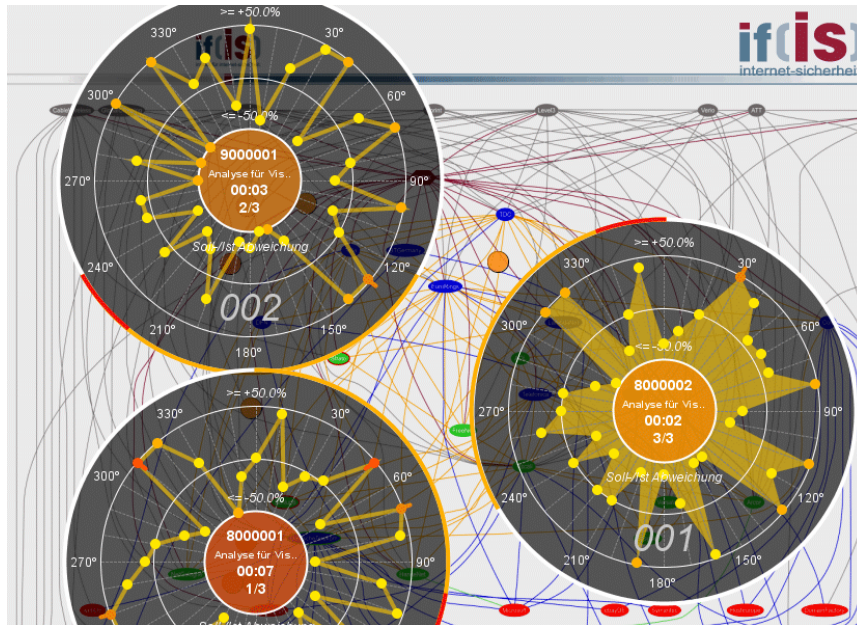


Verfügbarkeit und Notfallplanung mit Hilfe der Visualisierung



D•A•CH Security 2009

Visual Internet Sensor Information (VisiX)

Sebastian Spooren
spooren (at) internet-sicherheit.de

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

if(is)
internet-sicherheit.



Fachhochschule
Gelsenkirchen

Agenda

- Mehrwert durch Visualisierung
- Zustand großer Netzwerke
- Verfügbarkeit und Störungen darstellen
- Konzeption einer geeigneten Visualisierung
- Ergebnisse der Visualisierung
- Ergebnisse der technischen Umsetzung
- Fazit

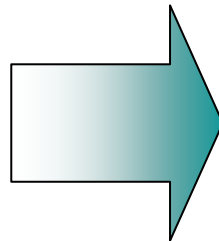
Mehrwert durch Visualisierung (1/2)

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
großer Netzwerke**

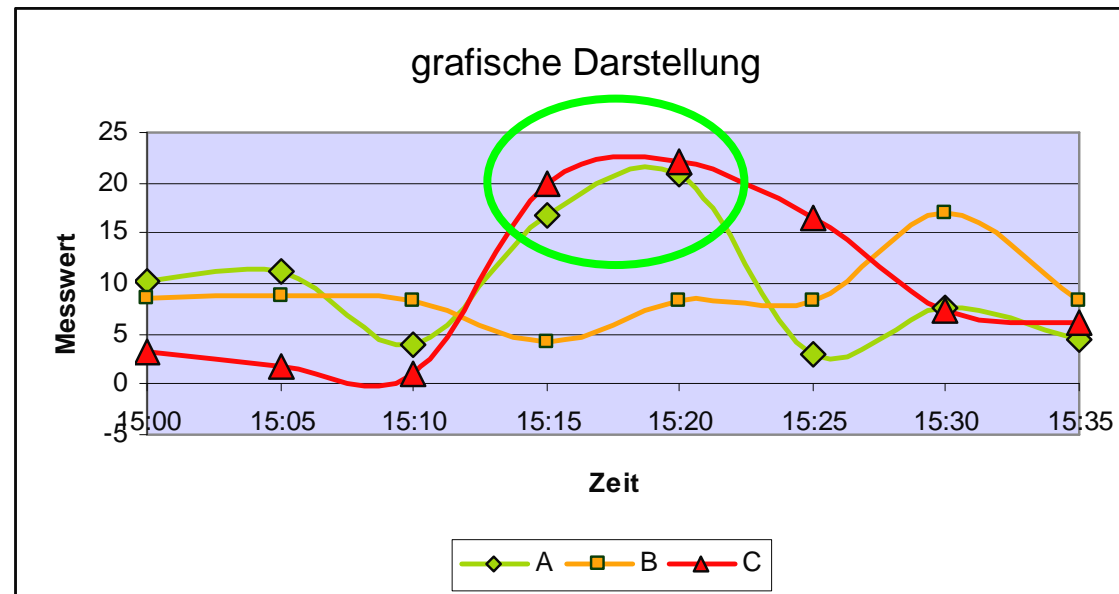
Mehrwert durch Visualisierung (2/2)

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

Zustand großer Netzwerke

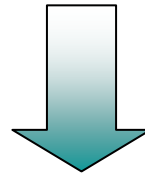
- **Viele Sub-Netze und zahlreiche Kommunikationsknoten**
 - Fülle an Informationen
 - Überblick über alle Kommunikationsknoten für Mensch unmöglich
- **Interesse von Netzmanagement- und Sicherheitszentren**
 - Verfügbarkeit laufender Systeme im Blickfeld
 - Schnelle Entscheidungshilfe bei Störungen und Angriffen

Schaffen von Präventivmaßnahmen → Im Notfall schnell reagieren

- Überblick über Veränderungen an Kommunikationsknoten
- Gefahren und Risiken rechtzeitig erkennen
- Schäden reduzieren
- Dringliche Entscheidungen müssen *einfacher, schneller* und *effizienter* getroffen werden

Entwicklung eines Visualisierungssystems

→ *Visualisierung vom aktuellen Zustand* großer Netzwerke / des Internets



Anforderungen an eine geeignete Visualisierung

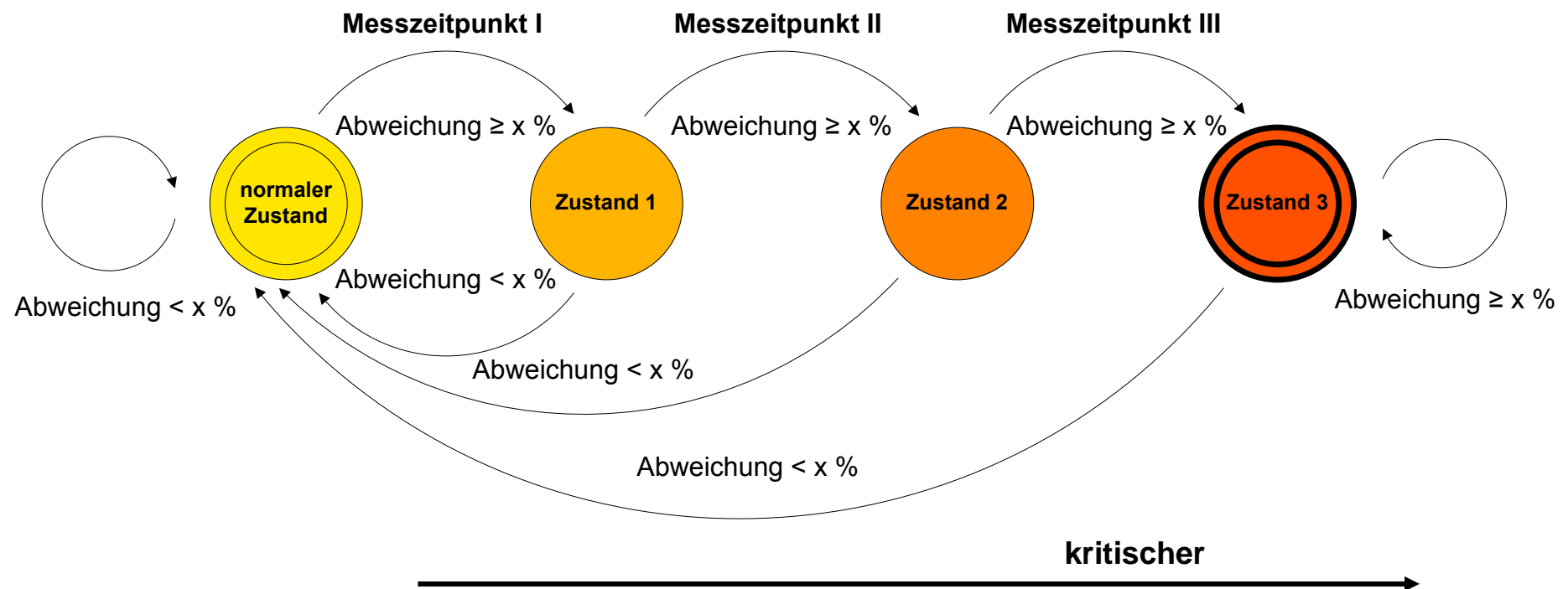
- Übersichtliche Darstellung durch Auswahl großer Kommunikationsknoten
- Anomalien, Störungen und komplexe Angriffsmuster darstellen
 - **Darstellen** bedeutender **Parameter** eines Knotens
 - Beispiel: TCP – Destination Port 25 (SMTP / für E-Mail-Kommunikation)
Ist das Datenaufkommen des E-Mail-Verkehrs im normalen Bereich?
 - **Zusammenhänge untereinander** müssen deutlich werden
- **Räumlicher** (wo) und **zeitlicher** (wann) **Kontext** müssen dargestellt werden

Konzeption einer geeigneten Visualisierung

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, folgt ein **Zustandswechsel**

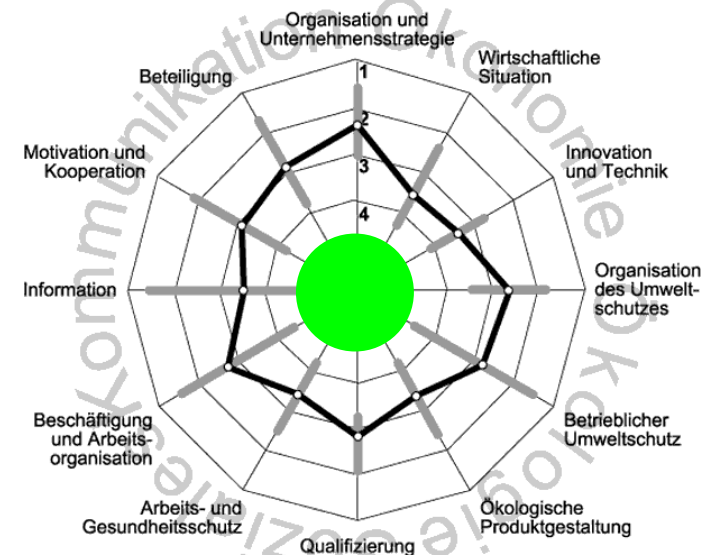


Konzeption einer geeigneten Visualisierung Darstellung eines Kommunikationsknotens

- 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)

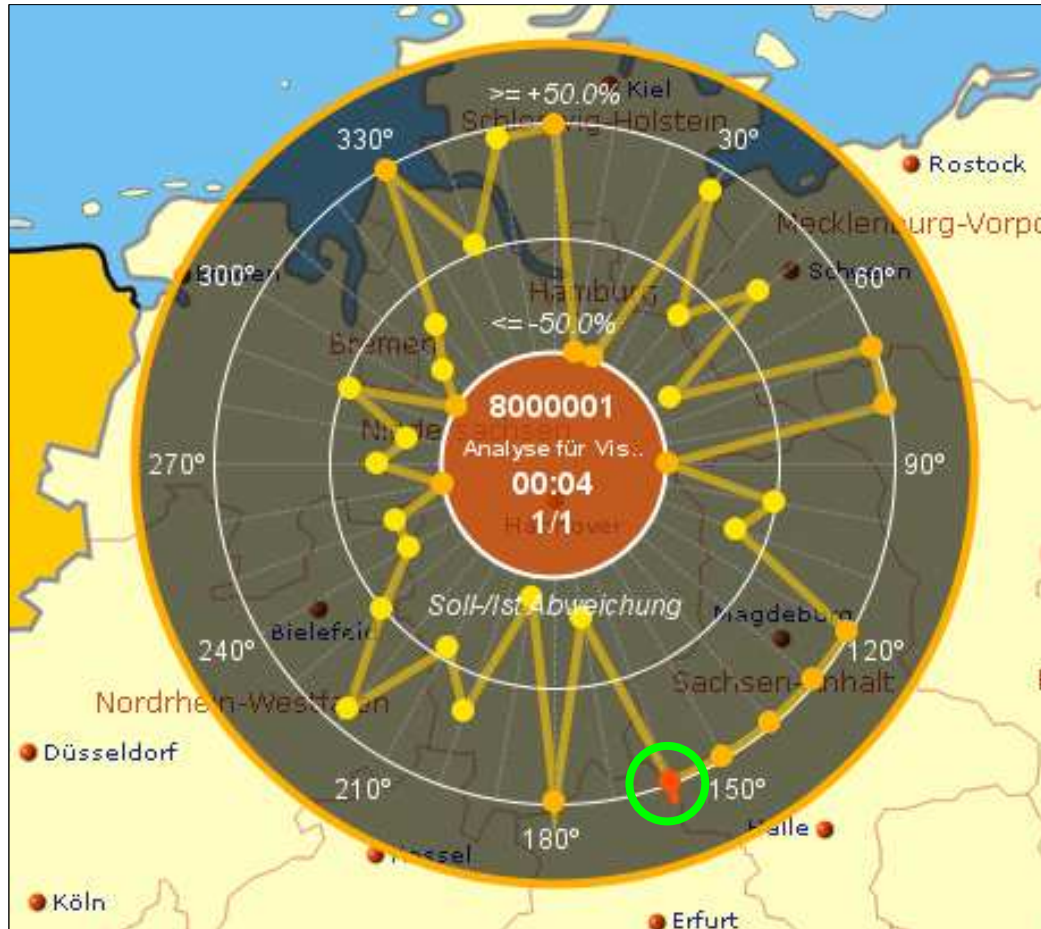
Dafür müssen **Struktur- und Wertedarstellungen kombiniert** werden

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



Ergebnisse der Visualisierung

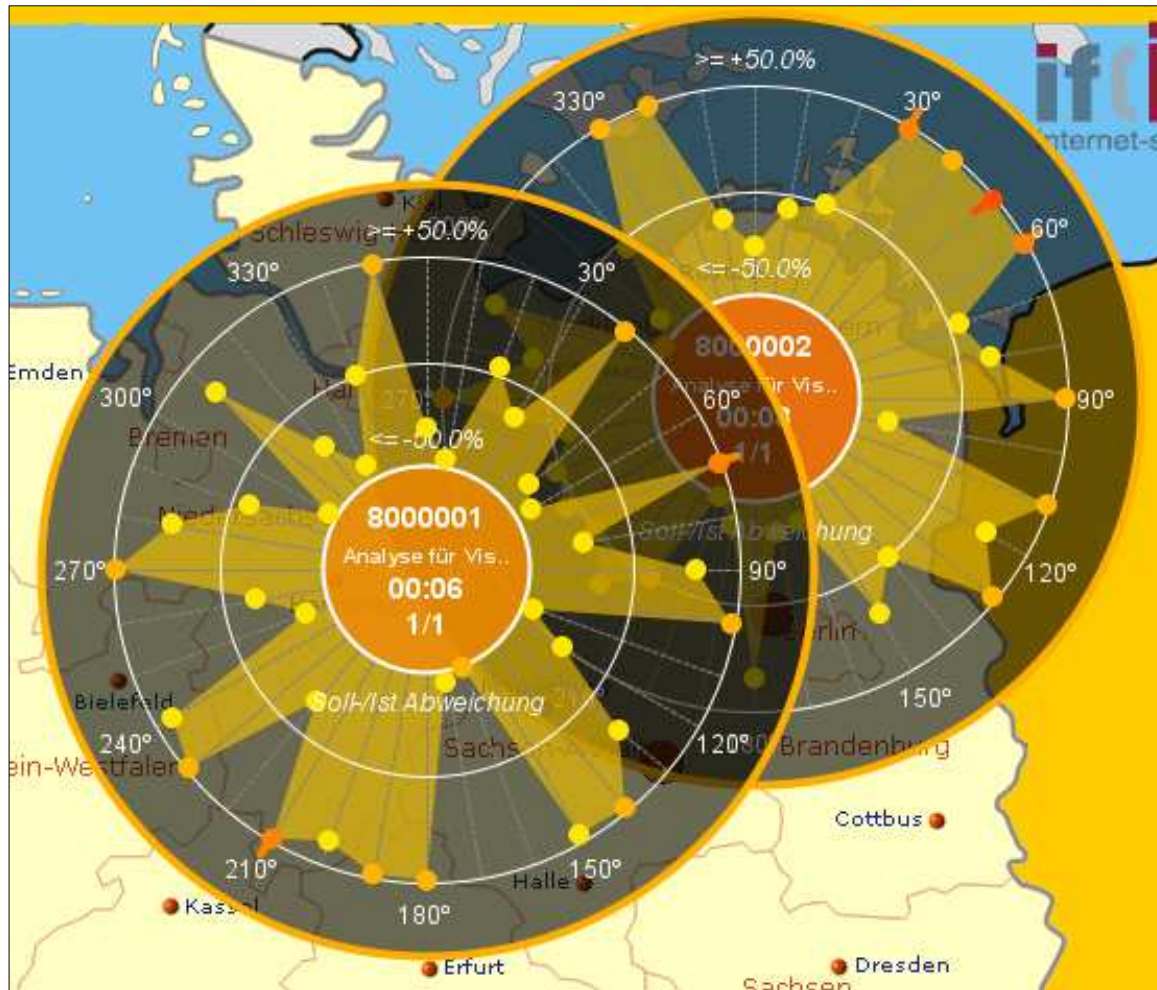
Umsetzung einer Darstellungskomponente



- 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

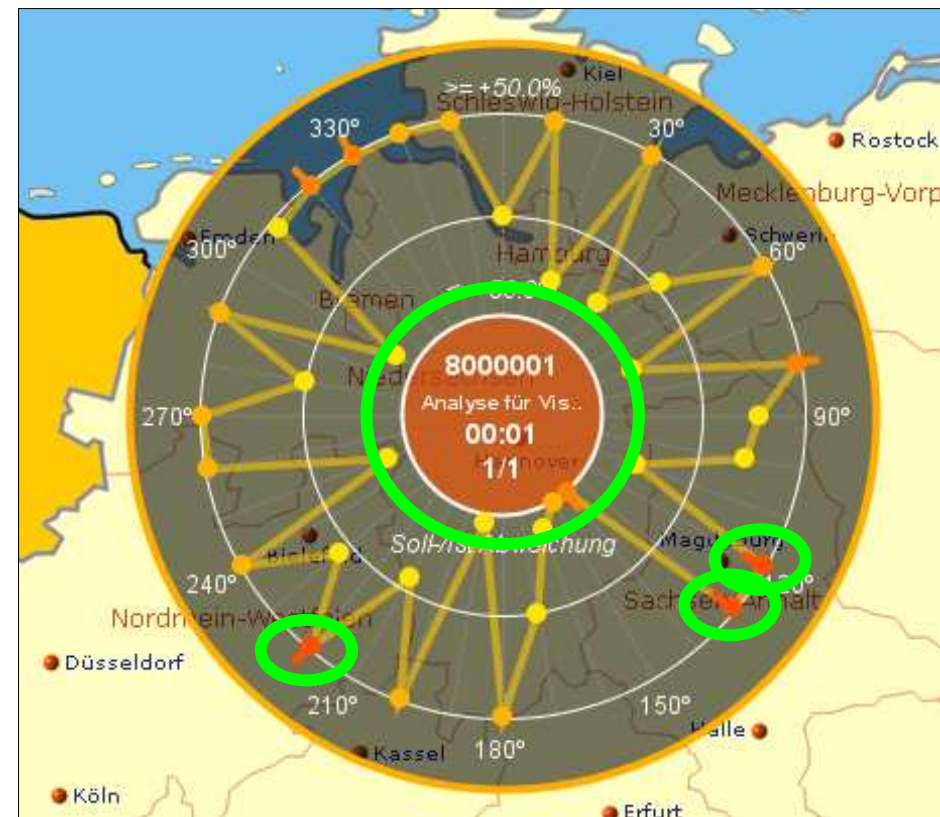
Weitere Herausforderung

- Darstellung komplexer Informationen auf möglichst kleinem Raum

Ergebnisse der Visualisierung

Aggregation von Zuständen einer Datenquelle (1/2)

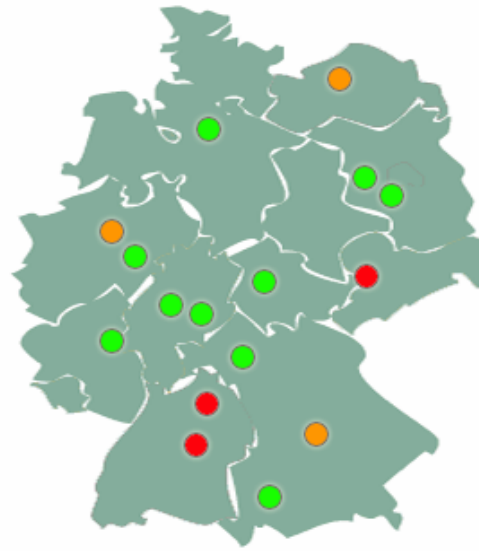
- Übersichtliche Darstellung der Zustände ermöglichen
 - Knoten möglichst auf *kleinem Raum* abbilden
 - **Zustände** der Parameter **zu einer Klasse zusammenfassen**
- Nur *ein abstrahierter Wert* stellt den Zustand eines Knotens dar
- Benutzer kann zu jedem Knoten auswählen
 - wie viele Merkmale vom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



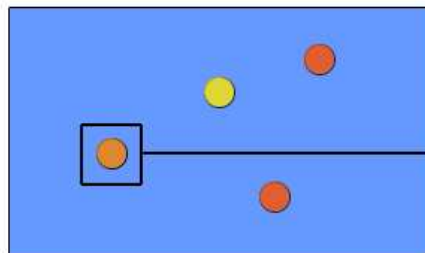
- Schneller Überblick über viele Daten
- Zustände lassen sich auf einen Blick miteinander vergleichen
- Gefahrenpotenzial lässt sich auf einen Blick erschließen

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

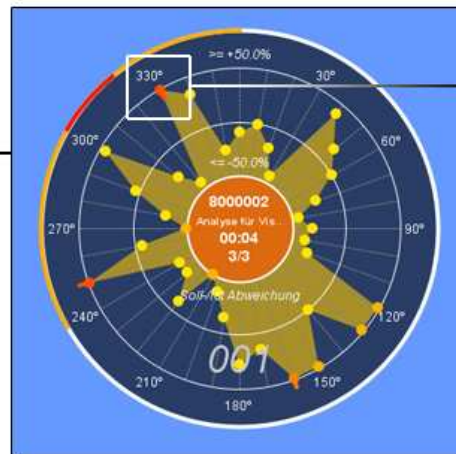
- Zustände der Parameter eines Kommunikationsknotens werden auch hier zu einem Zustand zusammengefasst

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

Durch Kombination der Darstellungen

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

Position	ID	Beschreibung	Soll/Ist-Abweichung	Status	Trend
TOP	121185	P (Product number 17)	+54,22 %	auffällig	abwiegend
TOP	81981	HTTP (Request Method HEAD)	+187,95 %	besonders auffällig	abwiegend
0°	121186	CMP (Type 0 echo reply (R))	+42,21 %	normal	stabil
15°	121187	CMP (Type 3 destination unreachable (R))	+106,84 %	normal	stabil
30°	121188	CMP (Type 4 source quench (R))	-2,81 %	normal	stabil
45°	121189	CMP (Type 12 destination port unreachable (R))	-34,87 %	normal	stabil
60°	121190	CMP (Type 8 echo request (R))	-44,84 %	normal	stabil
75°	121191	P (Product number 1)	-80,00 %	normal	stabil
90°	121192	P (Product number 2)	-88,84 %	normal	stabil
105°	491998	UDP (Destination port 55)	-43,88 %	normal	stabil
120°	491999	UDP (Destination port 141)	-49,86 %	normal	stabil
135°	524292	UCP (Registered destination port (1024-49151))	-126,33 %	normal	stabil
150°	199140	TCP (Source port 21)	-12,28 %	normal	stabil
165°	199141	TCP (Source port 20)	+121,21 %	normal	stabil
180°	199142	TCP (Source port 80)	+16,20 %	normal	stabil
195°	197183	TCP (Source port 443)	-23,28 %	normal	stabil
210°	317983	TCP (Dynamic source port (49152-65535))	-17,81 %	normal	stabil
225°	317984	TCP (Destination source port (0-65535))	+13,28 %	normal	stabil

Tabellarische Darstellung

level of detail



Ergebnisse der Visualisierung

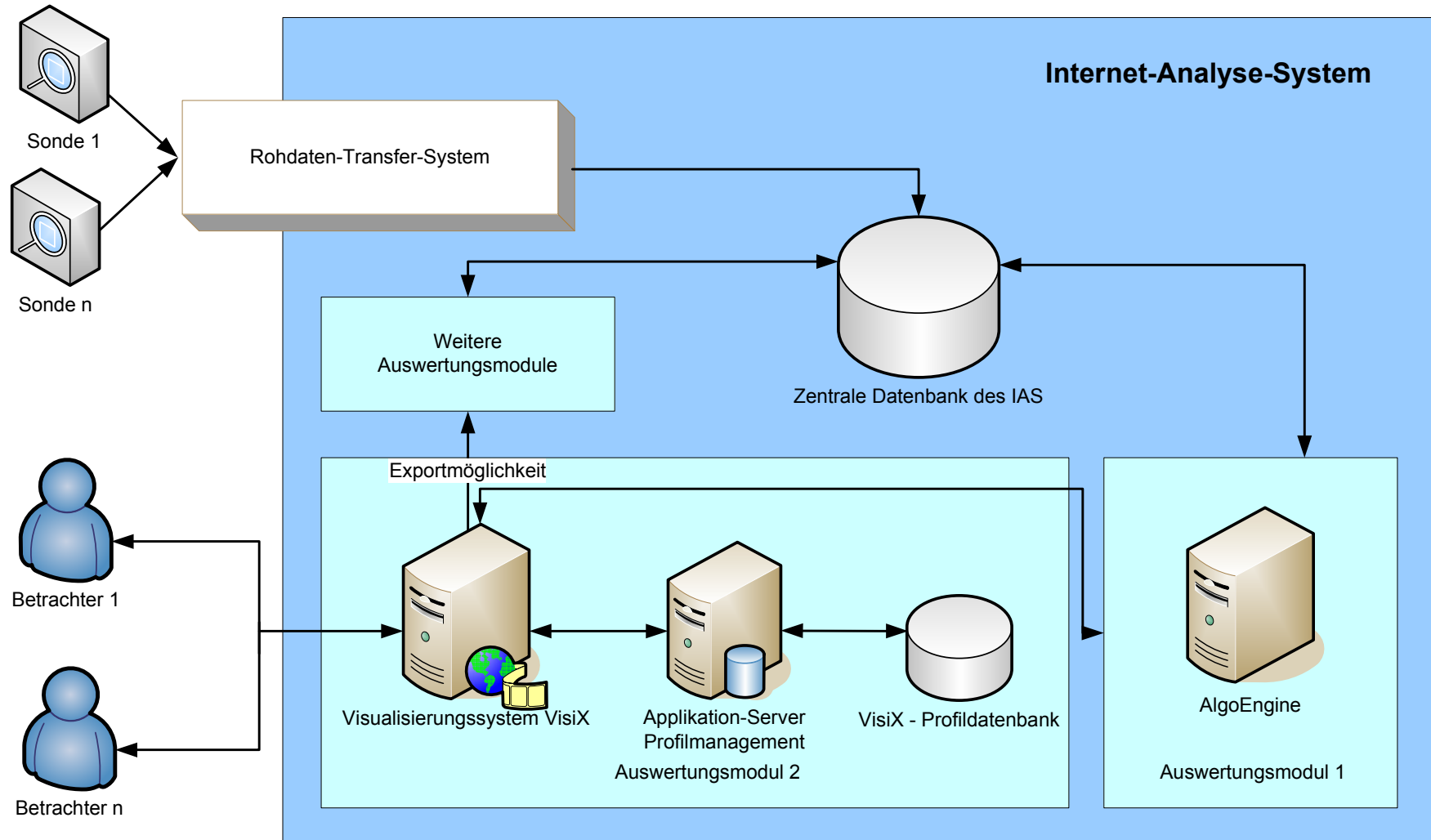
Beispiel einer DDoS-Attacke mit VisiX

- **DDoS-Attacke von unbekanntem Angreifer auf den Fachbereich Informatik der Fachhochschule Gelsenkirchen**
- 10 Minuten später
- Hohe Auslastung von ICMP Echo Reque. und TCP SYN Paketen reduzieren gesamten Netzwerkverkehr
- **Anomalien bei weiteren Diensten**
- DNS(130°) und SMTP(230°) können Ihre Arbeit nicht mehr im normalen Maße verrichten
- Wechseln Ihren Zustand



Abbildung 3

Ergebnisse zur technischen Umsetzung Topologischer Zusammenhang



Fazit (1/2)

- Bei Auswahl bedeutender Kommunikationsknoten:
Visualisierung vom **Zustand großer Netzwerke**
- **Auswirkungen von Anomalien können mit VisiX beobachtet werden**
- Anomalien können durch Soll-/Ist-Analysen verschiedener Kommunikationsknoten schnell miteinander verglichen werden:
Problem von lokaler oder regionaler/globaler Bedeutung?!
- **Komplexe Zusammenhänge können** zu einem Messzeitpunkt und über mehrere Messzeitpunkte hinweg **veranschaulicht werden**
- **Details on Demand**
- Schnittstelle für Datenexport bietet Möglichkeit für weiterführende Analysen

Fazit (2/2)

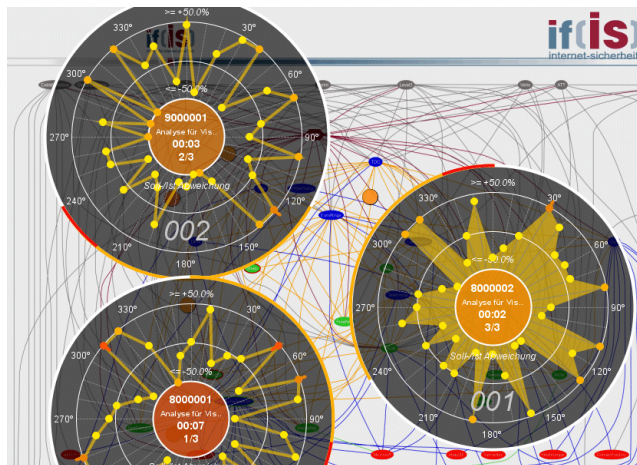
- **Flexible Architektur** ermöglicht **Integration in andere Anwendungsbereiche**
- Anbindung neuer Informationsquellen ohne Programmieraufwand möglich
 - anpassungsbedürftige Parameter lassen sich unabhängig vom Quellcode über deklarative Stellschrauben modifizieren
- **Zentrales Profil-Management**
 - Einstellungen müssen nicht bei jedem Programmstart neu konfiguriert werden
 - schneller Wechsel zwischen verschiedenen Anwendungsfällen jederzeit möglich

Praxistauglichkeit

- Prognosewerte müssen für Soll-/Ist- Abweichungen in angemessener Qualität vorliegen → unbrauchbare Abweichungen → unbrauchbaren Zuständen
- Liegen konkrete Soll-Werte vor (zum Beispiel: Ozonwerte), kann das Visualisierungssystem sofort verwendet werden

Verfügbarkeit und Notfallplanung mit Hilfe der Visualisierung

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?



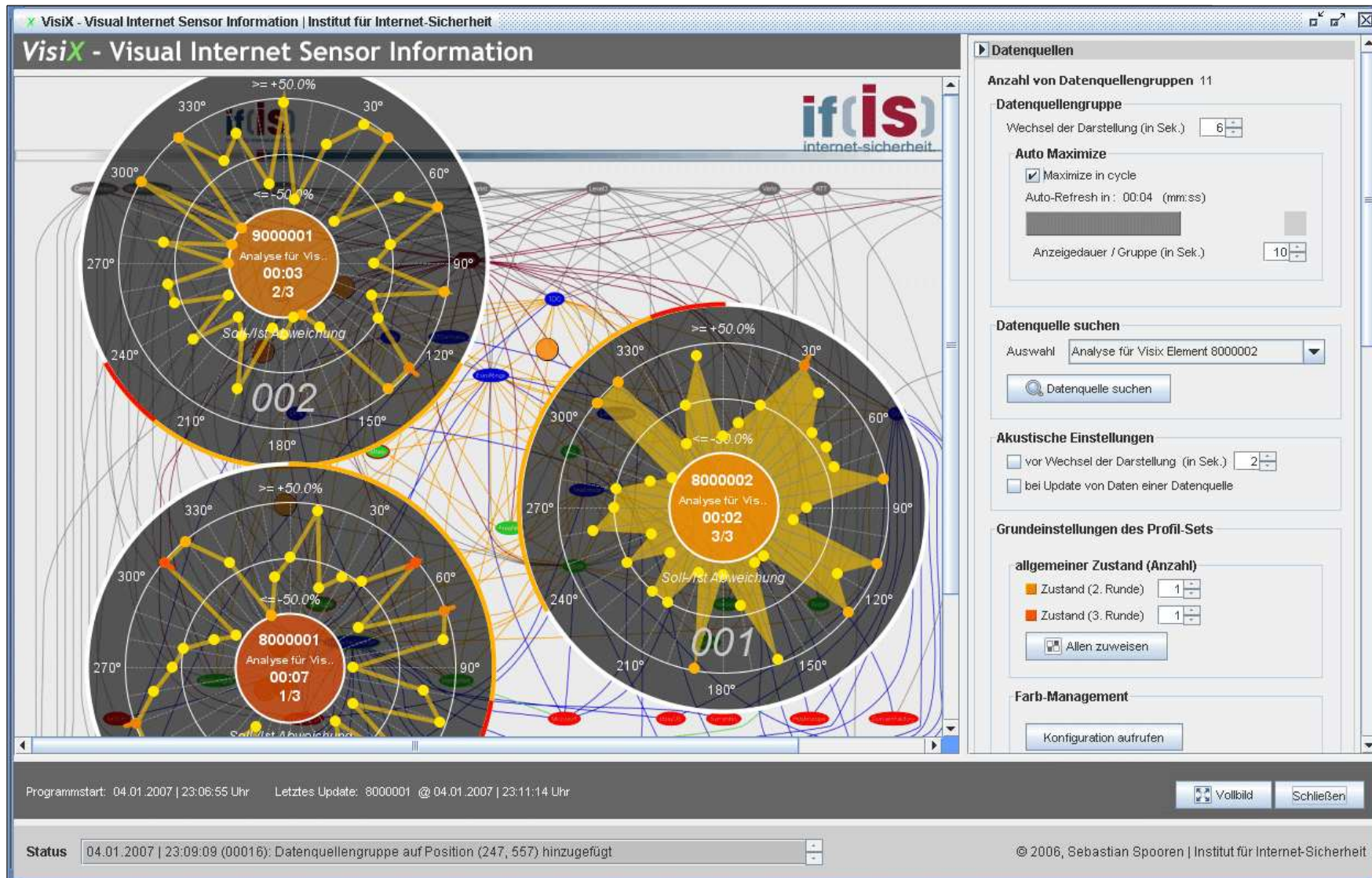
Sebastian Spooren
spooren (at) internet-sicherheit.de

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

if(is)
internet-sicherheit.

 Fachhochschule
Gelsenkirchen

Ergebnisse der Visualisierung Benutzerschnittstelle



Ergebnisse der Visualisierung

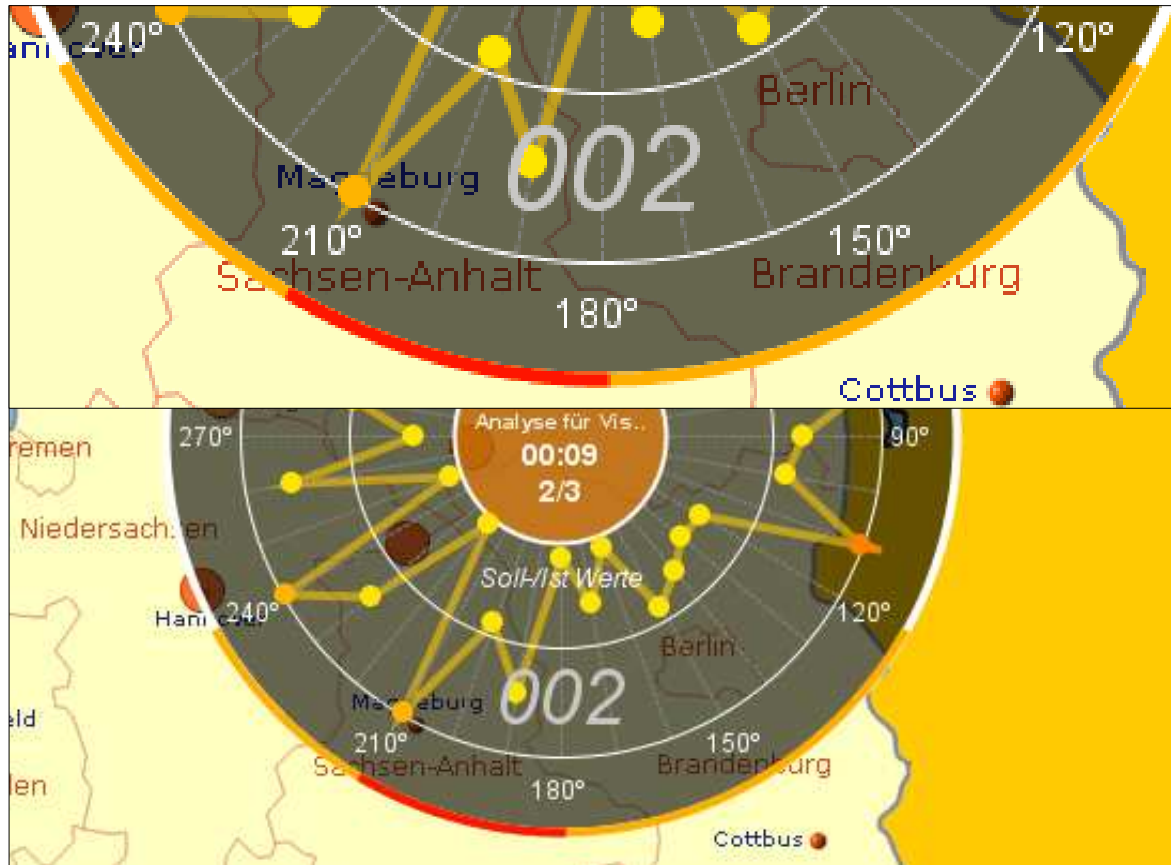
Mehrere Knoten auf gleichen Koordinaten (1/3)

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

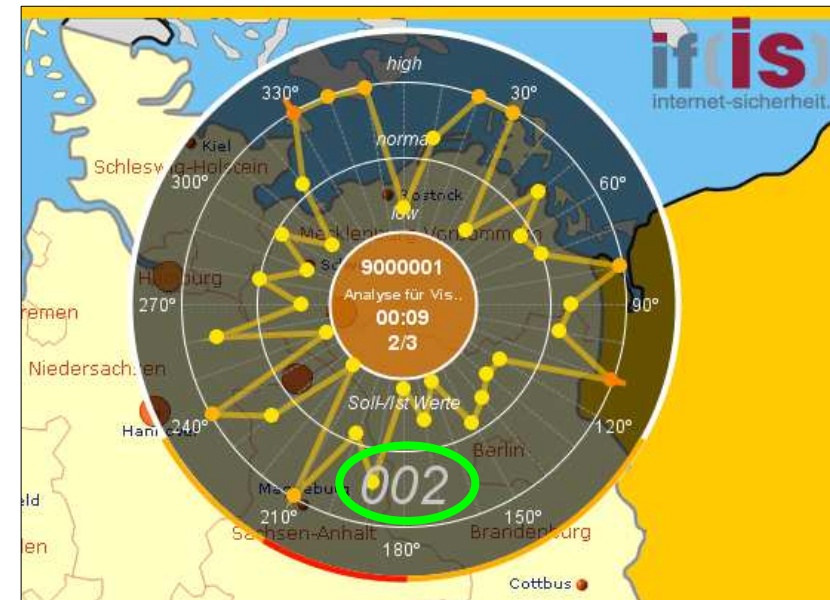
- *Alle* Datenquellen der Gruppe erhalten nahezu zeitgleich kritischen Zustand!

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	wechsell & halten	anzeigen
9000001	Analyse für Visix Element 9000001	auffällig	wechsell & halten	anzeigen
8000002	Analyse für Visix Element 8000002	normal	wechsell & halten	anzeigen

Schließen