Verfügbarkeit und Notfallplanung mit Hilfe der Visualisierung

Dipl.-Inform.(FH) Sebastian Spooren
Prof. Dr. Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)

Fachhochschule Gelsenkirchen

[spooren | pohlmann @ internet-sicherheit.de]

Zusammenfassung

Damit im Bereich der IT-Sicherheit dringliche Entscheidungen einfacher und schneller als bisher getroffen und komplexe Sachverhalte gegenüber Dritten verdeutlicht werden können, wurde am Institut für Internet-Sicherheit ein Visualisierungssystem entwickelt. Dabei wurde das System am Institut in das für den BSI entwickelte und im Einsatz befindliche *Internet-Frühwarnsystem* integriert.

Das Abbilden von Zuständen ausgesuchter Dienste und Kommunikationsknoten steht im Mittelpunkt dieser Arbeit, um die Verfügbarkeit und Störung einzelner Dienste und ganzer Knoten in einem Netzwerk zu veranschaulichen. Um trotz des immensen Datenverkehrsaufkommens bei großen Netzwerken eine übersichtliche Abbildung zu ermöglichen, werden im Vorfeld nur besonders relevante Kommunikationsknoten ausgewählt und unter Beachtung der Anonymität analysiert. Sie liefern dem Visualisierungssystem den notwendigen Input. Dabei werden für jeden Knoten eine Vielzahl von Soll-/Ist-Abweichungen berechnet, die zusammen die Grundlage für die Bewertung seines Zustandes bilden. Dieser wird, je nach Ausprägung der zugrunde liegenden Abweichungen, über verschiedene Farben visualisiert. Mit Hilfe des Visualisierungssystems kann der Benutzer jedoch nicht nur zusammengefasste Zustände der Kommunikationsknoten darstellen, sondern hat zusätzlich die Möglichkeit einzelne Soll-/Ist-Werte innerhalb eines Knotens zu überwachen und über Trendanzeigen den Verlauf von Abweichungen zu erkennen. Damit kann das Visualisierungssystem einerseits eingesetzt werden, um Details in individuell ausgewählten Parametern zu erkennen und andererseits um schnell und einfach einen Gesamtüberblick über den Zustand von großen Netzwerken zu bekommen.

Der Schwerpunkt dieser Arbeit ist die *technisch-wissenschaftliche Visualisierung* von Kommunikationsknoten in großen Netzwerken. Dies ist gerade für Netzmanagement- und Sicherheitszentren von großem Interesse, um stets die Verfügbarkeit von laufenden Systemen im Blickfeld zu haben und andererseits um bei Notfällen in der IT über eine Entscheidungshilfe zu verfügen.

1 Motivation

Seit dem 11. September 2001 ist in vielen Bereichen die Nachfrage nach Sicherheit so groß wie nie zuvor. Weltweit besteht immer öfter das Interesse Frühwarnsysteme zu schaffen, da-

mit Gefahren und Risiken noch schneller erkannt und bevorstehende Schäden nach Möglichkeit reduziert oder abgewendet werden können.

Konzepte der so genannten technisch-wissenschaftlichen Visualisierung bieten vereinfachte Sichtweisen auf komplizierte Strukturen [ScMu00]. Gerade bei dringlichen Angelegenheiten sind Entscheidungshilfen die einen schnellen Überblick bieten von großem Interesse. So können geeignete Visualisierungstechniken helfen, dass in komplexen Datenmengen böswillige Angriffe oder die Verbreitung von Schadsoftware schneller erkannt werden. Mit dieser Feststellung könnten zeitnah entsprechende Schutzmaßnahmen eingeleitet und die gewonnenen Informationen zum Schutz weiterer Instanzen an diese übermittelt werden.

2 Vorteile durch Visualisierung

Die Visualisierung (z.B. in Form eines Lagebildes) bietet große Vorteile, um schnell einen Eindruck und Überblick über viele Daten zu bekommen. So hilft eine geeignete Darstellung zum Beispiel bei dem Erkennen von gezielten Angriffen in Netzwerken. Werden bei der Visualisierung viele Kommunikationsparameter und -knoten berücksichtigt, kann das damit einhergehende Gefahrenpotenzial auf einen Blick erschlossen werden. In Analogie zu Wetterdaten können auch bei großen Netzwerken sehr viele Messwerte zu einem Zustand aggregiert werden.

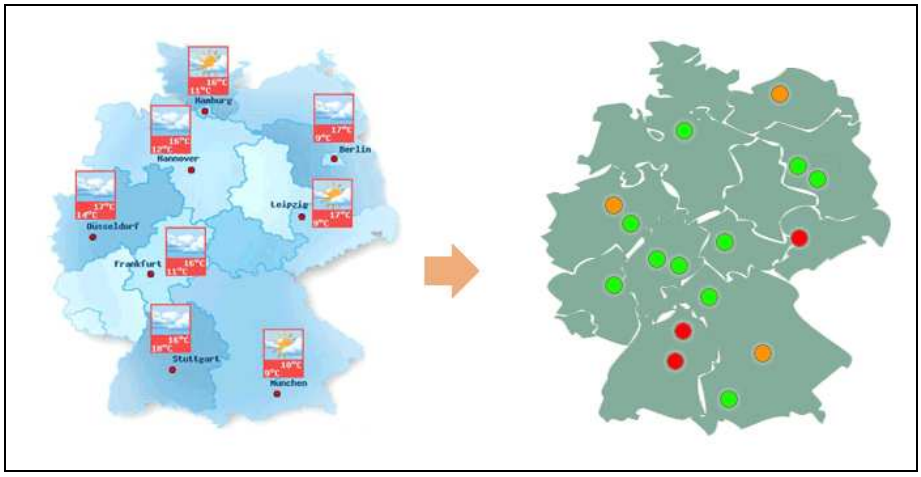

Abb. 1: Wetterzustände → Zustände von Kommunikationsknoten

Für einen Überblick ist es zunächst wichtig, dass nur essentielle und zusammengefasste Informationen dargestellt werden, um den Betrachter vor einer Informationsflut zu bewahren und seine Aufmerksamkeit nur auf das Wesentliche zu lenken. Große Netzwerke haben meist zahlreiche Kommunikationsknoten, die von verschiedensten Sicherheitssystemen wie Firewalls oder Intrusion-Detection-Systemen unter permanenter Überwachung stehen. Netzmanagement- und Sicherheitszentren haben daher großes Interesse, alle Störungen und Angriffe in Netzwerken zusammengefasst betrachten zu können, aber gleichzeitig auch die Betriebsbereitschaft und Verfügbarkeit von allen laufenden Systemen stets im Blickfeld zu haben.

Damit Gefahren so früh wie möglich eingedämmt werden können, ist es im Notfall ebenso wichtig, auch Zusammenhänge und Abhängigkeiten zwischen verschiedenen Kommunikationsparametern zu erkennen.

Die folgende Abbildung zeigt verschiedene Darstellungskomponenten des Visualisierungssystems um einerseits einen Überblick, andererseits Detailinformationen zwischen verschiedenen Parametern erkennen zu können. Zusätzlich können auch Details einzelner Parameter abgerufen werden. Darüber hinaus können einzelne Werte der Parameter auch in einer tabellarischen Darstellung mit anderen Kommunikationsparametern so genau verglichen werden, wie es grafische Darstellungen zumeist nicht ermöglichen.

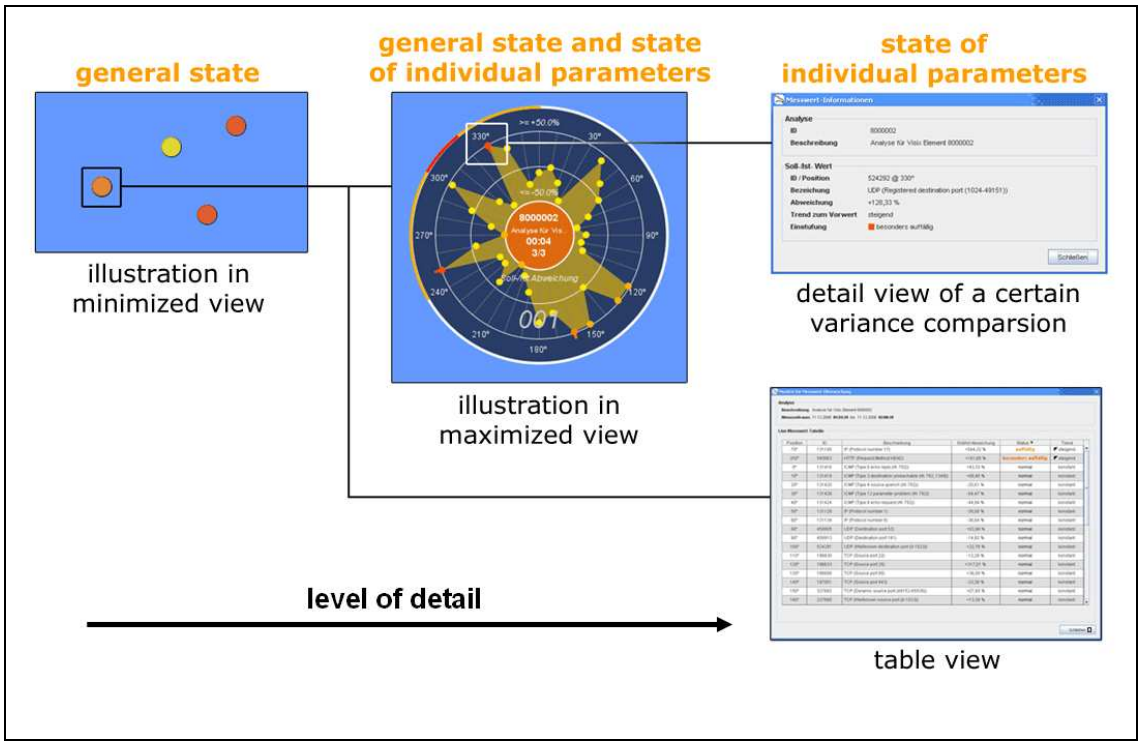

Abb. 2: Darstellungskomponenten des Visualisierungssystems

Der Anwender des Visualisierungssystems kann demnach ganz nach dem Prinzip „Overview first, then zoom and filter, and finally details on demand“ [Shne01] handeln, in dem er sukzessive weitere Details abruft und somit vor einer unnötigen Informationsflut verschont bleibt.

3 Bedrohungslage und Ist-Zustand im Überblick

Damit Lage-, Netzmanagement- und IT-Sicherheitszentren die Betriebsbereitschaft permanent laufender Systeme kontrollieren können, sollte neben einer Darstellung von Störungen und Angriffen auch der aktuelle Zustand einzelner Subnetze und Kommunikationsknoten in Netzwerken ständig abgebildet werden.

Um trotz des immensen Datenverkehrsaufkommens in großen Netzwerken den Zustand übersichtlich darzustellen, werden im Vorfeld nur besonders relevante Kommunikationsknoten für das Visualisierungssystem bestimmt. Diese werden ausschließlich unter Beachtung der Anonymität auf Unregelmäßigkeiten analysiert. Die ausgewählten Kommunikationsknoten liefern dem System den notwendigen Input. Dazu werden jeweils pro Knoten aus 870.000 verschiedenen Parametern aussagekräftige Kommunikationsparameter ausgewählt und in regelmäßigen Abständen an das System übermittelt. Aus diesen werden zeitlich abhängige Soll-/Ist-

Abweichungen berechnet und aus allen Abweichungen jeweils für einen Knoten ein zusammengefasster Zustand in Echtzeit visualisiert.

Mit Hilfe des Visualisierungssystems kann der Anwender nicht nur zusammengefasste Zustände ausgewählter Knoten darstellen, sondern hat außerdem die Möglichkeit, das Gefahrenpotenzial und die Verfügbarkeit einzelner Soll-/Ist-Werte (zum Beispiel: SMTP MAIL) zu überwachen.

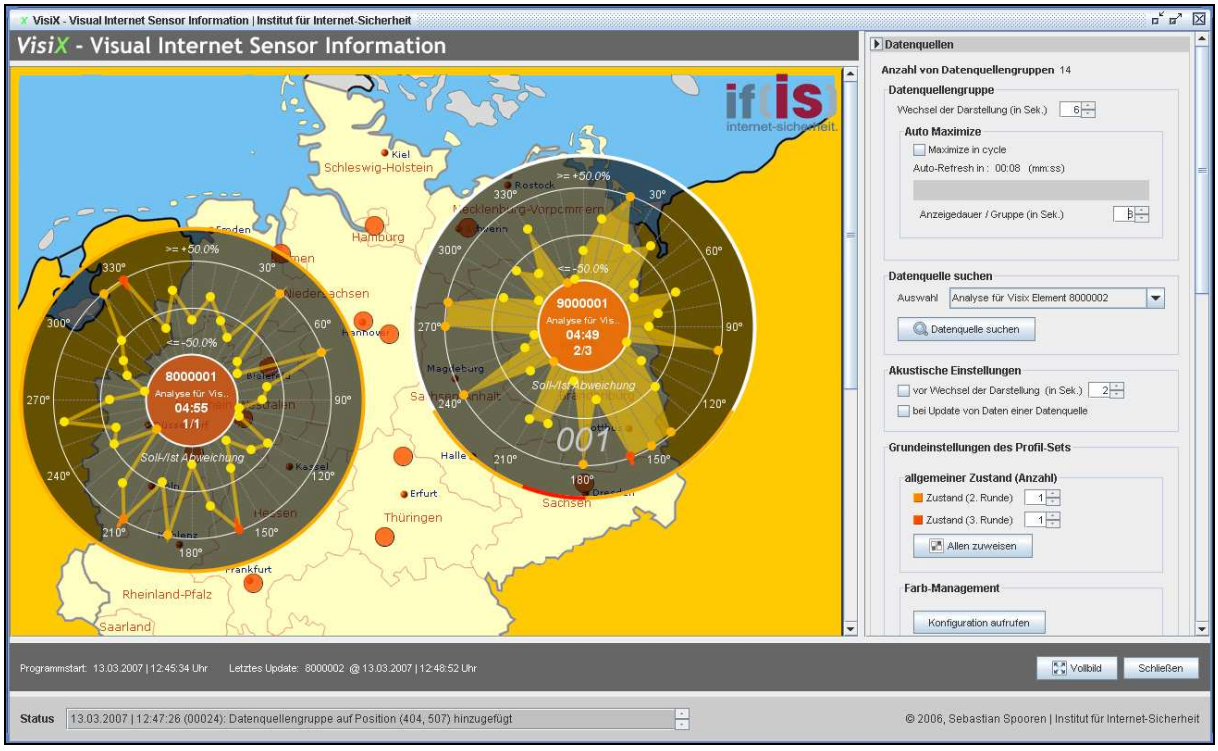

Abb. 3: Darstellung der Kommunikationsknoten beim laufenden System

In Abbildung 3 sind die Zustände von den meisten Kommunikationsknoten (z.B. bei Hamburg) als kleine farblich gefüllte Kreise dargestellt. Zwei Knoten befinden sich in der maximierten Darstellung, sodass sowohl in der Mitte der zusammengefasste Zustand des Knotens als auch die Zustände einzelner Kommunikationsparameter bzw. Soll-/Ist-Abweichungen abgelesen werden können. Je nach Grad der zugrunde liegenden Abweichungen und der daraus resultierenden Zustände werden zusammengefasste Zustände für ein Kommunikationsknoten generiert. Mögliche Zustände, sowohl für Parameter als auch Knoten sind: normal, bedrohlich und kritisch. Dabei wechseln die einzelnen Parameter eines Knotens beim wiederholten Auftreten von Grenzwertüberschreitungen ihren Zustand und visualisieren diesen geeignet. Wird ein kritischer Zustand erreicht, so wird die Aufmerksamkeit des Betrachters durch passende Visualisierungstechniken und optional auch mittels akustischer Ausgabe auf den betroffenen Kommunikationsknoten gelenkt.

Das Visualisierungssystem ist konzeptionell so aufgebaut, dass es auch in anderen Anwendungsbereichen eingesetzt werden kann. Es verfolgt dabei immer das Ziel, den Betrachter nur mit den Informationen zu versorgen, die dieser für die Erfüllung einer Aufgabe benötigt – ganz nach dem Grundsatz „*details on demand*“. Für weiterführende und detaillierte Analysen

mit anderen Systemen besteht außerdem die Möglichkeit, ausgewählte Parameter eines Kommunikationsknotens in ein unabhängiges Dateiformat zu exportieren.

3.1 Darstellung der Kommunikationsknoten

Abbildung 4 zeigt die Darstellung eines Kommunikationsknotens mit den Zuständen und Soll-/Ist-Abweichungen zugrunde liegender Kommunikationsparameter. Das Zentrum der Darstellungskomponente in Abbildung 4 repräsentiert den Ort der Messdatenerhebung und spiegelt über die Hintergrundfarbe des kleinsten Kreises den Zustand des Knotens wieder. Um einen solchen Knoten abzubilden, wählt der Benutzer des Systems im Vorfeld eine Visualisierungsgrundlage aus und positioniert dann den Kommunikationsknoten am Ort der Messdatenerhebung. Diese flexible und individuelle Zuordnung erlaubt es gleiche Datenquellen auf unterschiedlichen Visualisierungsgrundlagen, wie zum Beispiel auf einer geografischen oder topologischen Karte, abzubilden.

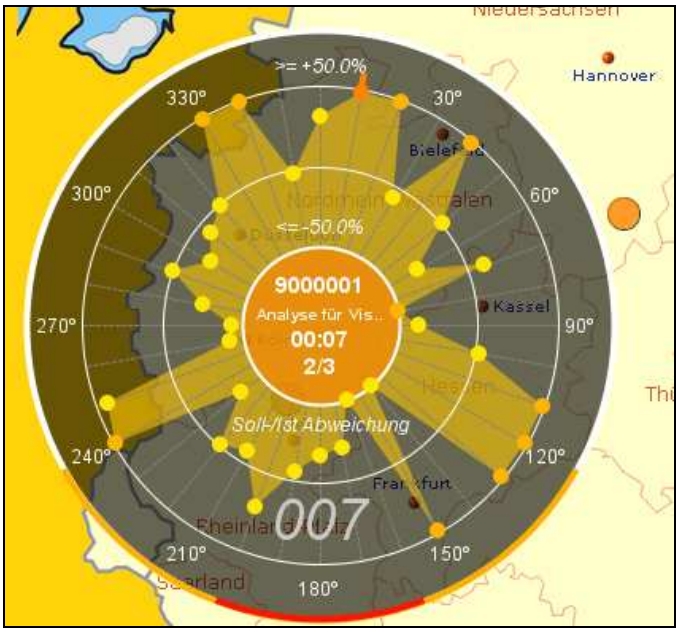

Abb. 4: Kommunikationsknoten mit zugrunde liegenden Parametern

Die Gradeinteilung bei der Darstellungskomponente grenzt die verschiedenen Kommunikationsparameter klar und deutlich voneinander ab, damit der Betrachter einzelne Parameter schnell aufzeigen und darüber hinaus auch mit dessen Hilfe schnell wieder finden kann. Die Auswahl der zu überwachenden Parameter wird an der vom Visualisierungssystem entkoppelten AlgoEngine (vgl. Kapitel 3.3) getroffen. Die Ausprägung einer Abweichung wird über die Radiusposition kodiert. Dabei kann jedem Parameter ein individueller Schwellwert zugewiesen werden. Weicht der Ist- gegenüber dem Sollwert um mehr als den im Vorfeld angegeben Schwellwert ab, so wird die Ausprägung einer Soll-/Ist-Abweichung auf der äußeren Schale abgebildet. Analog dazu wird der Ausprägung beim Unterschreiten von Soll-/Ist-Wert gegenüber dem Schwellwert auf der inneren Schale abgebildet. Nur die Soll-/Ist-Abweichungen, welche auf der inneren und äußeren Schale abgebildet werden wechseln ihren Zustand, wenn sie beim nächsten Datenupdate wiederum aufgrund ihrer Abweichung auf der gleichen Schale zum liegen kommen. Eine Trenddarstellung (vgl. Abbildung 4 bei 10°) verdeutlicht, ob die Abweichung vom Ist- gegenüber Sollwert ab- oder zugenommen hat.

3.2 Beispiel einer DDoS-Attacke mit VisiX

Das folgende Beispiel zeigt eine DDoS-Attacke von einem unbekannten Angreifer auf den Fachbereich Informatik der Fachhochschule Gelsenkirchen. Die linke Darstellung in Abbildung 5a repräsentiert den Zustand vor der DDoS-Attacke, während fünf Minuten später im rechten Bild jeweils eine deutliche Zunahme von ICMP - Echo Requests und TCP - SYN-Paketen über die Gradposition 20° und 90° zu erkennen ist.

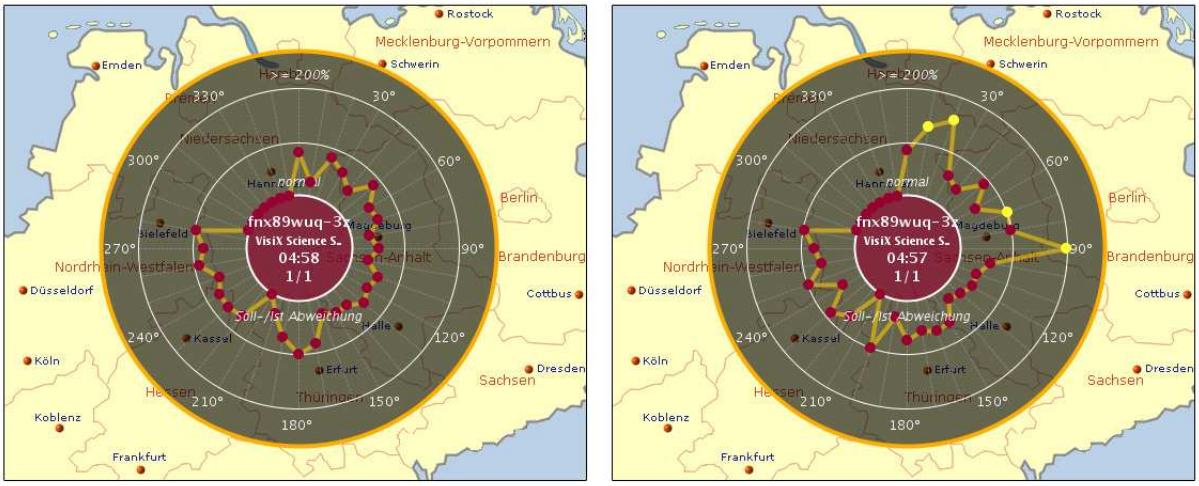

Abb. 5a: Visualisierung einer DDoS-Attacke nach fünf Minuten

Der rapide Anstieg von ICMP-Verkehr und SYN-Paketen macht sich im weiteren Verlauf bei anderen Diensten bemerkbar (vgl. Abbildung 5b). Durch die starke Auslastung im Netzwerk können Dienste wie DNS oder SMTP nicht mehr im normalen Maße ihre Arbeit verrichten. Dadurch reduziert sich der Netzwerkverkehr dieser Dienste gegenüber dem sonst üblichen Durchsatz. Dies wird fünf Minuten später in der Abbildung 5b, rechte Darstellung, deutlich. Nicht nur die Kommunikationsparameter für ICMP – Echo Requests und TCP – SYN-Paketen, sondern auch DNS-Requests (vgl. Abb. 5b, 130°) und SMTP-Traffic (vgl. Abb. 5b, 230°) weichen von Ihrem Normalverhalten ab, erreichen die Schwellwerte und wechseln Ihren Zustand in bedrohlich.

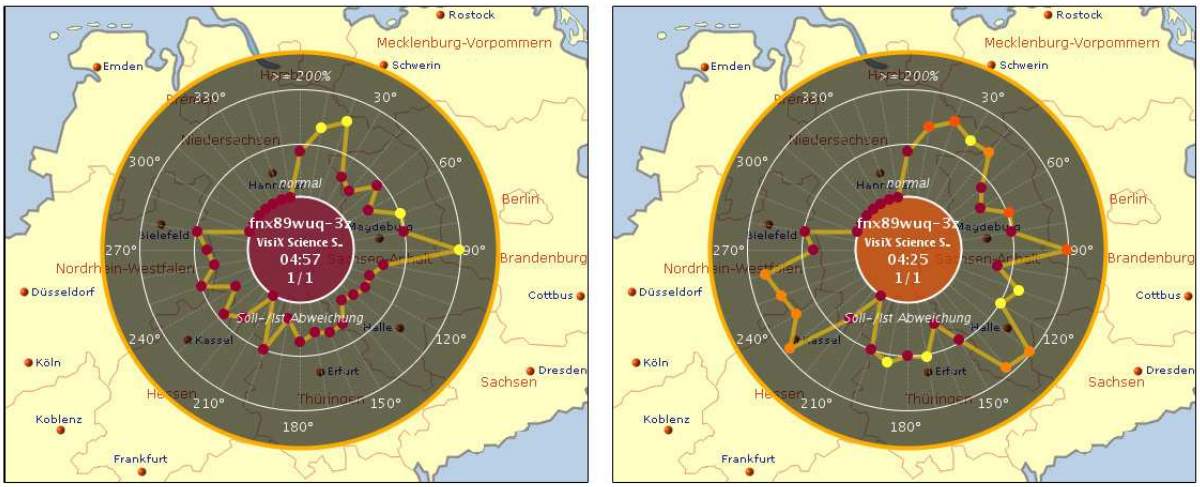

Abb. 5b: Visualisierung einer DDoS-Attacke nach zehn Minuten

3.3 Topologie der technischen Komponenten

Abbildung 6 zeigt den topologischen Zusammenhang zwischen dem Visualisierungssystem VisiX und den Komponenten des Internet-Analyse-Systems (kurz: IAS).

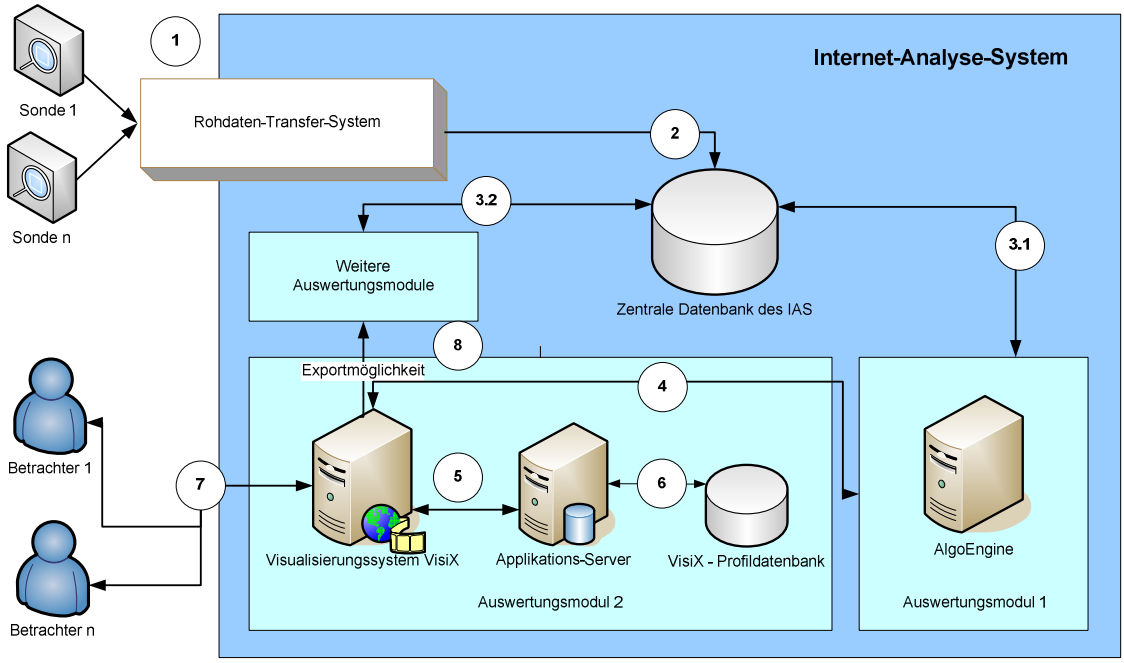

Abb. 6: Topologischer Zusammenhang der technischen Komponenten

Schritt 1 in Abbildung 6 stellt den Vorgang der Messdatenerhebung auf Basis von Sonden des IAS dar. Die Erfassung der Messdaten geschieht, indem Sonden für den Internetverkehr in eine Kommunikationsleitung integriert werden, um alle anfallenden Daten passiv abzugreifen. Bei der Erhebung von rund 870.000 unterschiedlichen Messwerten werden ausschließlich Header-Informationen extrahiert und in festen Intervallen an das Rohdaten-Transfer-System gesendet. Auf Basis des TCP werden die Daten über ein speziell dafür entwickeltes Netzwerkprotokoll [Proe05] zum Auswertungssystem übertragen.

In Schritt 2 wird veranschaulicht, dass die übertragenen Informationen in einer zentralen Datenbank des IAS persistent gespeichert werden. Die Speicherung der Kommunikationsdaten ist notwendig, damit Auswertungsmodule auf die Ansammlung der Messwerte, beispielsweise für die Erstellung von Profilen, jederzeit zurückgreifen können.

Die so genannte AlgoEngine [Deml07] fordert in *Schritt 3.1* die Messergebnisse an, um diese für weitere Auswertungsmodule, wie dem Visualisierungssystem, aufzubereiten. Danach werden die aufbereiteten Daten mit Hilfe der AlgoEngine in ein darstellungskonformes Format verpackt.

Schritt 3.2 soll deutlich machen, dass auch neben der AlgoEngine andere Auswertungsmodule wie das Reporting-System [Hunf07] existieren und die Möglichkeit haben, direkt auf die Datenbestände der zentralen Datenbank zuzugreifen.

Die AlgoEngine dient VisiX als Informationsquelle und ist über eine lose Kopplung in *Schritt 4* bidirektional realisiert. Über eine nach außen beschriebene Schnittstellendefinition erhält

das Visualisierungssystem notwendige Daten in einem generischen Format. Es ist eine bidirektionale Kommunikation zwischen beiden Komponenten notwendig, damit der Benachrichtigungswunsch aktueller Analyseergebnisse zwischen VisiX und dem Informationsbeschaffungsmodul über einen An- und Abmelde-Mechanismus realisiert werden kann.

Da die grafische Benutzungsoberfläche des Visualisierungssystems über viele verschiedene Konfigurationsparameter verfügt, können die Einstellungen mit Hilfe eines Profilmanagements über einen weiteren Applikationsserver zur Verwaltung der Profile (*vgl. Schritt 5*) in einer Datenbank hinterlegt werden (*vgl. Schritt 6*). Die zentrale Speicherung hat gegenüber der lokalen den Vorteil, dass der autorisierte Benutzer seine Profile unabhängig vom Ort über das Internet abrufen kann.

Schritt 7 soll die Schnittstelle zwischen Mensch und Computer, bestenfalls in Form von Großbildleinwand-Technik, verdeutlichen, damit die Ergebnisse des Visualisierungssystems vom Betrachter optimal wahrgenommen werden können.

Der letzte Schritt der Abbildung 6 (*vgl. Schritt 8*) zeigt die Möglichkeit auf, dass visualisierte Daten für andere Auswertungsmodule exportiert werden können. Auch hierbei ist es von großem Interesse, dass die Daten in ein generisches, und damit völlig vom IAS losgelöstes Format, transformiert werden können.

4 Ausblick

Das am Institut für Internet-Sicherheit entwickelte Visualisierungssystem hilft, Angriffe und Störungen im Bereich der IT-Sicherheit schneller zu erkennen aber auch die Betriebsbereitschaft von laufenden Systemen über Zustandsindikatoren zu überwachen. Dabei können komplexe Zusammenhänge unter den Kommunikationsparameter zu einem Messzeitpunkt, als auch einzelne Parameter über ein zugrunde liegendes Zustandsmodell sowie einer Trendanzeige über mehrere Messzeitpunkte verstanden werden.

Das Visualisierungssystem ist als Expertenwerkzeug zu verstehen, das durch neuartige Mehrwerte insbesondere bei dringlichen Entscheidungen, wie sie bei Frühwarnsystemen gefordert sind, zeitlich und qualitativ unterstützend wirken kann. Klare Vorteile werden mit dem System nicht nur hinsichtlich einer übersichtlichen Darstellung von komplexen Sachverhalten im Bereich der IT-Sicherheit erzielt, sondern auch durch die Möglichkeit Detailinformationen auf Abruf zu erhalten. Aufgrund der flexiblen Architektur lässt sich das Visualisierungssystem schnell in andere Anwendungsbereiche integrieren. Die Anbindung der Informationsquellen ist dabei im Idealfall ohne Programmieraufwand möglich, da sich anpassungsbedürftige Parameter unabhängig vom Quellcode modifizieren lassen.

Um mit diesem System beispielsweise den Zustand des Internets abzubilden, ist es erforderlich an strategisch ausgewählten Kommunikationsknoten Sonden des Internet-Analyse-Systems zu platzieren. Damit kann der Datenverkehr unter Berücksichtigung der Anonymität erfasst und anschließend geeignet visualisiert werden. Dabei wird alle fünf Minuten ausschließlich analysiert, welche Protokolle wie häufig verwendet wurden und auf welchen Ports die Kommunikation stattgefunden hat. Plötzlich auftretende Anomalien können durch Soll-/Ist-Analysen der verschiedenen Standorte schnell und einfach miteinander verglichen werden.

Wie das Anwendungsbeispiel mit der DDoS zeigt, können Netzmanagement-, Sicherheitszentren und Forschungseinrichtungen von der *technisch-wissenschaftlichen Visualisierung*

profitieren, wenn stets ein aktuelles Lagebild vom Zustand des Internets abgerufen werden kann. Die Auswirkung von Anomalien im Netzwerkverkehr auf andere Dienste kann mit VisiX schnell erkannt werden. Zudem steht der Überblick von vielen Kommunikationsknoten im Vordergrund, sodass schnell ersichtlich wird, ob Anomalien im Netzwerkverkehr von lokaler oder globaler Bedeutung sind.

Literatur

[Deml06] M. Deml: Konzeption und Implementierung eines Alarmierungsmoduls für ein Netzwerkmanagementsystem, Bachelor-Thesis am Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen (2006)

[Hein04] A. Heinecke: Mensch-Computer-Interaktion, Fachbuchverlag Leipzig im Carl Hanser Verlag (2004)

[Hunf07] K. Hunfeld: Entwicklung eines Reporting-Moduls für das Internet-Analyse-System, Diplomarbeit am Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen (2007)

[Jung98] V. Jung: Integrierte Benutzerunterstützung für die Visualisierung in Geo-Informationssystemen, In: TU Darmstadt, Frauenhofer IRB Verlag (1998)

[Proe05] M. Proest: Entwicklung einer Sonde für ein Internet-Analyse-System, Diplomarbeit am Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen (2005)

[ScMu00] H. Schumann, W. Müller: Visualisierung – Grundlagen und allgemeine Methoden, Springer Verlag (2000)

[Shne01] Ben Shneiderman: User Interface Design, mitp Verlag (2001)