatz

- Domänenspezifische Modellierung für Kritische Infrastruktur
  - (Wieder-) Verwendung von Domänenwissen und Methodenunterstützung
  - Templates für die Modellierung kritischer Infrastrukturen
  - Kataloge für allgemeine und domänenspezifische Bedrohungen und Maßnahmen



Kontakt

Projektwebsite: *www.mosaikprojekt.info*

Ansprechpartner

Clemens Teichmann

Fraunhofer-Institut für
Angewandte und Integrierte Sicherheit (AISEC)

Tel.: +49 89 32299 86-113
clemens.teichmann@aisec.fraunhofer.de