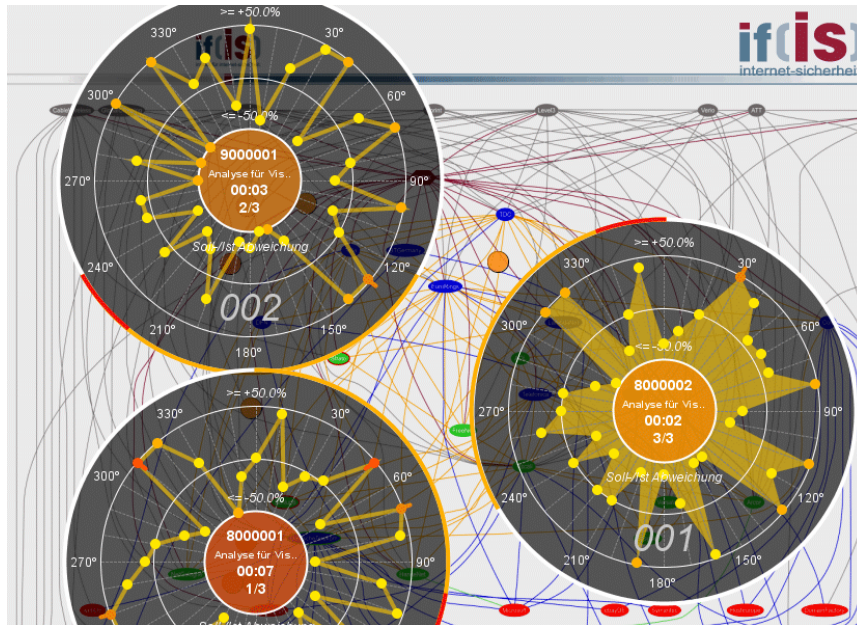


Visualisierung vom Zustand des Internets



Internet-Frühwarnsystem mit VisiX
Visual Internet Sensor Information

Sebastian Spooren
spooren (at) internet-sicherheit.de

Institut für Internet-Sicherheit
<https://www.internet-sicherheit.de>
Fachhochschule Gelsenkirchen

Agenda

- Mehrwert durch Visualisierung
- Zustand des Internets
- Konzeption einer geeigneten Visualisierung
- Ergebnisse der Visualisierung
- Ergebnisse der technischen Umsetzung
- Fazit

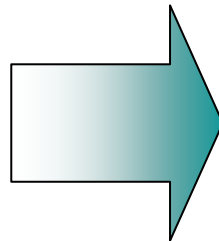
Mehrwert durch Visualisierung (1/2)

Ziele der Visualisierung

- Visualisierung kann helfen, um
 - verborgene oder schwer erkennbare Informationen einfach zu vermitteln
 - Strukturen darstellen und Zusammenhänge aufzeigen
 - die Aufmerksamkeit des Betrachters auf Bedeutsames zu lenken
 - Informationen besonders hervorheben
 - den Betrachter vor einer Informationsflut zu bewahren
 - Darstellen von Informationen die nur zur Erfüllung einer Aufgabe nötig sind

Ziele der Visualisierung

- Übersichtliche Darstellung
- Leichte Wahrnehmbarkeit
- Gute Einprägsamkeit



**Visualisierung vom Zustand
des Internets**

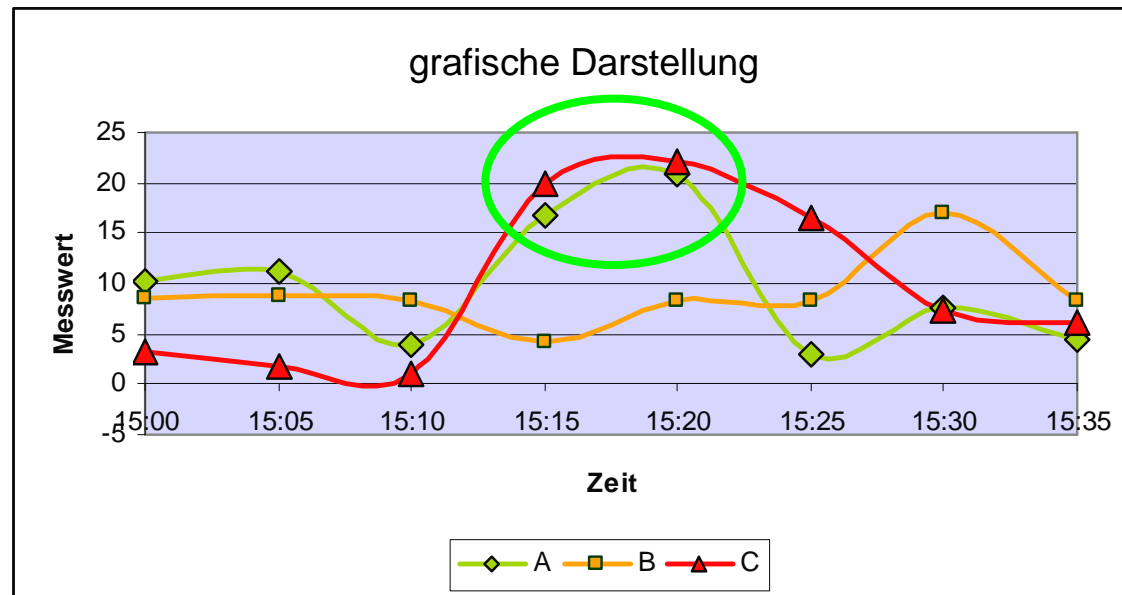
Mehrwert durch Visualisierung (2/2)

Vorteile der Visualisierung an einem Beispiel

- Drei unterschiedliche Messreihen (A,B,C) mit verschiedenen Messzeitpunkten

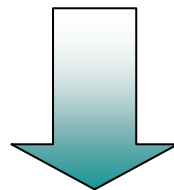
| Zeit | A | B | C |
|-------|------|-----|------|
| 15:00 | 10,3 | 8,5 | 3,3 |
| 15:05 | 11,3 | 8,8 | 1,8 |
| 15:10 | 3,9 | 8,4 | 1,1 |
| 15:15 | 16,8 | 4,2 | 19,9 |
| 15:20 | 21 | 8,4 | 22,1 |
| 15:25 | 2,9 | 8,4 | 16,5 |
| 15:30 | 7,5 | 17 | 7,4 |
| 15:35 | 4,4 | 8,3 | 6,1 |

tabellarische Darstellung



- **Ablesen *exakter Werte***
- **Erkennen von Strukturen** zwischen den Daten
- **Überblick über *alle* Daten** bekommen

- Sehr viele Netzwerke und zahlreiche Kommunikationsknoten
 - Fülle an Informationen
 - Überblick über alle Kommunikationsknoten für Mensch unmöglich
- **Präventivmaßnahmen müssen geschaffen werden**
 - Überblick über Veränderungen (Störungen, Angriffe) an Kommunikationsknoten
 - Gefahren und Risiken rechtzeitig erkennen
 - Schäden reduzieren



**Dringliche Entscheidungen müssen
einfacher, schneller und effizienter getroffen werden**

Konzeption einer geeigneten Visualisierung

Anforderungen an die Visualisierung

Entwicklung eines Visualisierungssystems zur Darstellung vom aktuellen Zustand des Internets

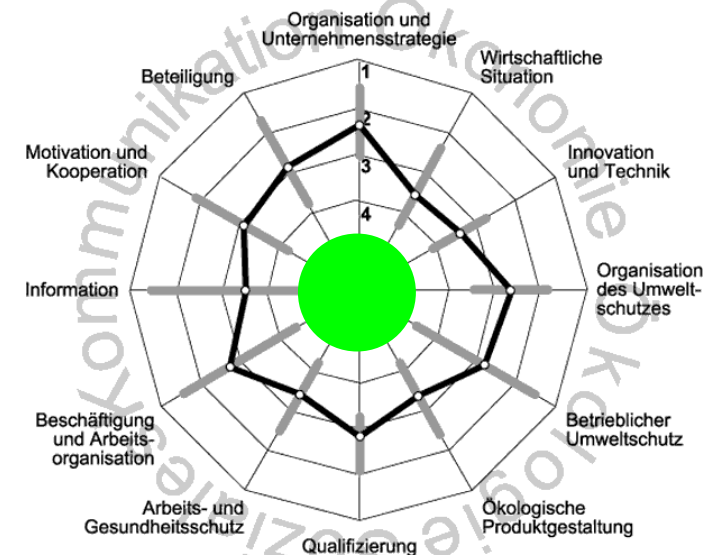
- Übersichtliche Darstellung wichtiger Kommunikationsknoten
- Schutzmaßnahmen für komplexe Angriffsmuster und Störungen
 - **Darstellung von** bedeutenden **Parametern** eines Knotens
 - Beispiel: TCP – Destination Port 25 (SMTP / für E-Mail-Kommunikation)
Ist das Datenaufkommen des E-Mail-Verkehrs im normalen Bereich?
 - **Zusammenhänge untereinander** müssen deutlich werden
- **Räumlicher** (wo) und **zeitlicher** (wann) **Kontext** müssen dargestellt werden

Konzeption einer geeigneten Visualisierung Darstellung eines Kommunikationsknotens

- Entwicklung einer **Darstellungskomponente** als Repräsentant eines **Kommunikationsknotens**
- Herausforderung bei der Abbildung
 - Übersichtliche Darstellung (Ort der Messdatenerhebung)
 - Detaildarstellung (Parameter eines Knotens)
 - Aktuelle Darstellung (Zeitpunkt der Messdatenerhebung)

Dafür müssen **Struktur- und Wertedarstellungen kombiniert** werden

- Als Basisform ein Netzdiagramm
- Parameterdarstellung über Achsen
- Zentrum des Diagramms spiegelt Ort der Messdatenerhebung wieder

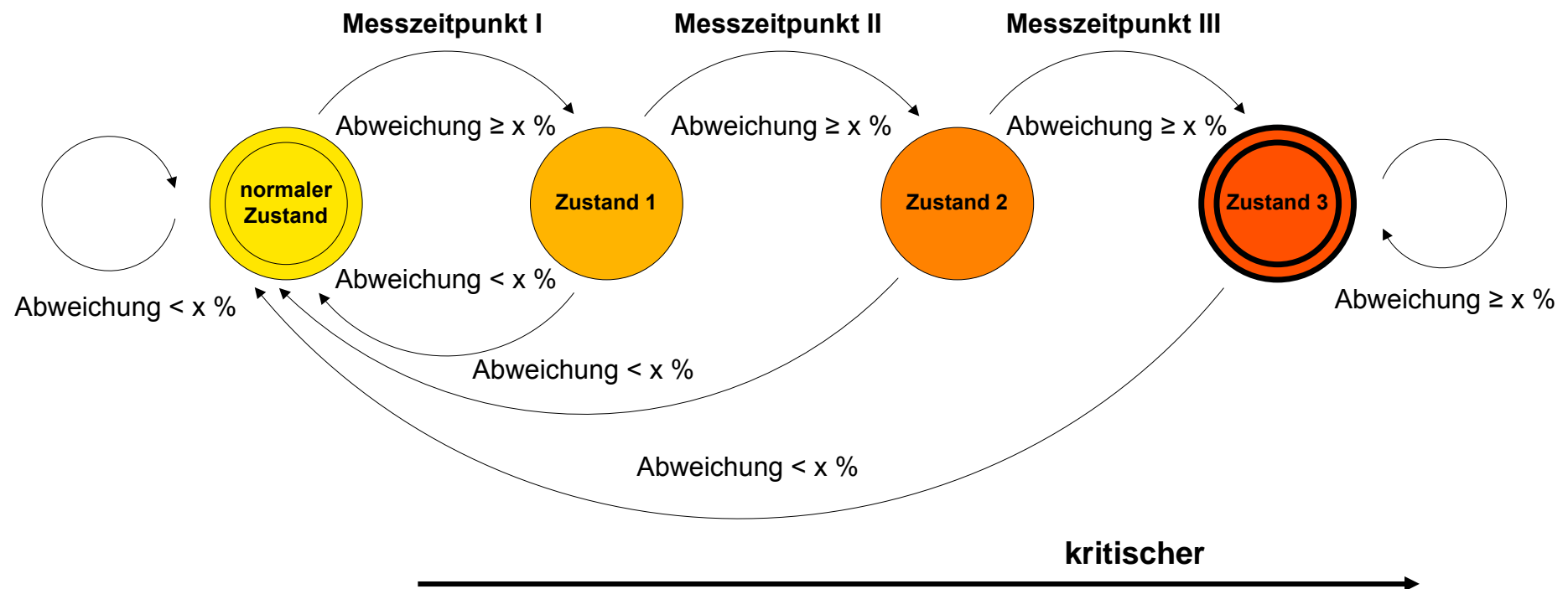


Konzeption einer geeigneten Visualisierung

Generierung von kritischen Zuständen für das Internet

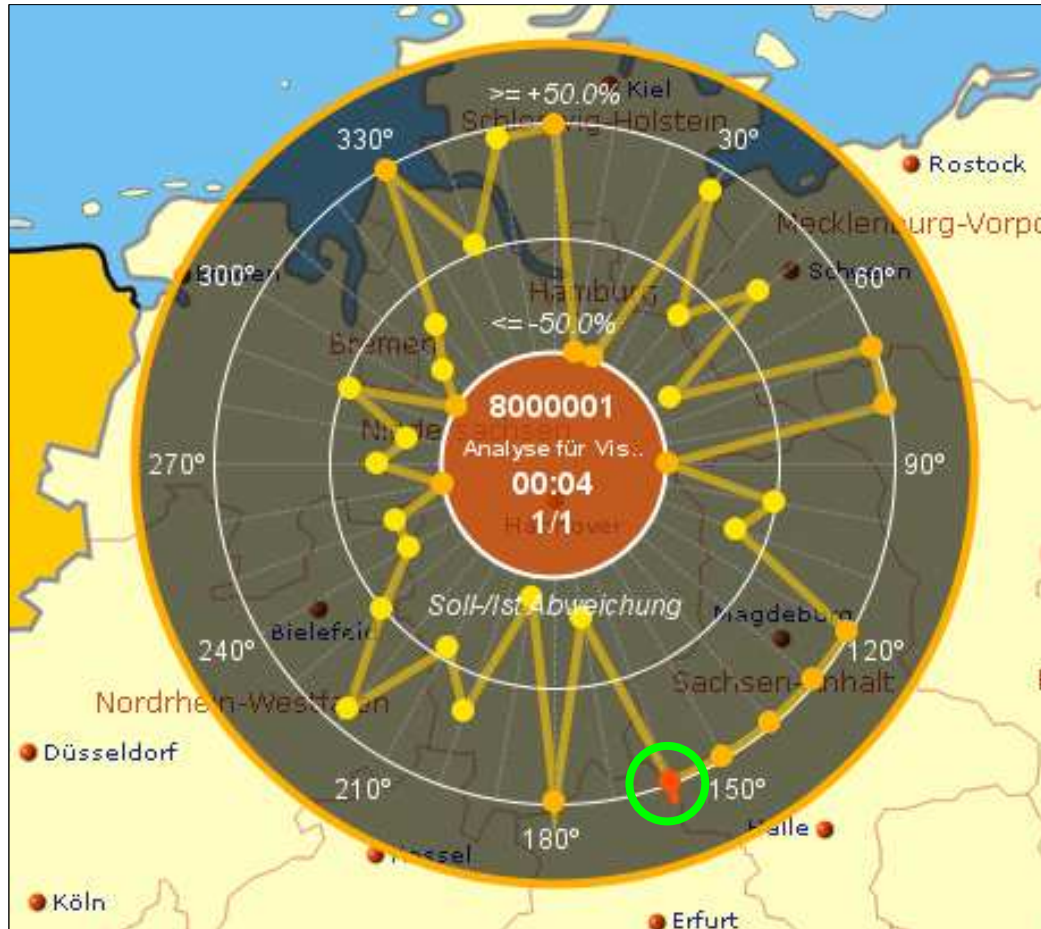
Um Zustände zu generieren, folgende Überlegungen ...

- Jedem Kommunikationsparameter liegt Soll-/Ist (Prognose-/Mess) Wert zugrunde
- weicht Ist- gegenüber Sollwert, um $x\%$ ($x = \text{Grenzwert}$) ab
→ Zustandswechsel



Ergebnisse der Visualisierung

Umsetzung einer Darstellungskomponente

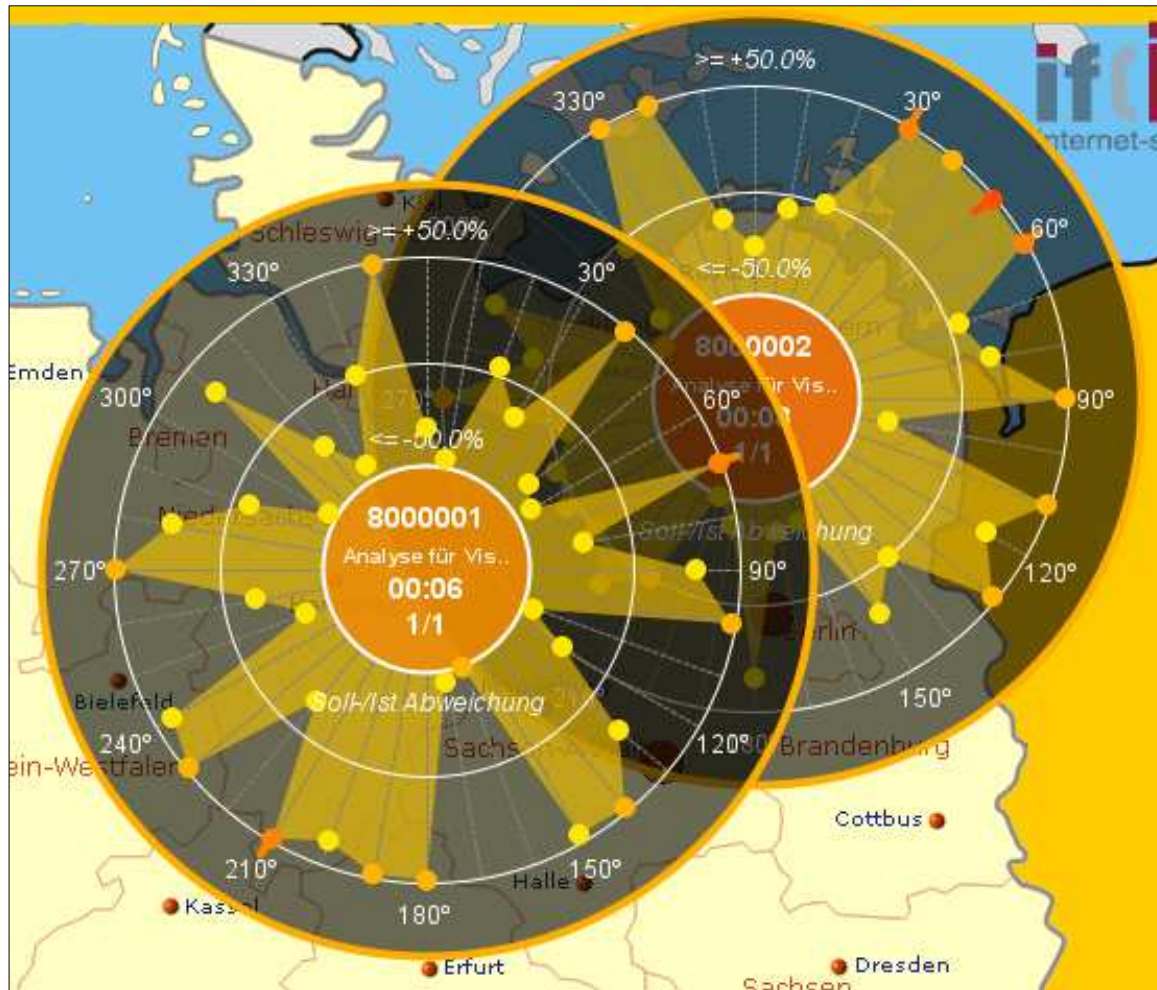


- Position eines Knotens
- Abgrenzung der Parameter durch Gradeinteilung
- Ausprägung einer Abweichung über Radiusposition
- Zustände über Farbe kodiert
- Trenddarstellung durch *Peak*
- Identifikation einer Quelle über Infopanel im Zentrum
- geschätzte Zeit bis Datenupdate
- gruppierte Darstellung der Parameter, um Zusammenhänge zu erkennen

Problem: Darstellung von mehreren Datenquellen in unmittelbarer Nähe

Ergebnisse der Visualisierung

Überschneidung der Darstellungskomponenten



- Überschneidung zweier Datenquellen bei der Darstellung ihrer Merkmale

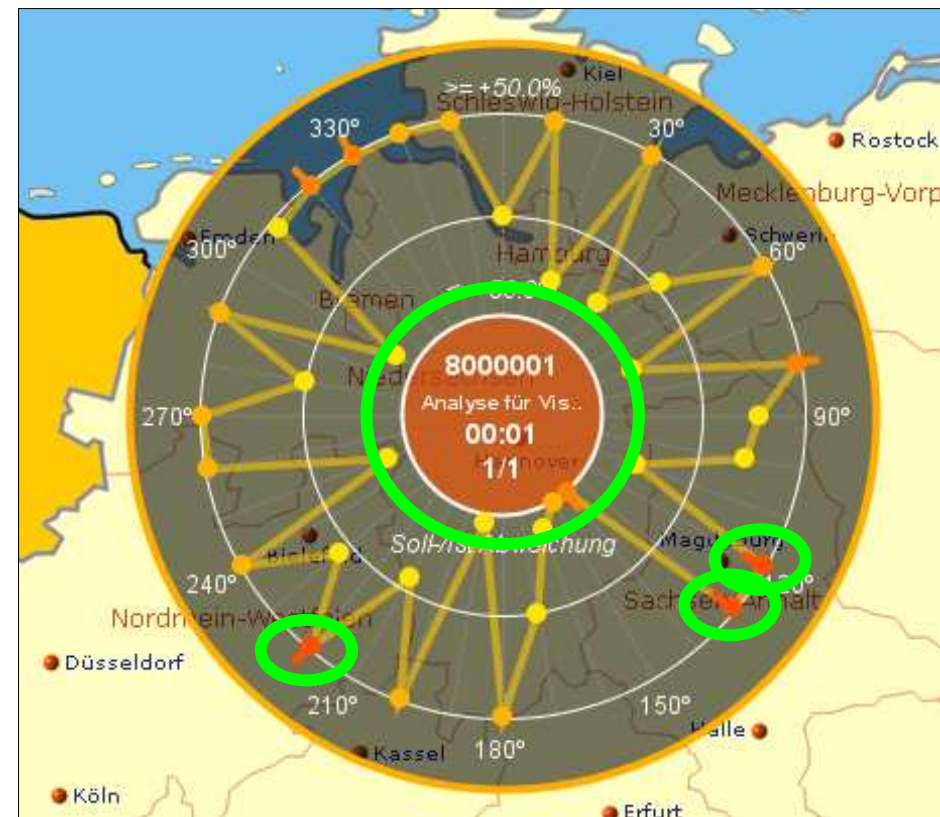
Weitere Herausforderung

- Darstellung komplexer Informationen auf möglichst kleinem Raum

Ergebnisse der Visualisierung

Aggregation von Zuständen einer Datenquelle (1/2)

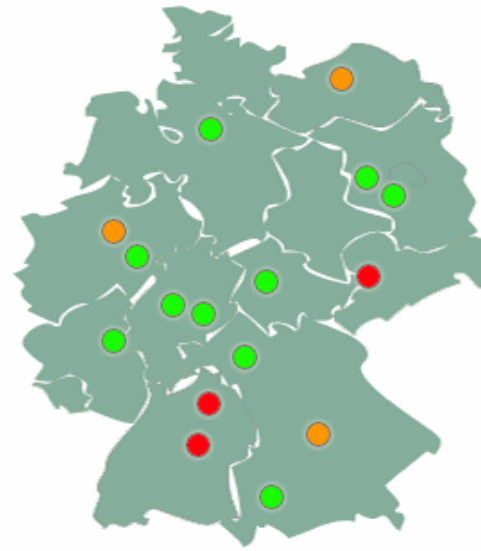
- Übersichtliche Darstellung der Zustände ermöglichen
 - Knoten möglichst auf *kleinem Raum* abbilden
 - **Zustände** der Parameter **zu einer Klasse zusammenfassen**
- Nur *ein abstrahierter Wert* stellt den Zustand eines Knotens dar
- Benutzer kann zu jedem Knoten auswählen
 - wie viele Merkmale vom Zustand X notwendig sind,
 - um einen *Allgemeinzustand X* zu visualisieren



Ergebnisse der Visualisierung

Aggregation von Zuständen einer Datenquelle (2/2)

Modell der Wetterzustände wird auf Zustände bedeutungsvoller Kommunikationsknoten übertragen



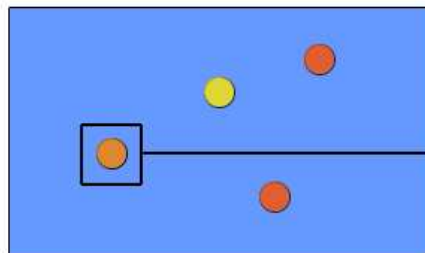
- übersichtliche Darstellung von Zuständen
- Zustände lassen sich auf einen Blick miteinander vergleichen

- Werte vieler Messstationen werden zusammengefasst und repräsentieren *einen Zustand* für ein Gebiet

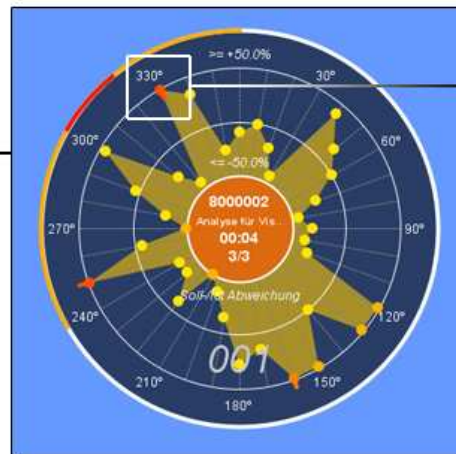
- Zustände der Parameter eines Kommunikationsknotens werden auch hier zu einem Zustand zusammengefasst

Ergebnisse der Visualisierung Übersicht der Darstellungskomponenten

- Informationsdarstellung nach dem Prinzip: „details on demand“



Grafische Darstellung in minimierter Ansicht



Grafische Darstellung in maximierter Ansicht



Detaildarstellung einer Soll-/Ist- Abweichung

| Position | ID | Beschreibung | Soll/Ist-Abweichung | Status | Trend |
|----------|--------|--|---------------------|-------------------|----------|
| 10P | 121181 | P (Product number 17) | +54,22 % | erfüllt | abwärtig |
| 10P | 81981 | HTTP (Standard Method 1420) | +18,35 % | besonders erfüllt | abwärtig |
| 2P | 121181 | CMP (Type 0 auto repair 782) | +42,21 % | normal | stabil |
| 2P | 121181 | CMP (Type 3 auto repair 782) | +100,00 % | normal | stabil |
| 2P | 121181 | CMP (Type 4 auto repair 782) | -25,81 % | normal | stabil |
| 2P | 121181 | CMP (Type 12 auto repair 782) | -34,87 % | normal | stabil |
| 4P | 121181 | CMP (Type 8 auto repair 782) | -44,84 % | normal | stabil |
| 6P | 121181 | P (Product number 1) | -80,00 % | normal | stabil |
| 6P | 121181 | P (Product number 2) | -88,84 % | normal | stabil |
| 8P | 491981 | UCP (Destination port 80) | -43,88 % | normal | stabil |
| 8P | 491981 | UCP (Destination port 443) | -49,85 % | normal | stabil |
| 11P | 524292 | UCP (Registered destination port 1024-49151) | -22,75 % | normal | stabil |
| 11P | 199101 | TCP (Source port 21) | -12,28 % | normal | stabil |
| 12P | 199101 | TCP (Source port 20) | +121,21 % | normal | stabil |
| 13P | 199101 | TCP (Source port 80) | +16,20 % | normal | stabil |
| 14P | 197181 | TCP (Source port 443) | -23,78 % | normal | stabil |
| 15P | 317981 | TCP (Dynamic source port 1024-65535) | -17,81 % | normal | stabil |
| 16P | 317981 | TCP (Destination source port 80) | +13,28 % | normal | stabil |

Tabellarische Darstellung

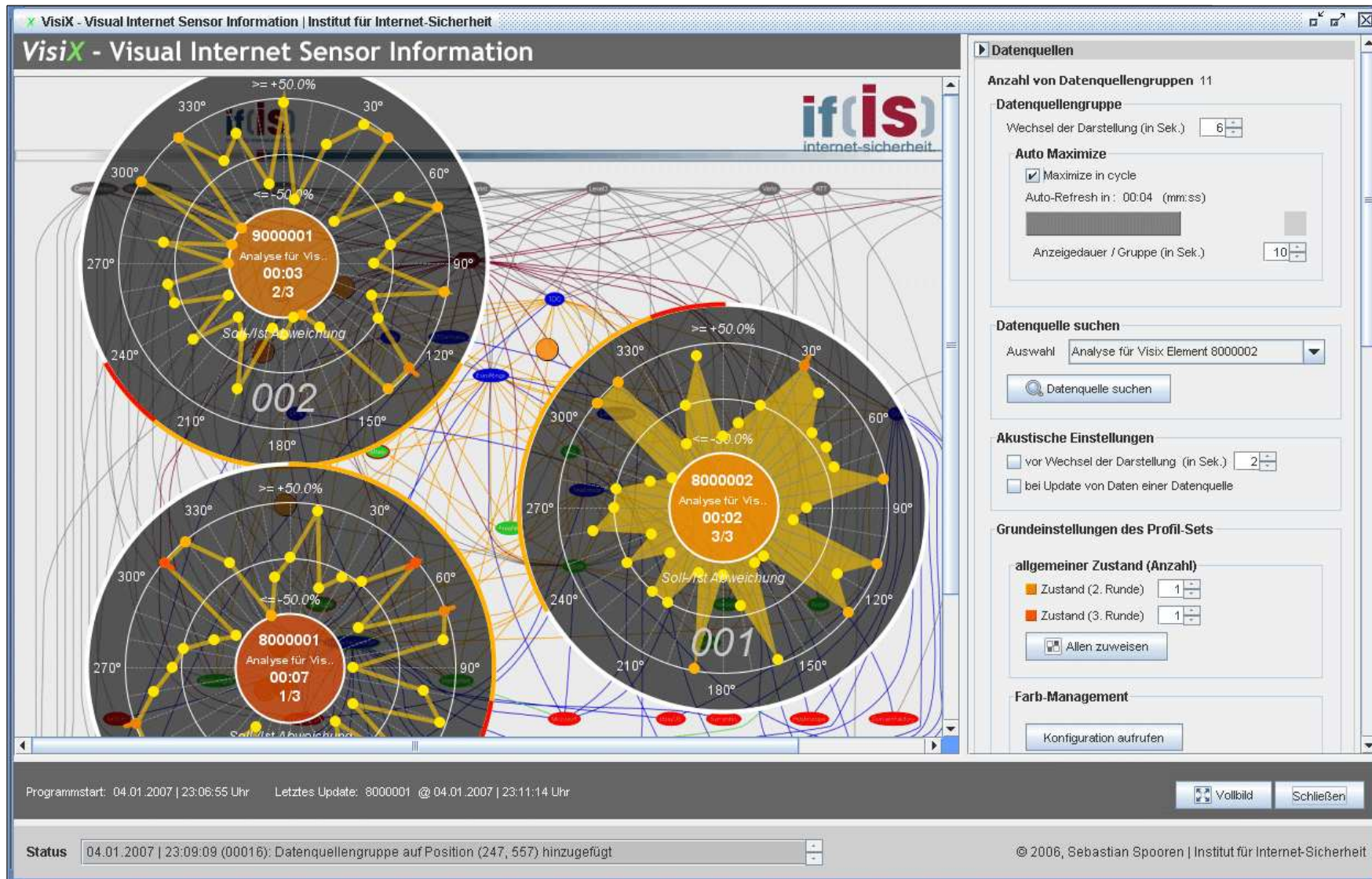
Durch Kombination der Darstellungen

- Überblick über möglichst viele Zustände
- Sicht auf Details und Zusammenhänge

level of detail



Ergebnisse der Visualisierung Benutzerschnittstelle



Ergebnisse der Visualisierung

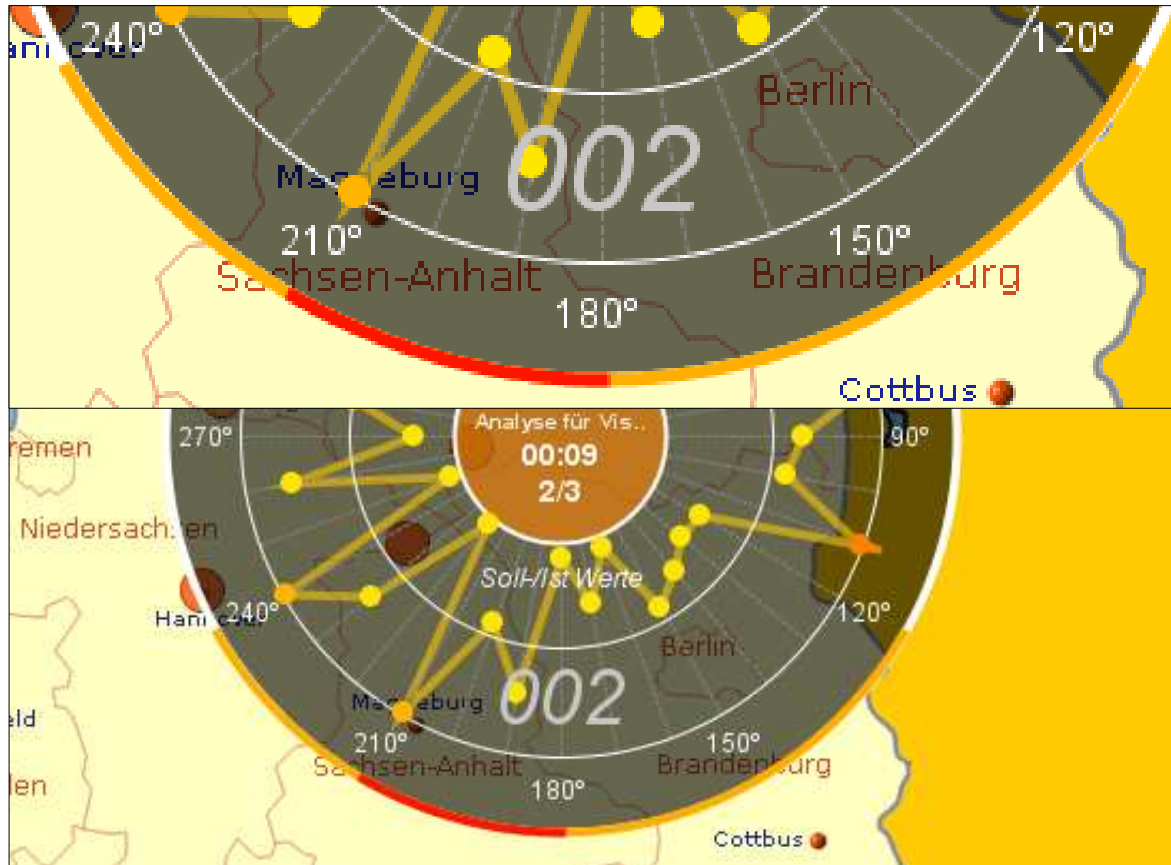
Mehrere Knoten auf gleichen Koordinaten (1/3)

Eine weitere Herausforderung besteht bei der Abbildung mehrerer Kommunikationsknoten auf gleichen Koordinaten

- beliebig viele Knoten in Form einer Gruppe zusammenfassen
- Lösung: noch mehr *Dynamik* in die Darstellung!
 - Jeder Kommunikationsknoten wird mit seinen Parametern in einem festen *Zeitfenster* visualisiert

Ergebnisse der Visualisierung

Mehrere Knoten auf gleichen Koordinaten (2/3)



3 Datenquellen zusammengefasst

- Radialer Fortschrittsbalken verdeutlicht verbleibende Zeit bis zum Wechsel der Darstellung

Problem

- Es kann bei den Datenquellen, *die gerade nicht dargestellt werden*, zu einem kritischen Zustand kommen

Noch problematischer

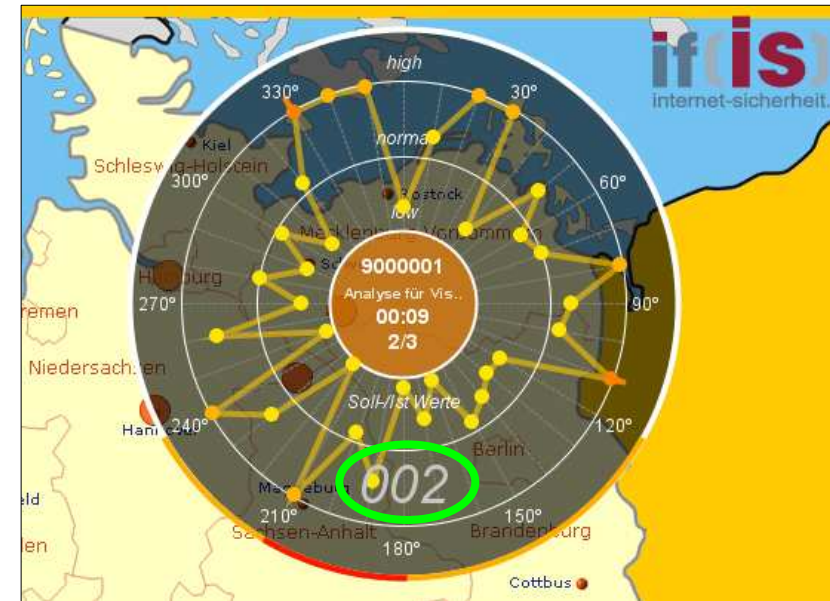
- *Alle* Datenquellen der Gruppe erhalten nahezu zeitgleich kritischen Zustand!

Ergebnisse der Visualisierung

Mehrere Knoten auf gleichen Koordinaten (3/3)

Lösung des Problems

- Datenquellengruppe bekommt ID
- Aufschlüsselung einer Datenquellengruppe in tabellarischer Form
- Sprung zu beliebiger Datenquelle möglich (zeitlicher Ablauf wird angehalten)



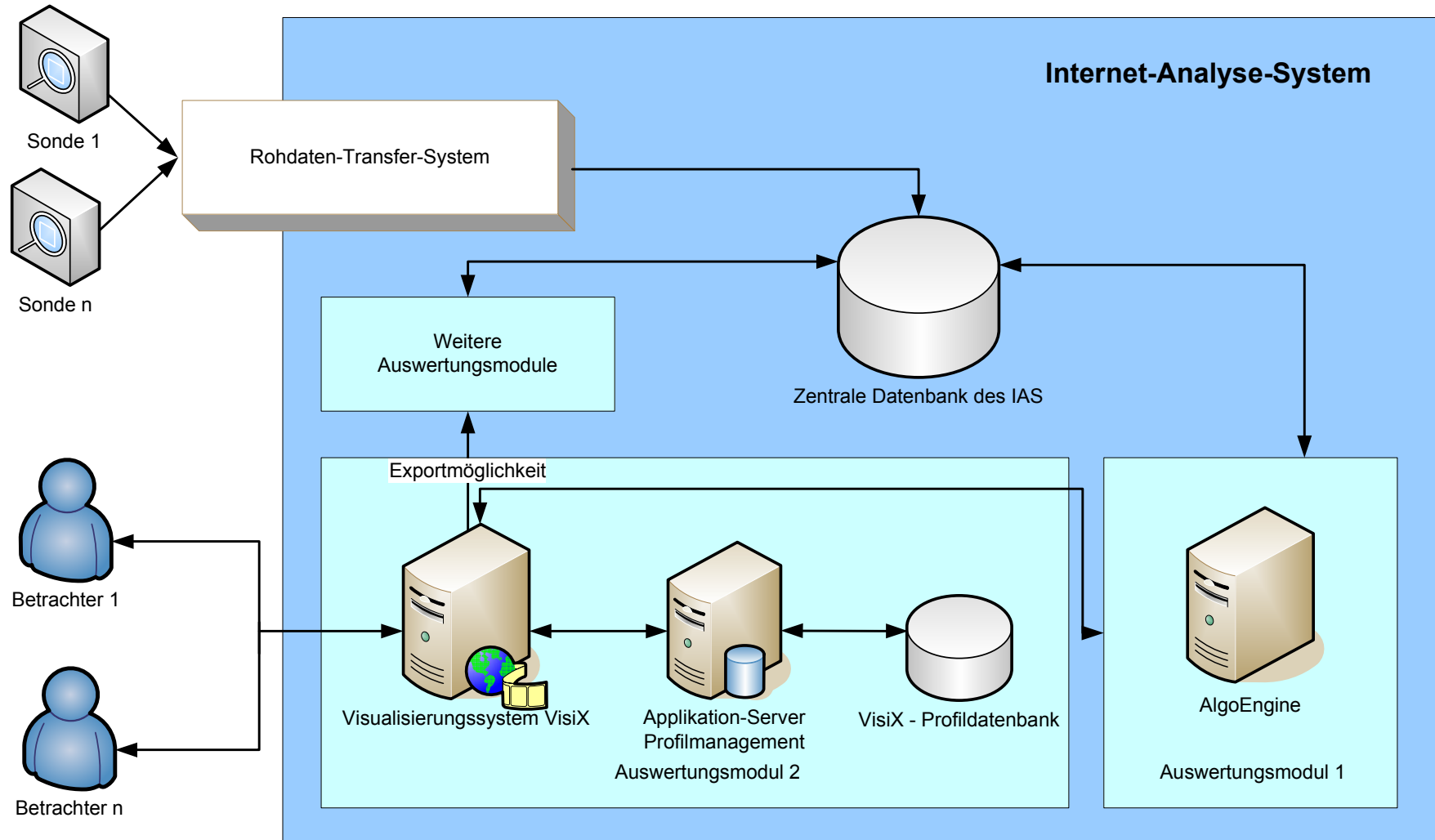
Aufschlüsselung der Datenquellengruppe

Datenquellenauswahl Gruppe: 002

| Id | Beschreibung | Status ▼ | Darstellung | Messwert-Details |
|---------|-----------------------------------|---------------------|-------------------|------------------|
| 8000001 | Analyse für Visix Element 8000001 | besonders auffällig | wechseln & halten | anzeigen |
| 9000001 | Analyse für Visix Element 9000001 | auffällig | wechseln & halten | anzeigen |
| 8000002 | Analyse für Visix Element 8000002 | normal | wechseln & halten | anzeigen |

Schließen

Ergebnisse zur technischen Umsetzung Topologischer Zusammenhang



Fazit (1/2)

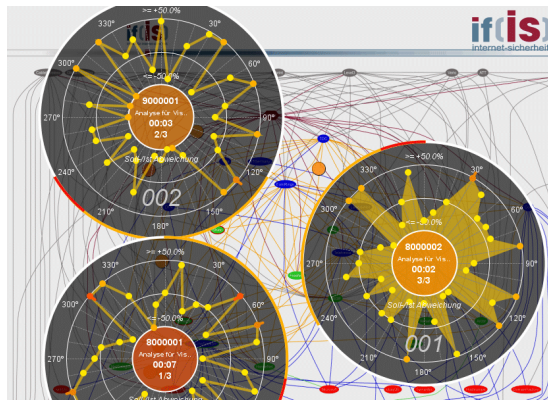
- Bei Auswahl bedeutender Kommunikationsknoten kann das Visualisierungssystem den **Zustand des Internets abbilden**
- **komplexe Zusammenhänge** können zu einem Messzeitpunkt und über mehrere Messzeitpunkte hinweg **veranschaulicht werden**
- Schnittstelle für Datenexport bietet Möglichkeit für weiterführende Analysen
- Aufgrund **flexibler Architektur** einfache **Integration in andere Anwendungsbereiche**
- Anbindung neuer Informationsquellen ohne Programmieraufwand möglich
 - anpassungsbedürftige Parameter lassen sich unabhängig vom Quellcode über deklarative Stellschrauben modifizieren

Fazit (2/2)

- Speicherung der Profile an zentraler Stelle
 - Einstellungen müssen nicht bei jedem Programmstart neu konfiguriert werden
 - schneller Wechsel zwischen verschiedenen Anwendungsfällen jederzeit möglich
 - ortsunabhängiger Zugriff auf unterschiedliche Anwendungsfälle
- Zur Praxistauglichkeit müssen Prognosewerte (für Soll-/Ist- Abweichungen) in angemessener Qualität vorliegen
→ unbrauchbare Soll-/Ist- Abweichungen → unbrauchbaren Zuständen
- Liegen hingegen konkrete Soll-Werte vor (zum Beispiel: Ozonwerte), kann das Visualisierungssystem sofort verwendet werden

Visualisierung vom Zustand des Internets

Vielen Dank für Ihre Aufmerksamkeit



Fragen ?

Sebastian Spooren
spooren (at) internet-sicherheit.de

Institut für Internet-Sicherheit
<https://www.internet-sicherheit.de>
Fachhochschule Gelsenkirchen

if(is)
internet-sicherheit.

 Fachhochschule
Gelsenkirchen