



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

IT Sicherheit in Kritischen Infrastrukturen

Forschungsansätze zur ganzheitlichen Risikobewertung

Dipl. oec.

Michael Sparenberg

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule Gelsenkirchen
<https://www.internet-sicherheit.de>

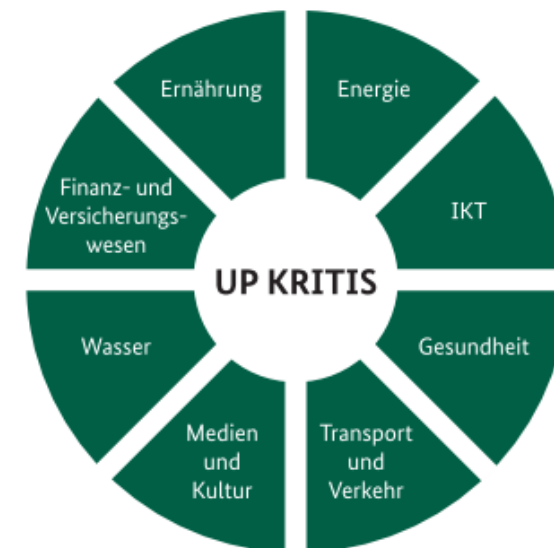


▪ Begriffsdefinition KRITIS (BSI)

„Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“

▪ Sektorengliederung Kritischer Infrastrukturen (BMI)

- Energie
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit
- Wasser
- Ernährung
- Finanz- und Versicherungswesen
- Staat und Verwaltung
- Medien und Kultur



▪ **Wesentliche Merkmale der Energiewirtschaft**

- Grundversorgungsbereich
- Höchste Stabilitätsanforderungen
- Maximaler Schutzbedarf



▪ **Rechtliche Rahmenbedingungen: Energiewende**

- Energiekonzept der Bundesregierung (2010), EU Klima- und Energierahmen 2030:
- Bis 2022: alle Kernkraftwerke in Deutschland abgeschaltet
- Bis 2050: 80% der Stromversorgung aus erneuerbaren Energien (EE)
- Bis 2050: klimaschädliche Treibhausgase um 80 bis 95% reduziert

■ Implikationen

- Reduktion grundlastfähiger Kapazitäten (Kernkraft, Kohle)
- Höherer Anteil von Energieerzeugungsanlagen mit volatilem Output (PV, Wind)
- Begrenzte Speichermöglichkeiten für erneuerbare Energie
- Höherer Bedarf an Transmissionskapazitäten
- Zunehmende Dezentralisierung der Energieerzeugung



Rahmenbedingungen

▪ **Rechtliche Rahmenbedingungen: IT-Sicherheitsgesetz**

- Einhaltung bestimmter IT-Sicherheitsstandards verankert
- Verpflichtung privater Betreiber zur Meldung von IT-Sicherheitsvorfällen
- Ergänzende IT-Regelungen im Umsetzungsplan KRITIS

▪ **Implikationen**

- Obligatorisches Risikomanagement
- Höhere Transparenzanforderungen
- Technische und organisatorische Anpassungen



- **Konsequenzen der veränderten Rahmenbedingungen**
- Höherer Mess- und Regelbedarf in Energieversorgungsnetzen
- Teilweise Öffnung vormals geschlossener Systeme / Übertragungswege
- Vermehrter Einsatz von IT-Komponenten in Produktionsumgebungen
- Neuartige Angriffsvektoren und komplexere Sicherheitsrisiken
- Schmalere Zeitfenster für Korrekturingriffe
- **Fazit: →
Höhere Anforderungen an Qualität, Umfang und Verfügbarkeit
entscheidungsrelevanter Daten**

- **Pilotprojekt: IT-Sicherheit in der Energiewirtschaft**

- Stadtwerke Aachen AG - STAWAG
- Institut für Internet-Sicherheit – if(is)

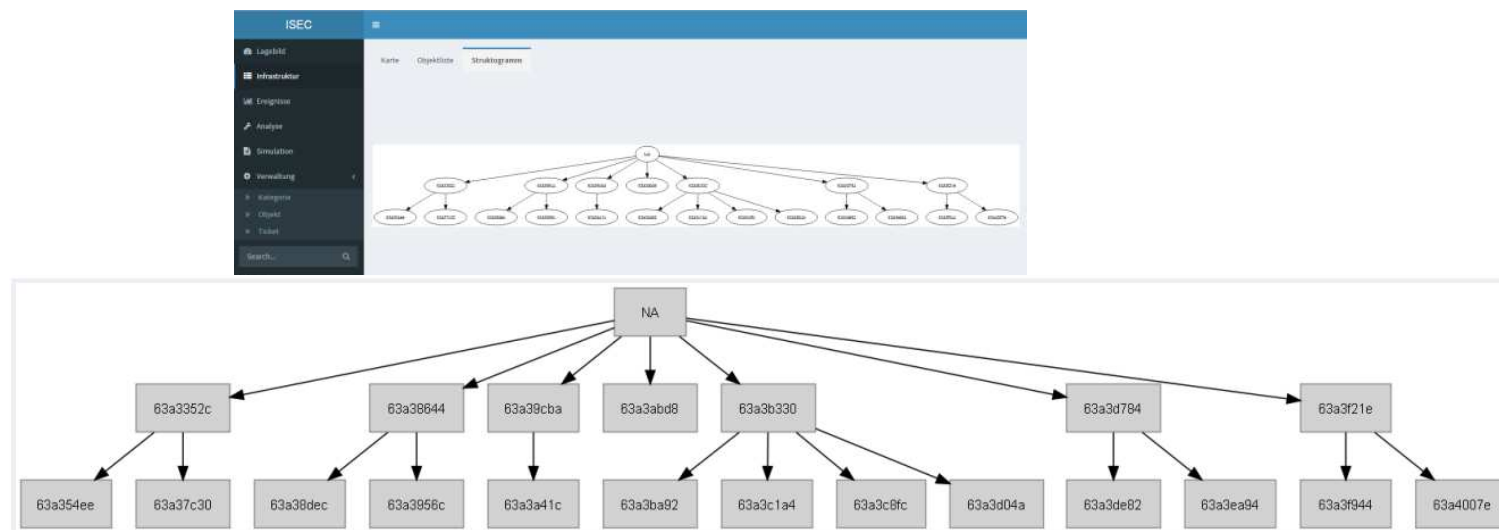


- **Forschungsziele**

- Ganzheitliche Bewertung IT-spezifischer Risiken in Produktionsumgebungen der Energiewirtschaft
- Komplementäre Ausrichtung zu ISM-Systemen
- Proaktive Sicherheitsfeatures (Simulation, Prognose)

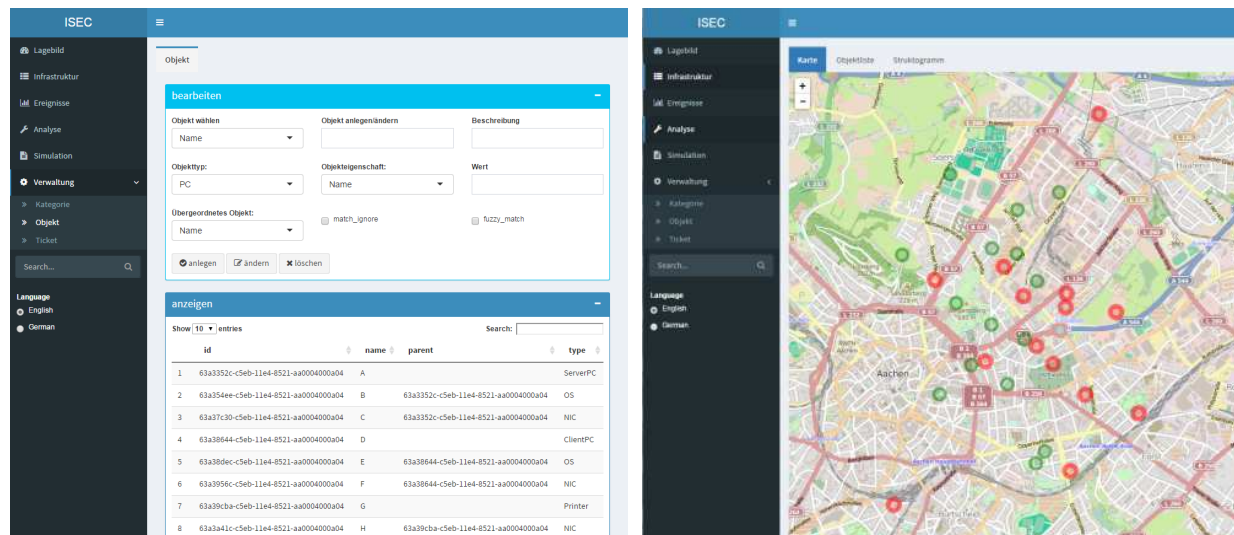
• Lösungsansatz

- Zentrale Inventarisierung der IT-Infrastruktur (Transparenzanforderungen)
- Ganzheitliche Risikobewertung im Wirkungskontext der Einsatzumgebung
- Kontinuierliche Bereitstellung entscheidungsrelevanter Daten
- Aktuelles Lagebild der IT-Sicherheit



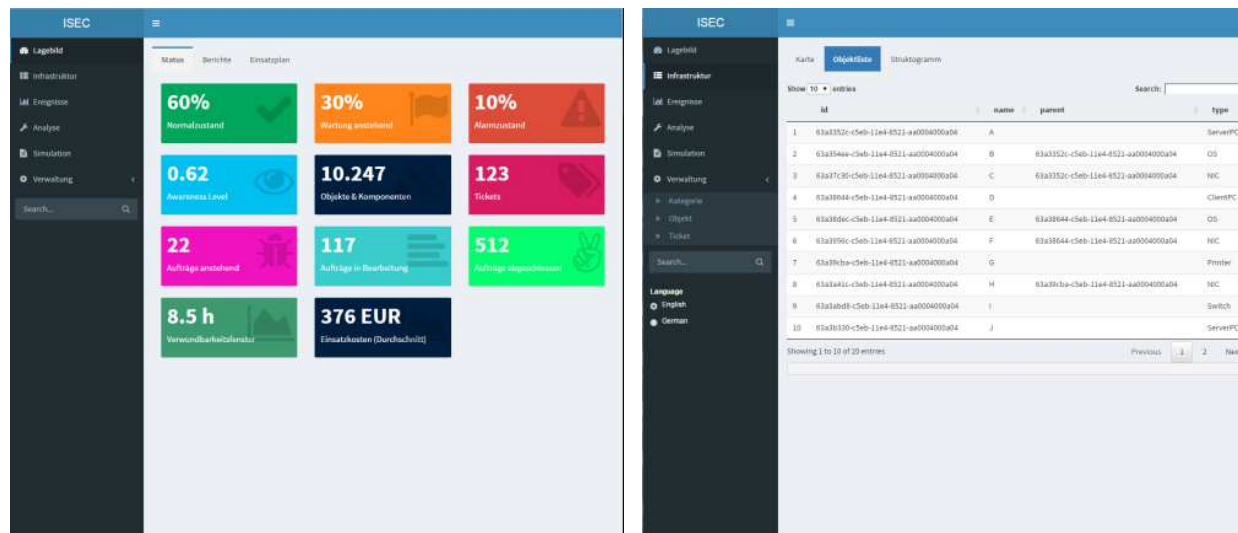
Features

- **IT Asset Management**
- Zentrale Datenverwaltung aller IT-Objekte
- Strukturvisualisierung (Verbundobjekte, Komponenten, Netzwerke)
- Modellierung technisch-organisatorischer Abhängigkeiten (Wirkungskontext)
- Kartenansicht (Geolocation, Clustering)



Features

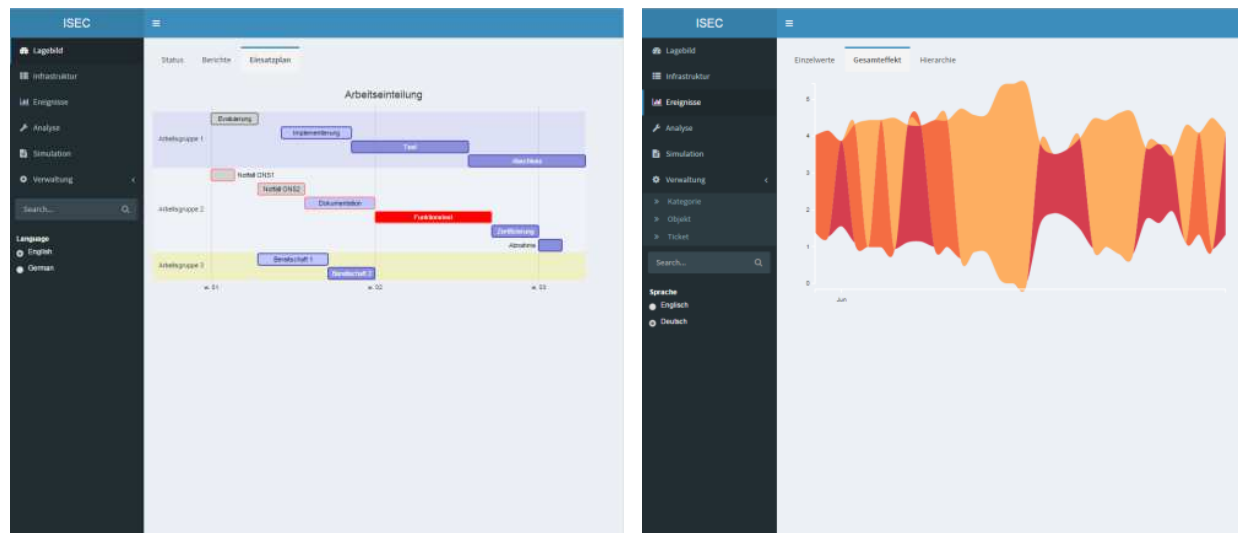
- **Risk Assessment**
- Aktuelles Sicherheits-Lagebild (Dashboard der wichtigsten Kennzahlen)
- Analysefunktionen und Kennzahlendatenbank
- Darstellung akuter Sicherheitsvorfälle und betroffener Objekte
- Simulation von Schwachstellen und Störfällen



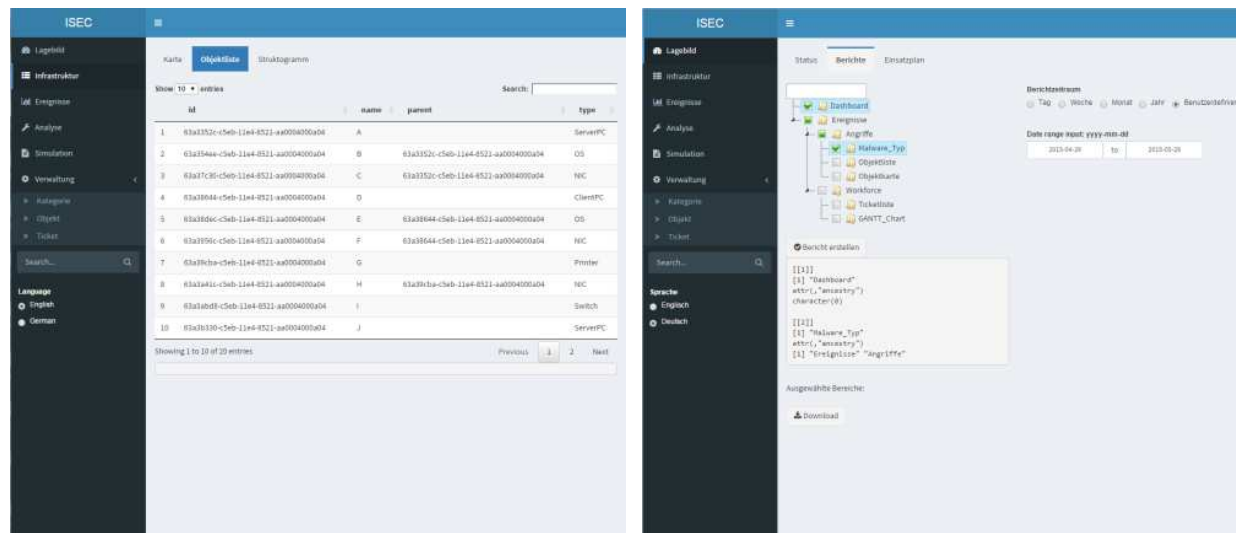
Features

- **Incident Handling**

- Darstellung des Handlungsbedarfs in Verbindung mit Sicherheitsvorfällen
- Unterstützung / Priorisierung der Einsatzplanung (Workforce Management)
- Protokollierung aller sicherheitsrelevanten Ereignisse
- Vollständige Dokumentation der Sicherungsmaßnahmen



- **Weiterentwicklung**
- Verbesserung der Datenverfügbarkeit (Spezifikationen)
- Datenpool zum Incident Handling (Best Practices, Guidelines)
- Praxisgerechte Ausgestaltung der Rahmenbedingungen in KRITIS-Bereichen
- Erfahrungsaustausch und Dialogforum für Wirtschaft und Wissenschaft



- **Forschungsförderung und Projektpartnerschaft**
- **Optionen zur Mitwirkung:**
 - Zugriff auf Spezifikationen industrieller Hardware-Komponenten
 - Anonymisierte Statistiken zu Sicherheitsvorfällen und Gegenmaßnahmen
 - Gemeinsame Entwicklung von Simulationen und Datenmodellen
 - Neue Lösungskonzepte und Funktionserweiterungen
 - Anwendungstransfer in vergleichbare IT-Umgebungen (Industrie 4.0)
 - Beteiligung an Projektkonsortien und Anträgen zur Forschungsförderung
 - ...



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Vielen Dank für Ihre Aufmerksamkeit!

Q&A

Dipl. oec.
Michael Sparenberg

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule Gelsenkirchen
<https://www.internet-sicherheit.de>

if(is)
internet-sicherheit.