

Visualisierung komplexer Sicherheitssituationen in einem Netzwerk

Sebastian Spooren

Sebastian Spooren
spooren@internet-sicherheit.de

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



- Einführung in das Thema Visualisierung
- Ausgangssituation
- Konzeption eines Visualisierungssystems
 - Anforderungen
 - Entwurf einer geeigneten Visualisierung
- Ergebnisse der Visualisierung
- Ergebnisse der technischen Umsetzung
- Fazit

Einführung in das Thema Visualisierung

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

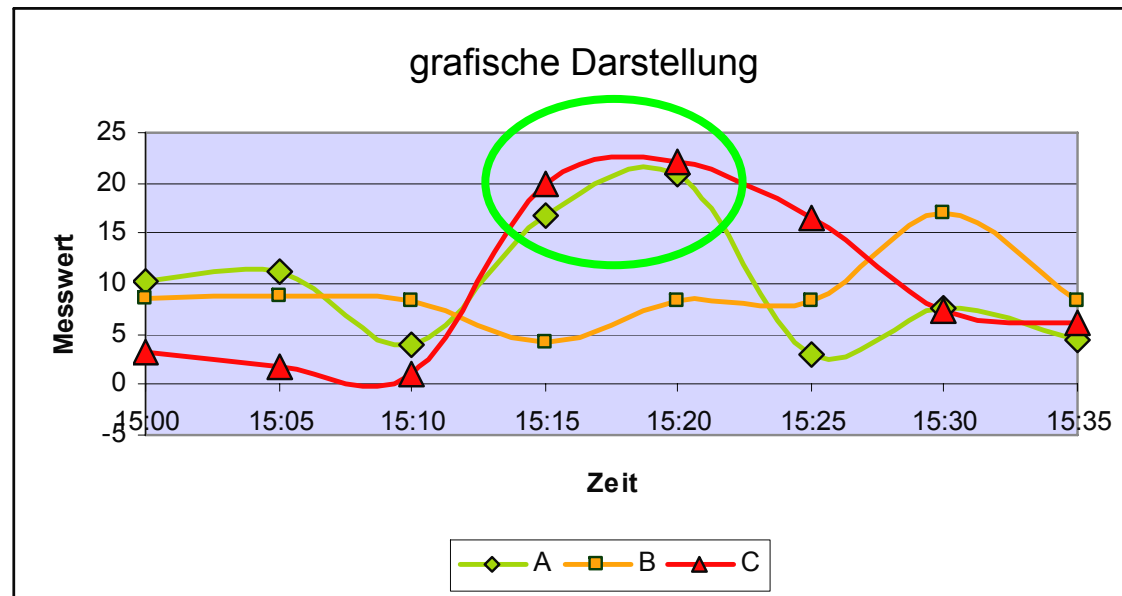
Einführung in das Thema Visualisierung

Vorteile der Visualisierung an einem Beispiel

- 3 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

- große Netzwerke mit zahlreichen Kommunikationsknoten
 - Zugang zu relevanten Daten, einerseits von zugrunde liegenden Kommunikationsparametern aber auch den Kommunikationsknoten, aufgrund der Fülle an Informationen meist ziemlich schwierig
- Präventivmaßnahmen müssen geschaffen werden
 - Gefahren und Risiken rechtzeitig erkennen
 - Schäden reduzieren
- Um wichtige Veränderungen (Störungen, Angriffe, ...) in Netzwerken auf einen Blick erkennen zu können, besteht großes Interesse bei
 - Netzmanagement- und Sicherheitszentren
- **Dringliche Entscheidungen auf dem Gebiet der IT-Sicherheit müssen *einfacher, schneller und effizienter* als bisher getroffen werden**

Konzeption einer geeigneten Visualisierung

Anforderungen an die Visualisierung

Entwicklung eines Visualisierungssystems zur Darstellung vom aktuellen Zustand des Internets

→ Prävention von komplexen Sicherheitssituationen in einem Netzwerk

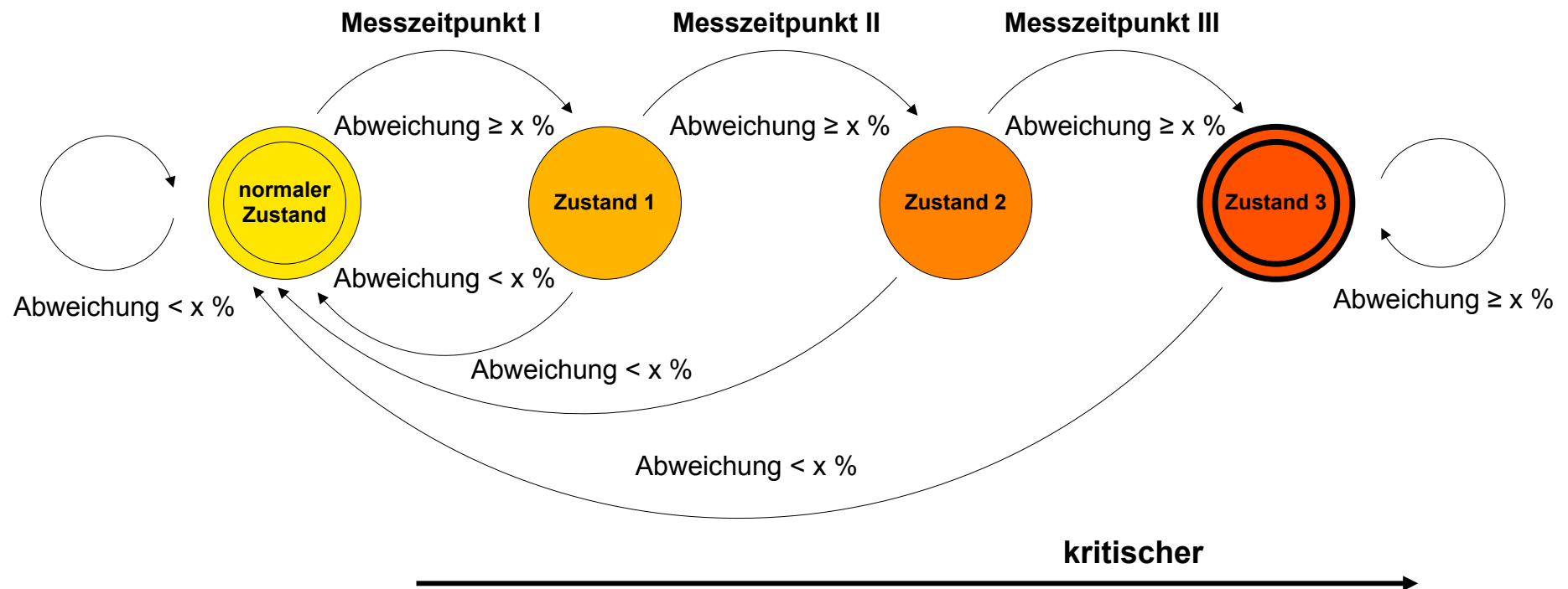
- Darstellung aktueller Zustände von Parametern eines Kommunikationsknotens
 - Beispiel: TCP – Destination Port 25 (SMTP / für E-Mail-Kommunikation)
 - Ist das Datenaufkommen des E-Mail-Verkehrs im normalen Bereich?
 - Anzahl darzustellender Parameter *pro Datenquelle* zunächst auf 36 beschränkt
- Übersichtliche Darstellung aktueller Zustände
- Schwerpunkt
 - Entwicklung einer grafischen Darstellungskomponente als Repräsentant eines Kommunikationsknotens

Konzeption einer geeigneten Visualisierung

Entwicklung eines Zustandsmodells

Um Zustände zu generieren, folgende Überlegungen ...

- Jedem Kommunikationsparameter soll ein Soll-/Ist- Wert (Prognose-/Mess- Wert) zugrunde liegen, um einen *Zustand* generieren zu können
- weicht Ist- gegenüber Sollwert, um $x\%$ ($x = \text{Grenzwert}$) ab
→ Zustandswechsel



Konzeption einer geeigneten Visualisierung

Erste Überlegungen an eine Visualisierung...

- Bezugssystem entwerfen, um Zustände und auch Werte der 36 Soll-/Ist- Abweichungen für jeweils eine Datenquelle abbilden zu können
 - Zusammenhänge untereinander müssen deutlich werden
- Zweites Bezugssystem ist zu berücksichtigen
 - Jede Datenquelle erfasst ihre Daten an unterschiedlichen Orten und zu verschiedenen Zeitpunkten
 - Es muss ein räumlicher und zeitlicher Bezug beachtet werden

Konzeption einer geeigneten Visualisierung

Entwurf einer Darstellungskomponente (1/2)

- Herausforderung besteht bei der Verknüpfung beider Bezugssysteme
 - Es müssen bei der Abbildung folgende Faktoren zugleich berücksichtigt werden
 - Übersichtliche Darstellung (Ort der Messdatenerhebung)
 - Aktuelle Darstellung (Zeitpunkt der Messdatenerhebung)
 - 36 verschiedene Soll-/Ist- Abweichungen mit ihren Werten und Zuständen
 - Dafür müssen Struktur- und Wertedarstellungen kombiniert werden
 - Als Basisform wird ein Netzdiagramm verwendet

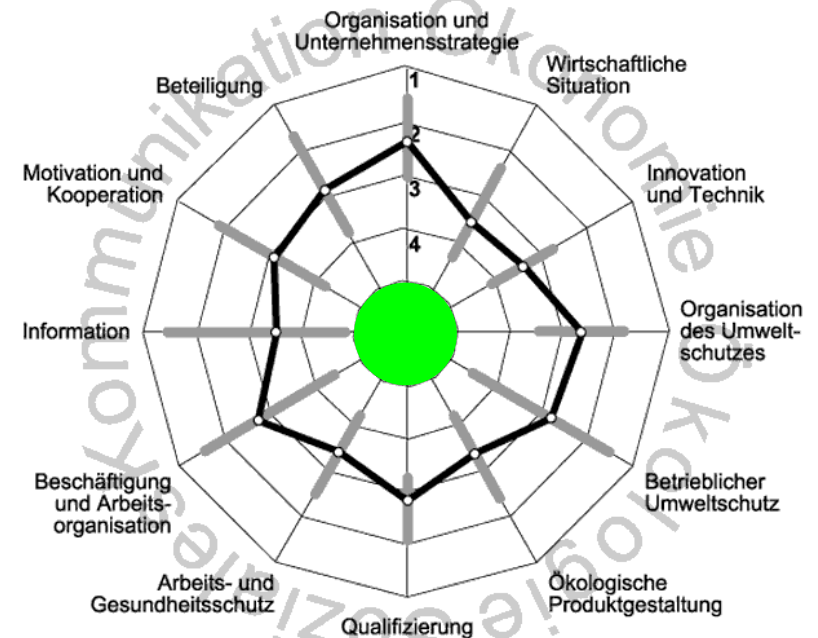
Konzeption einer geeigneten Visualisierung

Entwurf einer Darstellungskomponente (2/2)

- Merkmalsraum wird über alle Achsen verteilt abgebildet
- Netzdiagrammtechnik erlaubt auch Abbildung von 36 Soll-/Ist- Abweichungen

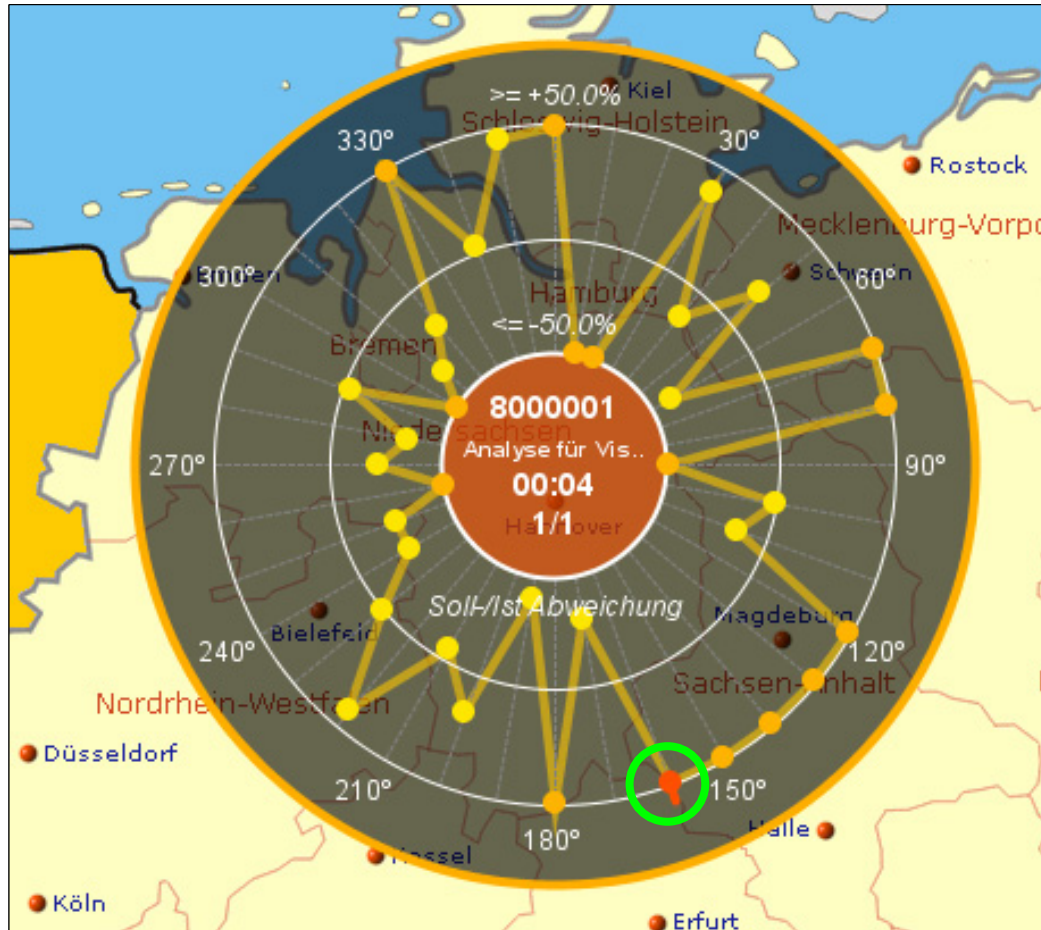
- Des Weiteren lässt sich der Raumbezug zu einer Visualisierungsgrundlage herstellen

- Zentrum der Diagrammform könnte Gebiet der Messdatenerhebung symbolisieren
- wenn Diagramm transparent dargestellt wird → Verknüpfung beider Bezugssysteme
- Zeit benötigt keine eigene Dimension bei der Abbildung!
 - Zustand wird nicht kontinuierlich, sondern diskret zu bestimmten Messzeitpunkten generiert



Ergebnisse der Visualisierung

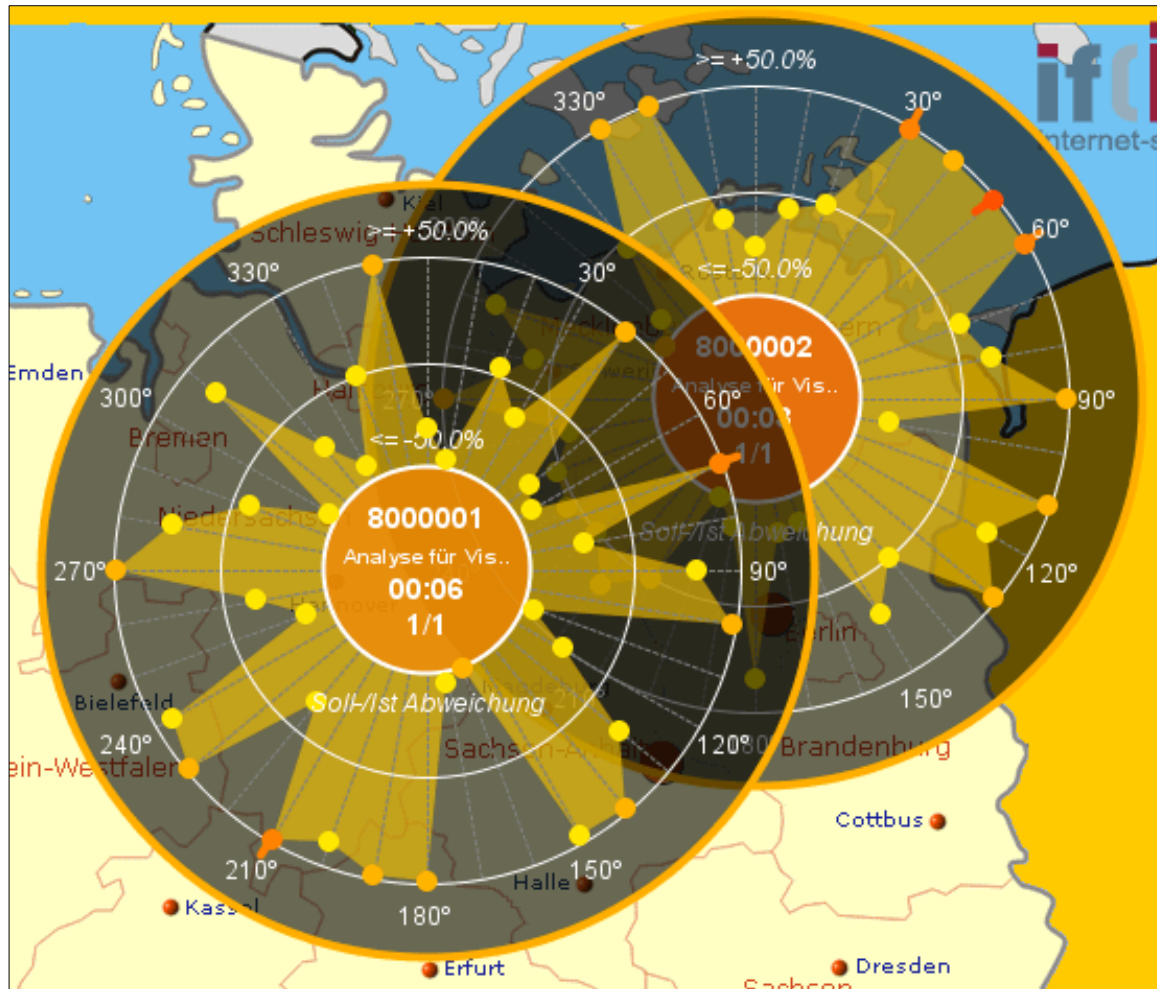
Umsetzung einer Darstellungskomponente



- Benutzer bestimmt Position
- Abgrenzung der Merkmale
- Ausprägung einer Abweichung wird über Radiusposition abgebildet
- Zustände werden über die Farbe dargestellt
- Trenddarstellung
- Identifikation einer Quelle
- *geschätzte* Zeit bis Datenupdate
- Erkennen von Zusammenhängen
- Elemente werden gruppiert dargestellt

Problem: Darstellung von mehreren Datenquellen in unmittelbarer Nähe

Ergebnisse der Visualisierung Überschneidung der Darstellungskomponenten



- Überschneidung zweier Datenquellen bei der Darstellung ihrer Merkmale

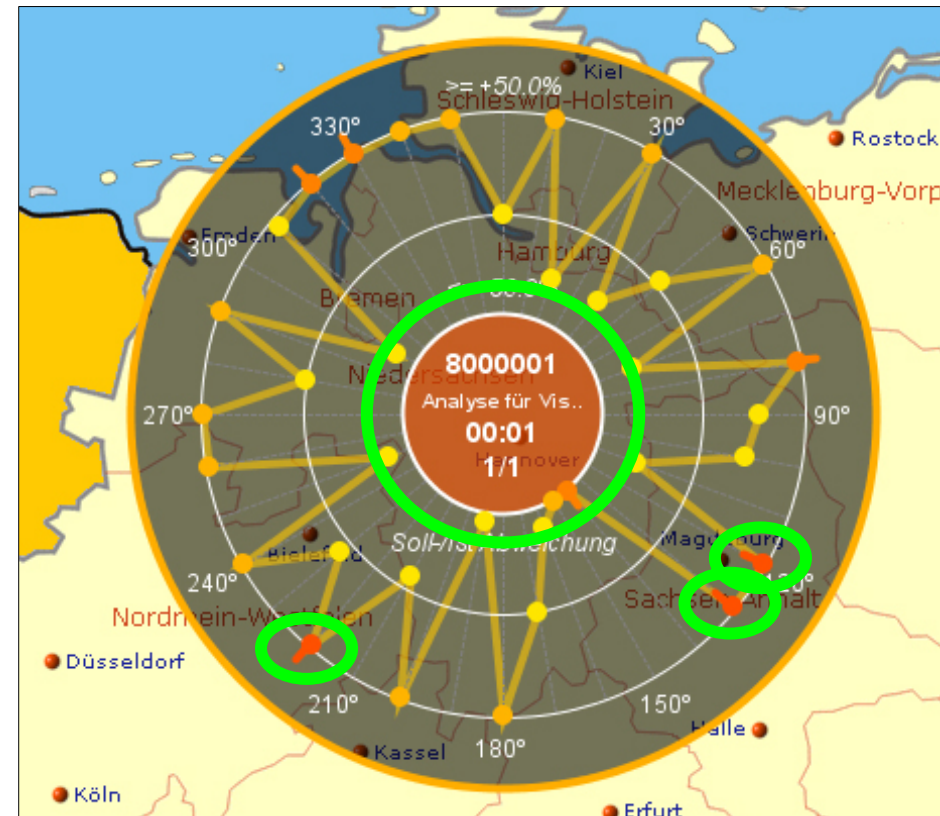
Weitere Herausforderung

- Darstellung komplexer Informationen auf möglichst kleinem Raum

Ergebnisse der Visualisierung

Aggregation von Zuständen einer Datenquelle (1/2)

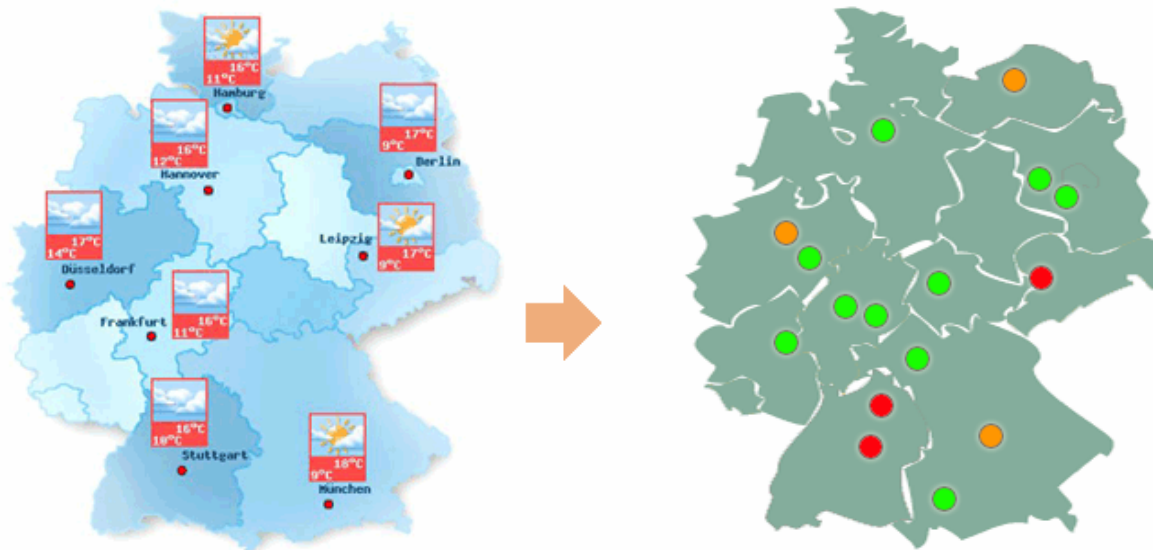
- Ziel der Arbeit ist auch die *übersichtliche Darstellung von Zuständen*
 - Daher alternative Möglichkeit die Zustände der Merkmale durch Zusammenfassen zu einer Klasse auf möglichst *kleinem Raum* abzubilden
- Nur *ein abstrahierter Wert* repräsentiert den Zustand für alle zugrunde liegenden Parameter einer Datenquelle
- Benutzer kann zu jeder Datenquelle 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

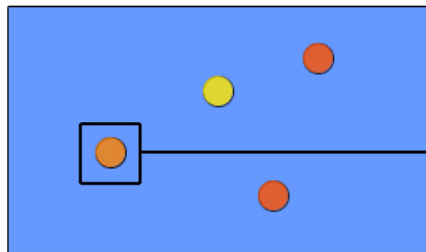
- *Kombination* beider Darstellungen ermöglicht
 - Überblick über möglichst viele Zustände
 - Sicht auf Details und Zusammenhänge

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

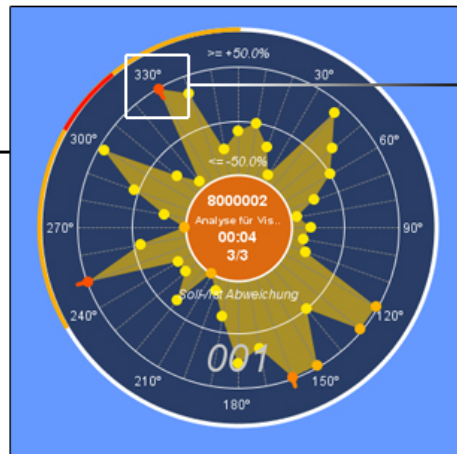
- Zustände der Parameter eines Kommunikationsknotens werden auch hier zu einem Zustand zusammengefasst

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

Messwert-Übersicht

Analyse Beschreibung: Analyse für Visix Element 8000002
Messzeitraum: 11.12.2008 08:58:08 bis 11.12.2008 02:00:00

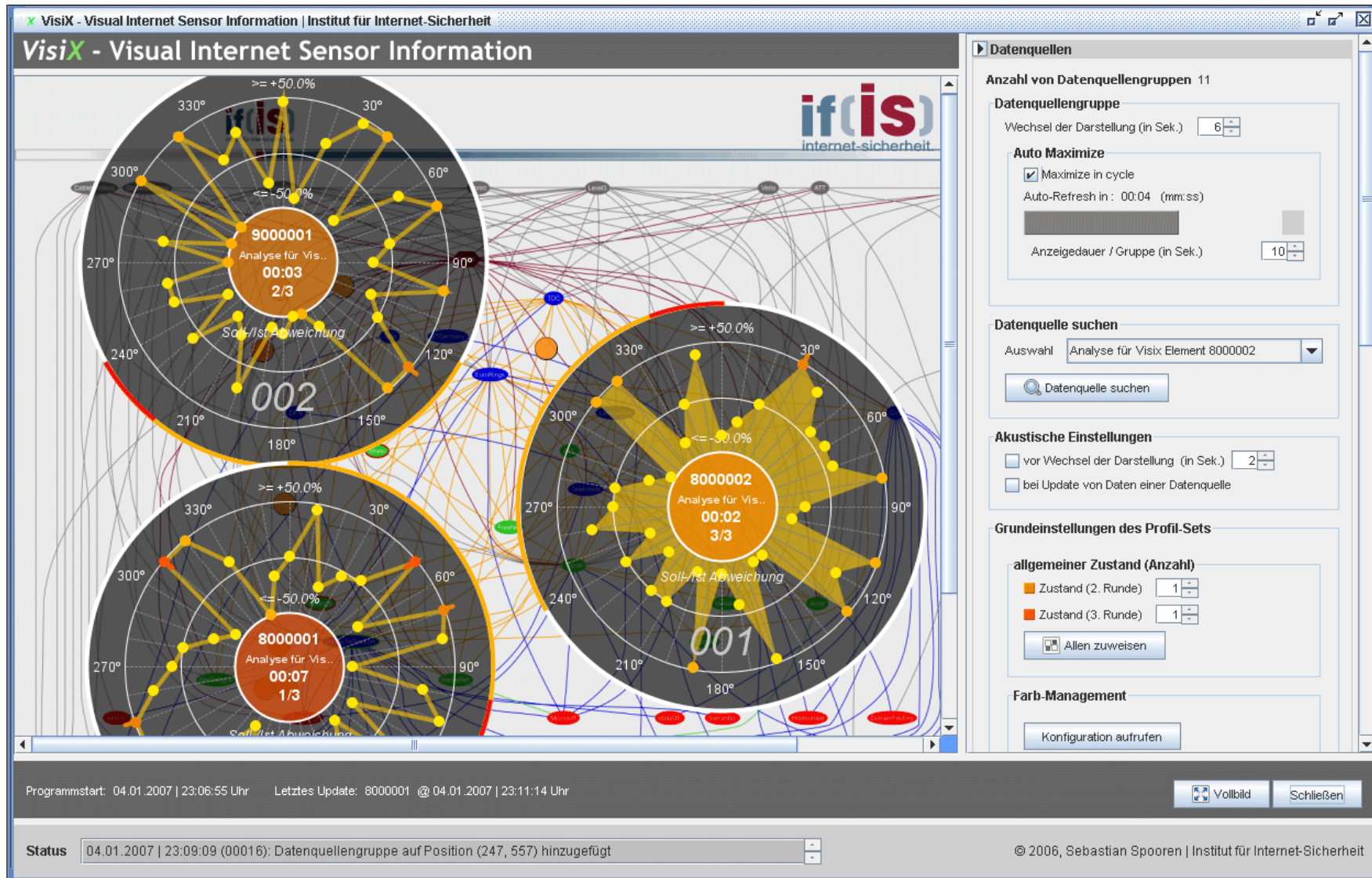
Position	ID	Beschreibung	Soll/Ist-Abweichung	Status	Trend
70°	131145	P (Protocol number 17)	+54,32 %	auffällig	steigend
350°	543983	HTTP (Request Method HEAD)	+181,85 %	besonders auffällig	steigend
0°	131416	CMP (Type 8 echo reply (R: 792))	+43,33 %	normal	konstant
130°	131418	CMP (Type 3 destination unreachable (R: 792, 3:498))	+80,45 %	normal	konstant
210°	131420	CMP (Type 4 source quench (R: 792))	-20,61 %	normal	konstant
30°	131426	CMP (Type 12 parameter problem (R: 792))	-24,47 %	normal	konstant
40°	131424	CMP (Type 8 echo request (R: 792))	-44,54 %	normal	konstant
60°	131128	P (Protocol number 1)	-30,80 %	normal	konstant
60°	131134	P (Protocol number 6)	-38,64 %	normal	konstant
90°	493905	UCP (Destination port 53)	+23,90 %	normal	konstant
90°	493913	UCP (Destination port 161)	+14,85 %	normal	konstant
100°	524292	UCP (Registered destination port (1024-49151))	+126,33 %	normal	konstant
110°	198930	TCP (Source port 23)	-12,26 %	normal	konstant
120°	198933	TCP (Source port 25)	+317,21 %	normal	konstant
130°	198988	TCP (Source port 80)	+38,00 %	normal	konstant
140°	197051	TCP (Source port 443)	-23,38 %	normal	konstant
150°	327882	TCP (Dynamic source port (49152-49151))	+27,85 %	normal	konstant
180°	327888	TCP (Wellknown source port (1023))	+13,38 %	normal	konstant

Tabellarische Darstellung

level of detail



Ergebnisse der Visualisierung Benutzerschnittstelle



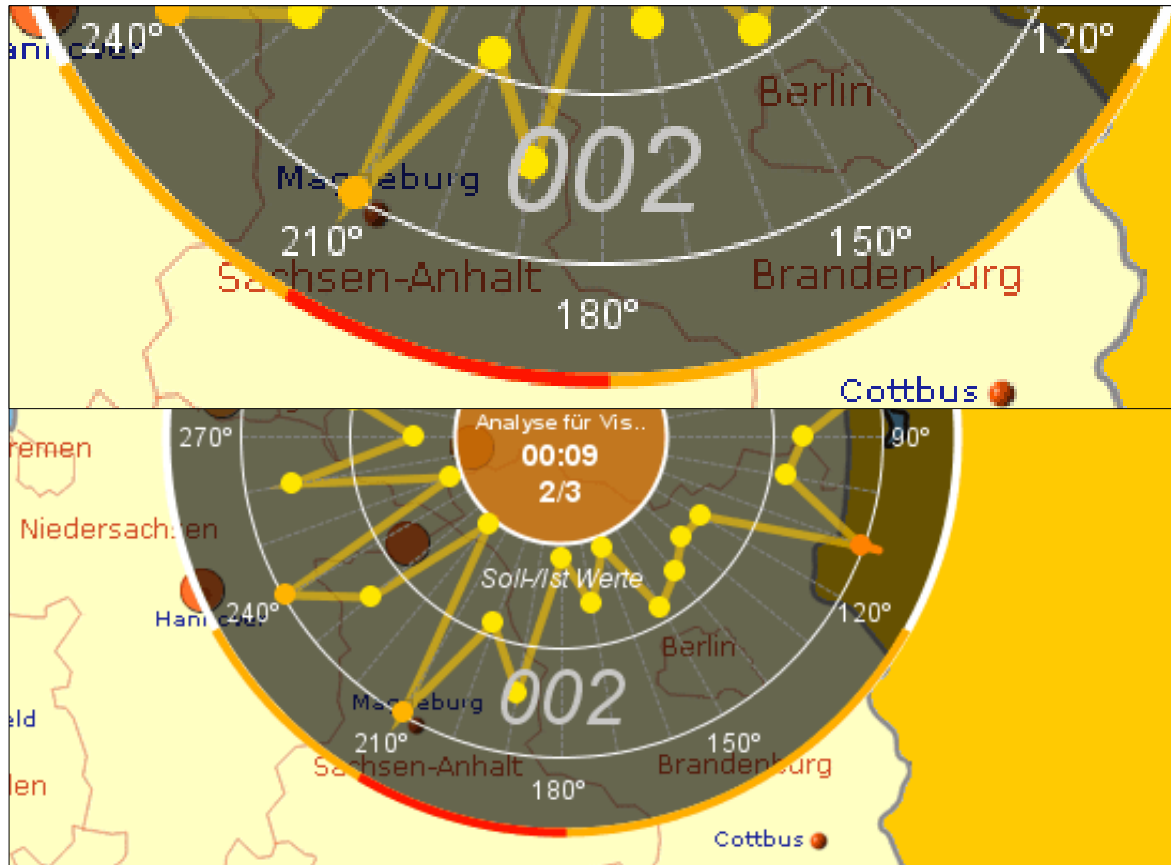
Ergebnisse der Visualisierung

Datenquellengruppe (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 Datenquellengruppe (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

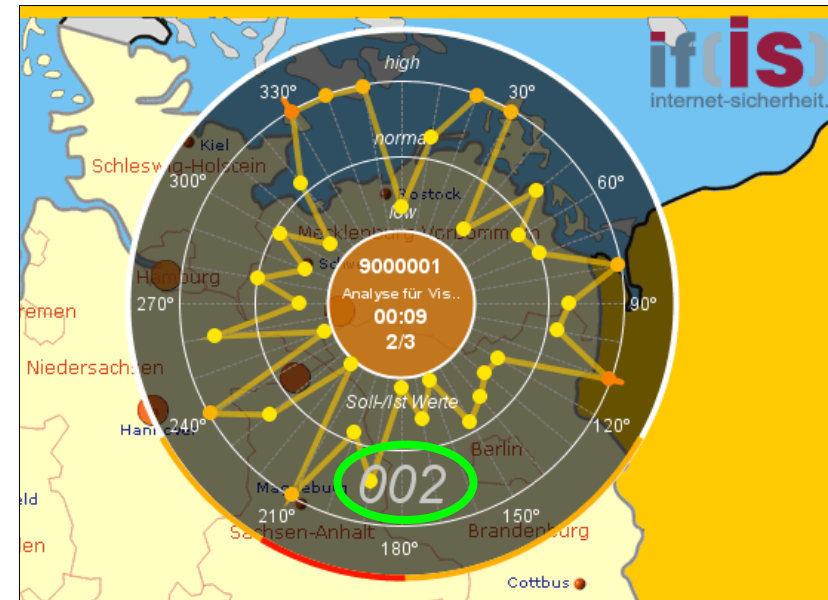
Noch problematischer

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

Ergebnisse der Visualisierung Datenquellengruppe (3/3)

Lösung des Problems

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



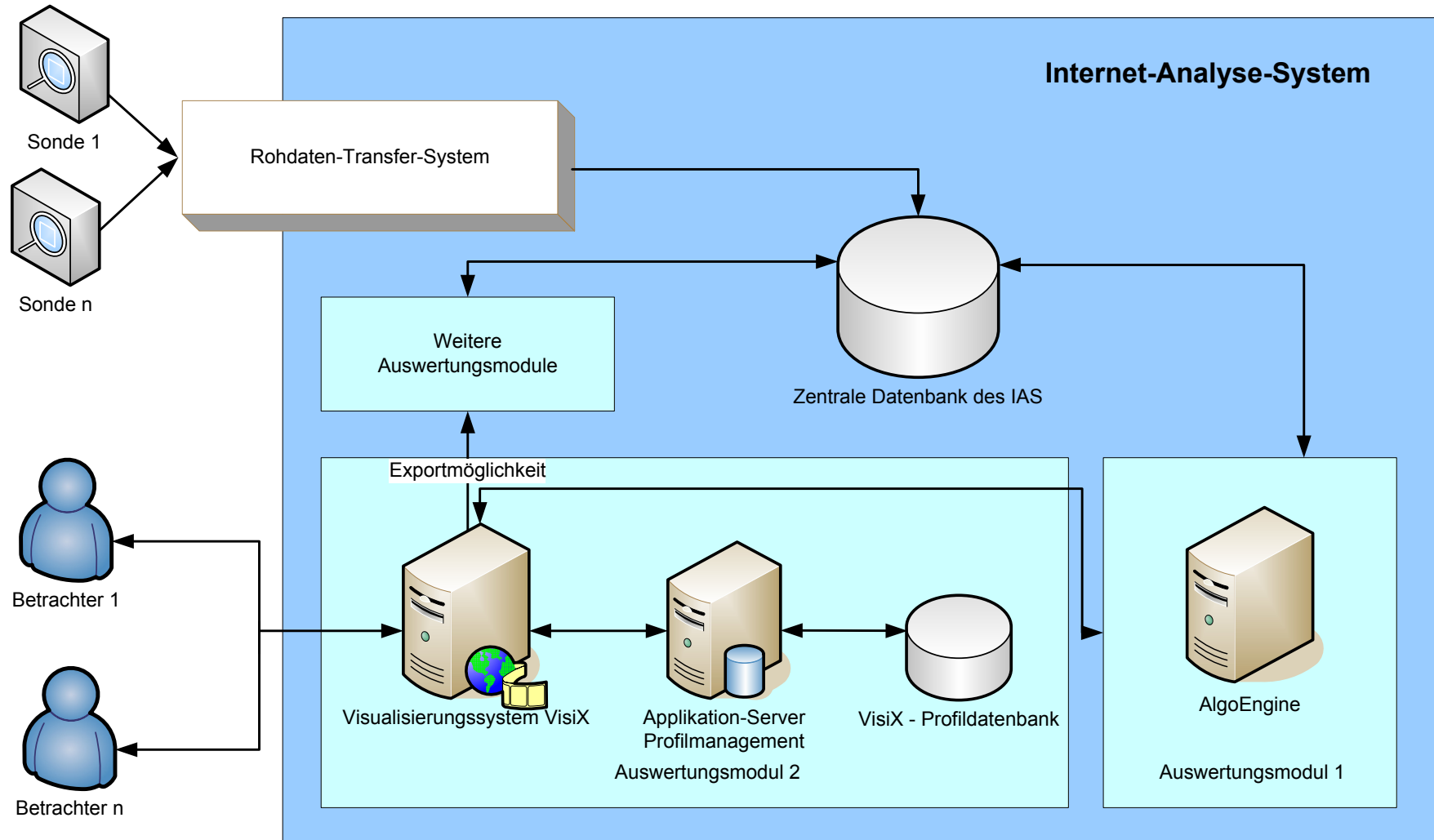
Aufschlüsselung der Datenquellengruppe

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)

- Das Visualisierungssystem kann helfen, komplexe Zusammenhänge zu einem Messzeitpunkt und über mehrere Messzeitpunkte hinweg zu verstehen
- Schnittstelle für Datenexport bietet Möglichkeit für weiterführende Analysen
- Aufgrund der flexiblen Architektur lässt sich das Visualisierungssystem nicht wie viele andere Systeme, nur für einen speziellen Anwendungsbereich einsetzen
- Die Anbindung neuer Informationsquellen ist im Idealfall 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
- Prognosewerte (für Soll-/Ist- Abweichungen) müssen mithilfe mathematischer Modelle (bspw. auf Basis neuronaler Netze) in angemessener Qualität vorliegen, um das Visualisierungssystem praxistauglich zu machen
 - → unbrauchbare Soll-/Ist- Abweichungen → unbrauchbaren Zuständen
- Liegen hingegen konkrete Soll-Werte vor (zum Beispiel: Ozonwerte), kann das Visualisierungssystem sofort verwendet werden

Visualisierung komplexer Sicherheitssituationen in einem Netzwerk

Sebastian Spooren
spooren@internet-sicherheit.de

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

