Visual Analytics zur Firewall-Konfiguration und Analyse von Netzwerkverkehr

Fabian Fischer, Johannes Fuchs, Florian Mansmann, Daniel A. Keim
Lehrstuhl für Datenanalyse und Visualisierung, Universität Konstanz

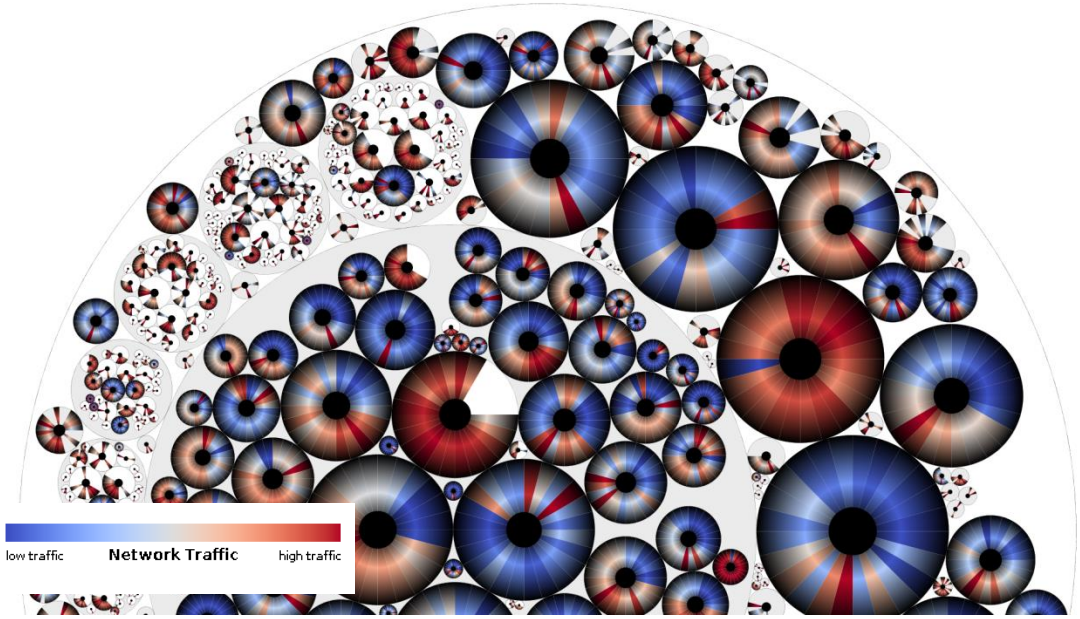

Abbildung 1: ClockMap Visualisierung: Visualisierung von Netzwerkverkehr eines großen Unternehmensnetzwerks. Die farbigen Segmente der einzelnen Kreise repräsentieren den Verlauf des stündlichen Netzwerkverkehrs verschiedener Computer für jeweils 24 Stunden.

Kurzfassung:
Vertrauen im Bereich Netzwerksicherheit schaffen bedeutet auch, die aktuelle Netzwerksituation, Netzwerkauslastung und Systemkonfiguration im Blick zu behalten und die aktuellen Abläufe zu verstehen. Ein blindes Vertrauen in vollautomatische Systeme ist in der heutigen dynamischen, sich schnell verändernden Welt nicht möglich und wird zu einem Vertrauensverlust führen. Thema des IT-Sicherheitskongress 2013, und Ziel von *Visual Analytics* ist es, Vertrauen und Sicherheit zu erhöhen und neue Erkenntnisse aus dynamisch, schnell wachsenden Datenmengen zu gewinnen. In unserem Beitrag wird die Idee von Visual Analytics kurz beschrieben und anhand von zwei erfolgreichen Anwendungen mit neuartigen Visualisierungsansätzen im Bereich Firewall-Konfiguration und Netzwerkanalyse verdeutlicht.

Stichworte: Visual Analytics, Netzwerksicherheit, Firewall, Netzwerkverkehr

1. Einleitung

Heutzutage bildet beinahe jedes Unternehmen ein potentielles Ziel für digitale Angriffe. Unterschiedlichste Schutzmechanismen versprechen Sicherheit gegenüber Zugriffen von Unberechtigten. Allerdings erfordern diese eine kontinuierliche Wartung zum Schutz gegen Angreifer. Da sich die technologischen Grundlagen des Netzwerkverkehrs und auch die Methoden der Angreifer ständig ändern, liefern automatische Ver-

fahren zwar wichtige Hinweise, können aber keine wirkliche Sicherheit garantieren. Die Idee unseres Visual Analytics Ansatzes ist es deshalb, den Menschen in die Analyse einzubeziehen und sein Wissen und seine Wahrnehmungsfähigkeiten zu nutzen, um eine effektive Analyse der Netzwerkdaten zu garantieren sowie Sicherheit und Vertrauen in die Systeme zu schaffen. In zwei Szenarien werden Beispiele für eine erfolgreiche Anwendung dieser Technologie gegeben.

Bei der Konfiguration von Firewalls in großen Netzwerken müssen die Regeln sinnvoll und lückenlos aufeinander abgestimmt werden, um unerlaubte Zugriffe zu unterbinden und das Netzwerk vor digitalen Eindringlingen oder Policy-Verstößen zu schützen. Allerdings reicht die einmalige korrekte Konfiguration nicht aus. Im laufenden Betrieb müssen neue Regeln definiert und alte angepasst werden, um auf stetig wechselnden Strategien der Angreifer zu reagieren. Die Menge der Regeln wird schnell sehr groß und komplex. Der Aufwand, diese zu warten steigt an und wechselndes Personal erschwert die fortwährende lückenlose Konfiguration der Firewalls. Mit Hilfe von Visualisierungen kann die Konfiguration einer Firewall erleichtert werden. Zusammenhänge und Abhängigkeiten zwischen verschiedenen Regeln können auf visuelle Weise dem Netzwerkadministrator kommuniziert werden, um ihn bei der Erstellung der Regeln sowie der Wartung bestehender Regeln zu unterstützen. *Visual Firewall* [1] ist ein Visualisierungsprogramm, welches Netzwerk-Administratoren bei der korrekten Firewall-Konfiguration unterstützt, indem die bestehende Struktur anschaulich dargestellt wird und interaktiv verändert werden kann.

Die Netzwerkverantwortlichen sind aber nicht nur für die korrekte Konfiguration der Systemdienste verantwortlich, sondern auch für die Überwachung des Netzwerkverkehrs. Zum einen stellt sich hier die Frage, ob die eingesetzten Regeln korrekt funktionieren und ob ein auffälliges Nutzungsverhalten einzelner Subnetze oder Computer vorliegt. Auch bei dieser Aufgabenstellung können neuartige visuelle und interaktive Techniken helfen, einen Überblick über die vorliegenden Verbindungsdaten zu erhalten. Die Visualisierungstechnik *ClockMap* [2] nutzt kompakte visuelle Repräsentationen, sogenannten Glyphen, welche in einer zirkulären Treemap-Darstellung (vgl. Abbildung 1) angeordnet sind.

2. Der Visual Analytics Ansatz

Visual Analytics [3] ist ein interdisziplinärer Ansatz (vgl. Abbildung 2) und stellt eine Kombination aus automatischen analytischen Methoden und Methoden der Informationsvisualisierung dar. Da bei der automatischen Verarbeitung und Anomalie-Erkennung der Benutzer im Verarbeitungsprozess in der Regel kaum involviert ist, muss dieser den Endergebnissen der automatischen Algorithmen blind vertrauen. Demgegenüber steht die Informationsvisualisierung, bei der Daten dem Benutzer auf anschauliche Weise präsentiert werden.

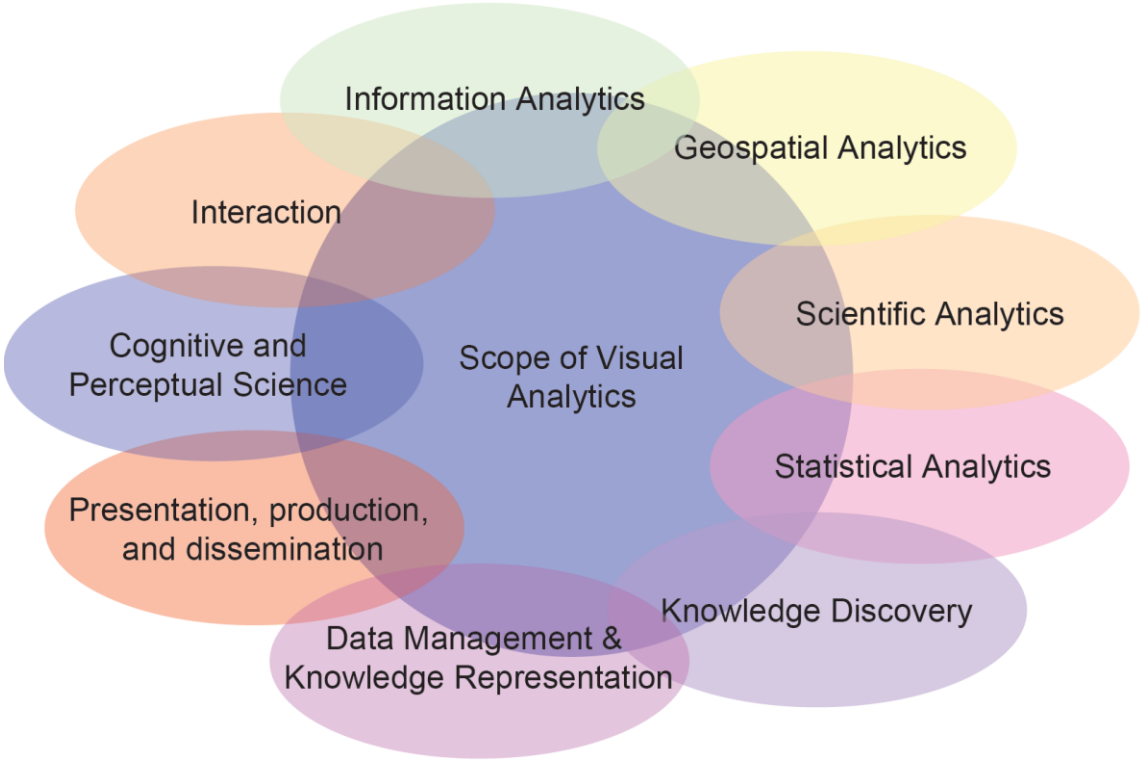

Abbildung 2: Visual Analytics: Die Kombination aus unterschiedlichen Forschungsgebieten trägt dazu bei aus großen und komplexen Datenmengen Erkenntnisse zu gewinnen.

Der Visual Analytics Ansatz verbindet die Stärken der visuellen Wahrnehmung des Menschen mit den technisch weitreichenden Möglichkeiten der automatischen Datenanalyse durch den Computer. Kognitive Wahrnehmungsprozesse und das Hintergrundwissen einer Person sind unabdingbare Faktoren bei der Datenanalyse, welche kein automatischer Prozess simulieren kann. Dem gegenüber steht der Computer mit hoher Rechenleistung und einem effektiven und effizienten Bearbeiten von klar definierten Aufgaben. Die Kombination beider Kompetenzen trägt entscheidend dazu bei, relevante Informationen aus einer überwältigend großen Menge an Informationen zu extrahieren und das Vertrauen in die (semi-)automatischen Prozesse zu stärken.

Um eine optimale Verbindung zwischen Mensch und Computer herzustellen, sind interaktive Visualisierungen nötig. Der Analyst kann dadurch die Daten explorieren, automatische Analyseprozesse lenken, sowie die Zwischenergebnisse verstehen und bewerten. Im Gegensatz zur reinen Informationsvisualisierung ist der Analyst nicht nur passiver Betrachter von Ergebnissen, sondern kann aktiv bei der automatischen Analyse mitwirken und diese beeinflussen.

Besonders im Bereich Netzwerksicherheit wird Visual Analytics in der Zukunft eine wichtige Rolle spielen. Extrem komplexe Datensätze müssen hier analysiert und ausgewertet werden. Dabei ist es wichtig, automatische Prozesse nachvollziehen und lenken zu können, um schnell mögliche Sicherheitslücken und Angriffsszenarien zu erkennen und darauf reagieren zu können.

3. Visual Analytics zur Firewall-Konfiguration

Firewall-Regeln liegen meist in gegliederter textueller Form vor, und können mit dem Programm *Visual Firewall* [1] analysiert und exploriert werden. Als visuelle Hauptkomponente kommt hierbei die sogenannte *Sunburst-Visualisierung* zum Einsatz, die durch unterschiedliche Interaktionstechniken eng mit der textuellen Regeldefinition verknüpft ist.

Die *Sunburst-Darstellung* spiegelt die Struktur der Firewall-Regeln in hierarchischer Form wider, welche je nach Anwendungsszenario visuell verändert werden können. Die oberste Ebene der Hierarchie bildet den Mittelpunkt der Visualisierung. Daraufhin tragen verschachtelte Ringe die nächsten Hierarchiestufen ab. Die Ringe werden aufgrund der Anzahl an Knoten auf dieser Hierarchiestufe unterteilt. Der Prozess wird so lange wiederholt, bis die unterste Hierarchieebene erreicht ist. Der Vorteil einer Sunburst-Visualisierung gegenüber einer Treemap ist die Anordnung der Hierarchieebenen. Während in einer Treemap-Visualisierung der Fokus auf den Blättern liegt, stellt eine Sunburst-Visualisierung die hierarchische Struktur der Daten explizit dar (siehe Abbildung 3). Dies begünstigt die hierarchische Darstellung einer Firewall-Regel. Auf der ersten Ebene finden sich somit die Namen der Zugriffssteuerungslisten, auf der zweiten die Zugriffsrechte („permit“ oder „denied“), auf der dritten die berücksichtigten Protokolle (z.B., „tcp“, „udp“ etc.) und abschließend Informationen über Quelle und Ziel.

Die Anzahl der sichtbaren Hierarchieebenen kann mit Hilfe eines Schiebereglers beliebig variiert werden. Dies erleichtert die visuelle Exploration der Daten, da unwichtige Elemente ausgeblendet werden können. Darüber hinaus verfügt die Visualisierung über eine Zoom-Funktionalität. Ein automatischer Zoom vergrößert die Visualisierung entsprechend dem zur Verfügung stehenden Platz. Wenn weniger Hierarchiestufen angezeigt werden, wird die Visualisierung dementsprechend größer. Der Analyst kann aber auch manuell auf beliebige Stellen der Abbildung zoomen und so seinen Fokuspunkt willkürlich setzen. Um den Fokus der Analyse weiter zu vertiefen, oder sehr kleine Schriftzüge sichtbar zu machen, kann die Größe einzelner Kreissegmente beliebig variiert werden um unwichtige Bereiche zu verkleinern und interessante mehr Platz einzuräumen.

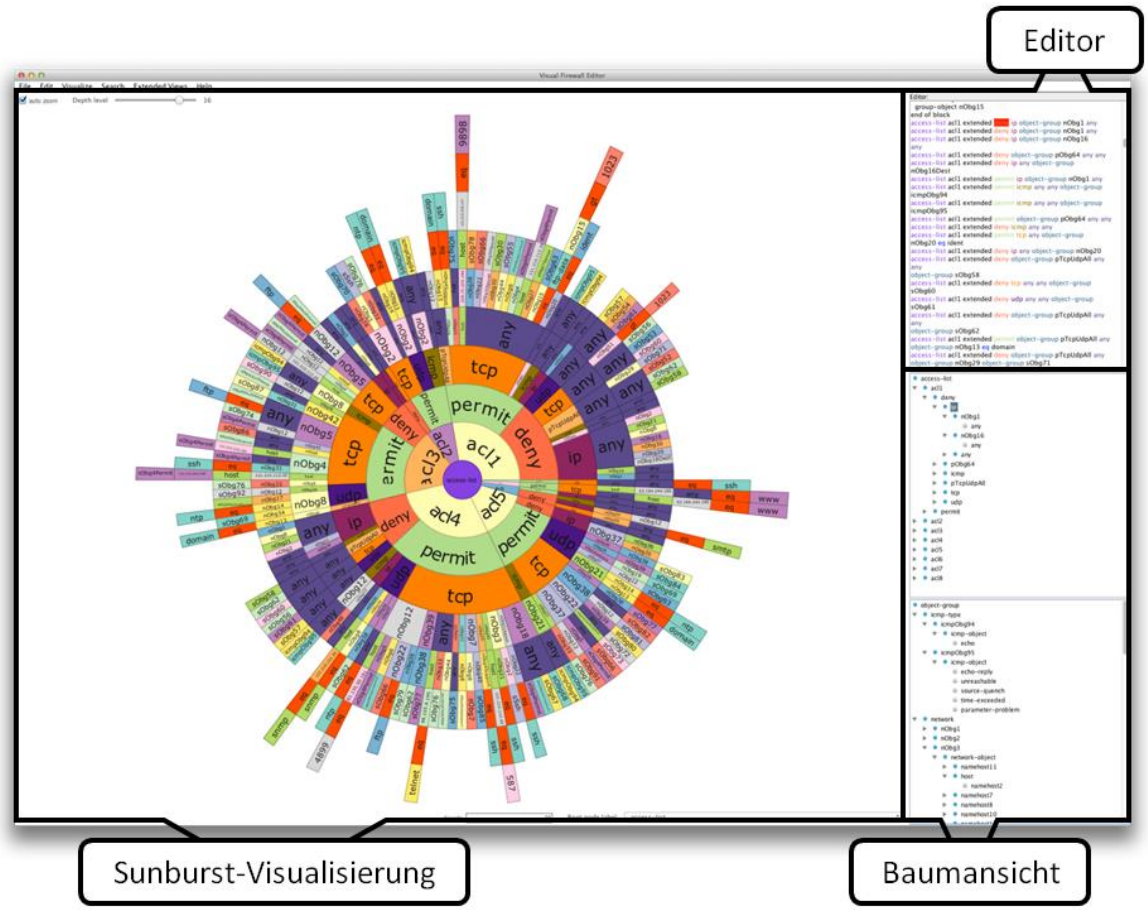

Abbildung 3: Visual-Firewall: Im linken Bereich des Tools befindet sich die Sunburst-Visualisierung. Auf der rechten Seite ist der Editor angeordnet. Beide Teile sind miteinander verlinkt und ermöglichen so ein übersichtliches Konfigurieren der Firewall Regeln. Durch Zuweisung von Kennzahlen können stark- und weniger frequentierte Regeln visuell hervorgehoben werden.

Die Visualisierung ist direkt mit einem Editor und einer Baumansicht verbunden, mit dem die Regeln editiert oder neue generiert werden können. Selektiert der Analyst ein Kreissegment mit der linken Maustaste, wird der dazugehörige Eintrag im Editor visuell hervorgehoben und das entsprechende Element in der Baumansicht geöffnet und markiert. Umgekehrt zeigt eine Textselektion den entsprechenden Knoten in der Visualisierung an. Der Editor kann wie ein gewöhnliches Textbearbeitungsprogramm verwendet werden. Hilfreiche Funktionen, wie beispielsweise das Kopieren und Einfügen von Regeln oder das Rückgängigmachen vorheriger Aktionen beschleunigen die Arbeit. Da Firewall-Regeln einer strikten Syntax unterliegen schlägt ein im Editor integriertes Hilfeprogramm dem Netzwerkadministrator automatisch sinnvolle „keywords“ vor. Dadurch wird eine falsche Konstruktion von Regeln vermieden und die Arbeit beschleunigt.

Die Baumansicht bildet eine alternative textuelle Darstellungsform der hierarchischen Daten. Zugriffssteuerungslisten können in strukturierter Form exploriert werden, in-

dem die einzelnen Einträge ähnlich einem Dateisystem aufgeklappt werden können, um die darunter liegende Elemente anzuzeigen.

Mit Hilfe von automatischer Analyse und Visualisierung können zum Beispiel sehr schnell ungenutzte Regeln herausgefiltert werden. Dafür werden entsprechende Zähler verwendet, die anzeigen, wie häufig eine Regel bei bestimmten Netzwerkverkehrsströmen verwendet wird. Mittels interaktiver Filtertechniken können lediglich die Regeln angezeigt werden, welche nie zum Einsatz kommen, was natürlich nicht unbedingt heißt, dass die Regeln nicht gebraucht werden. Die Visualisierung kann als exploratives Werkzeug verwendet werden, um die Regeln genauer zu untersuchen und die direkte Verbindung zwischen Visualisierung und Regeleditor erlaubt dabei das sofortige Löschen oder Editieren überflüssiger Regeln.

Auch sich widersprechende Regeln können, durch die enge Verknüpfung von Visualisierung und Editor, schnell ausfindig gemacht und behoben werden. Wie in Abbildung 5 ersichtlich beinhaltet die Zugriffssteuerungsliste „acl2“ sich widersprechende Regeln. Netzwerkverkehr über das „tcp“ Protokoll wird durch eine Regel blockiert, durch eine andere hingegen erlaubt. Dieser Widerspruch kann durch den Netzwerkadministrator visuell schnell erfasst und durch die Verlinkung von Visualisierung und Editor auch schnell behoben werden.

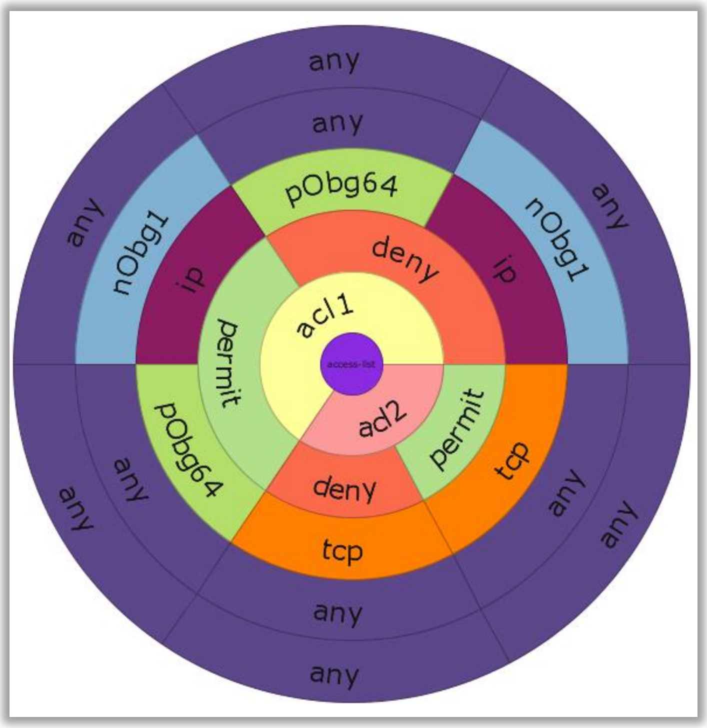

Abbildung 4: Sunburst-Visualisierung: Die Zugriffssteuerungsliste „acl2“ beinhaltet zwei kontradiktorische Regeln. Das „tcp“ Protokoll wird einerseits blockiert, andererseits aber freigegeben. Mit Hilfe der einheitlichen Farbkodierung lassen sich die Widersprüche schnell erkennen und mit Hilfe des Editors beheben.

4. Visual Analytics zur Analyse von Netzwerkverkehr

Aufgrund des Datenvolumens und der Komplexität der Daten ist es nicht einfach, einen Überblick über den Netzwerkverkehr einer Organisation oder eines Unternehmens zu geben. Dabei müssen einzelne Netzwerkkomponenten, Subnetze, sowie das ganze Unternehmensnetzwerk überwacht und auf Unregelmäßigkeiten hin analysiert werden.

ClockView [4], sowie die visuelle Weiterentwicklung *ClockMap* [2] sind Visual Analytics Tools zur Verbesserung der Netzwerksicherheit mit Hilfe einer visuellen Analyse des Netzwerkverkehrs. Dabei wird jede Netzwerkkomponente separat mit Hilfe einer kreisförmigen Uhr (Clock) als Kreis repräsentiert. Diese Kreise werden in 24 gleichgroße Segmente unterteilt. Jedes Segment repräsentiert eine Stunde, wodurch ein kompletter Tag abgebildet werden kann. Eine Farbkodierung repräsentiert die Anzahl an Verbindungen oder übertragenden Datenpaketen in der jeweiligen Stunde. Im Beispiel in Abbildung 5 ist somit ersichtlich, dass von 00:00 Uhr bis 09:00 Uhr morgens kein Datenverkehr von diesem Computer ausging. Erst ab 09:00 Uhr beginnt der Datenverkehr leicht zu steigen. Es ist anzunehmen, dass es sich hierbei um einen Büroarbeitsplatz handelt, der nachts komplett ausgeschaltet ist. In der Mittags-Zeit ist ein hohes Datenaufkommen (dunkelrotes Segment) festzustellen, was z.B. auf erhöhte Internetnutzung in der Mittagspause zurückzuführen sein könnte. Anschließend sinkt das Datenvolumen wieder ab (hellblaue Segmente), bis es in den Abendstunden wieder zunimmt (hellrote Segmente) und dann bis 23:00 Uhr weniger wird (dunkelblaue und hellblaue Segmente) und dann komplett endet (weiße Segmente).

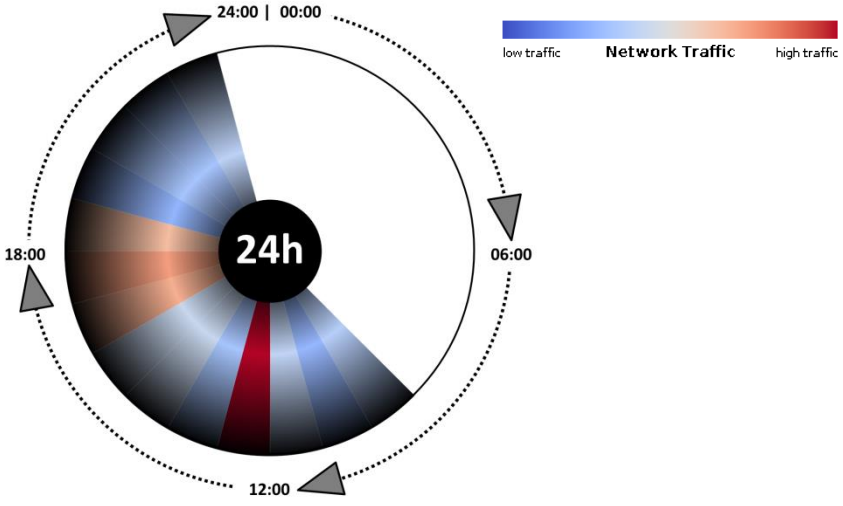

Abbildung 5: Clock-Darstellung: Die einzelnen Segmente des Kreises repräsentieren jeweils eine Stunde eines 24-Stunden Tages. Die Farbkodierung spiegelt die Menge des Netzwerkverkehrs zu der jeweiligen Stunde wider. Da in dem Zeitraum von 00:00 Uhr bis 09:00 Uhr und von 23:00 Uhr bis 23:59 Uhr Kein Datenverkehr vorlag, werden keine Segmente eingezeichnet.

Diese Visualisierung des Netzwerkverkehrs für einen einzelnen Computer bietet sich somit als sehr kompakte und skalierbare Darstellungsweise an. Typische Muster lassen sich auch bei geringer Auflösung des Kreises noch gut erkennen. Wenn nun ein Über-

blick über den Netzwerkverkehr von Tausenden Computern erstellt werden soll, stellt sich die Frage, welche Anordnung solcher Kreise am geeignetsten ist. In ClockView [4] wurde eine Matrix-Darstellung gewählt, wobei jeder Computer die gleiche Größe erhält. ClockMap [2] dahingegen macht sich die hierarchische Ordnung des vorliegenden Netzwerks zu nutzen. Dies könnte z.B. eine Unternehmenshierarchie mit den verschiedenen Gebäuden, Abteilungen oder Arbeitsgruppen sein, oder auch die verschiedene Subnetzwerke basierend der IP-Adressen der Computer. Diese Information wird nun bei der Positionierung der Clocks berücksichtigt. Grundlage bildet ein zirkulärer Treemap-Algorithmus. Eine Treemap ist eine Visualisierungsart, welche besonders für hierarchische Daten geeignet ist. Dabei werden Rechtecke oder Kreise ineinander geschachtelt um die unterschiedlichen Ebenen der Hierarchie widerzuspiegeln.

In unserem Fall repräsentiert jedes Subnetz der IP-Adresse eine Hierarchiestufe. Auf der tiefsten Stufe werden die einzelnen Netzwerkkomponenten (/32) in zirkulärer Weise angeordnet. Mit Hilfe von Interaktionstechniken kann der Analyst interaktiv eine Abstraktionsstufe heraus zoomen. Dadurch schließen sich die kreisförmig angeordneten Elemente zu einer einzelnen Clock zusammen und repräsentieren somit jeweils das allgemeinere Subnetz (/24). Der Netzwerkverkehr sämtlicher Netzwerkkomponenten wird aggregiert und mit Hilfe einer einzelnen Clock dargestellt. Diese Zoom- und Abstraktionsfunktionalität kann so lange wiederholt werden, bis letztendlich nur noch eine Clock den kompletten Netzwerkverkehr des gesamten Netzwerkes darstellt (/0). In ClockMap kann das automatisch generierte hierarchische Layout der einzelnen Clocks zudem manuell mit Hilfe von Interaktionstechniken beeinflusst werden. Der Benutzer kann im Laufe seiner Analyse, Clocks verschieben, anderen Gruppen zuweisen, oder gänzlich neue Gruppen erstellen. Sehr auffällige Clocks können dadurch separat voneinander analysiert werden, oder ähnliche Clocks zusammen gruppiert werden. Das Layout der Visualisierung passt sich den Änderungen an, indem Aggregationen und die geänderten Positionen von Clocks neu berechnet werden. Um spezielle Netzwerkkomponenten zu finden oder auf einzelnen Attributen zu filtern ist eine Suchfunktion in ClockMap integriert.

In Abbildung 6 ist ein typischer Workflow für die Exploration auffälliger Muster abgebildet. Der Nutzer startet ClockMap auf den NetFlow-Daten des vergangenen Tages. Der Datenverkehr aller überwachten Computer wird aggregiert und als einzelne Zeitserie in einer einzelnen Clock repräsentiert (1. Schritt). Der Nutzer erkennt nun schon ein sehr globales Muster, dass zwischen 23:00 Uhr und 23:59 Uhr wohl am meisten Datenverkehr aufgetreten ist (dunkelrotes Segment). Durch Hineinzoomen wird die nächste Hierarchie-Ebene geladen. Es werden alle Subnetzwerke angezeigt. Aufgrund der Größe lässt sich erkennen, dass in diesem Netzwerk ein Subnetzwerk besonders groß ist. Dieses wird durch Selektion weiter exploriert. Innerhalb dieses findet sich nun z.B. eine sehr auffällige Clock eines Subnetzwerks, welche keinerlei Datenverkehr in der Nacht zu haben scheint. Dieses verdächtige Netzwerkverhalten kann näher untersucht werden, indem der Analyst nun in dieses Netzwerk hineinzoomt, um weitere Details zu erhalten. Die Unregelmäßigkeit könnte zum Beispiel auf eines Routen- oder Internetausfalls zurückzuführen sein. Die Auswahl dieses Subnetzwerkes und Hinein-

zoomen, ermöglichen die Exploration aller beteiligten Computer als letzten Schritt der Analyse. Durch das Hintergrundwissen des Analysten, kann die Beobachtung dadurch erklärt werden, dass dieses Subnetz, für den drahtlosen Internetzugang des Unternehmens verwendet wird und somit nachts keinen Datenverkehr aufweist, was zudem der üblichen Policy in diesem Netzwerk entspricht.

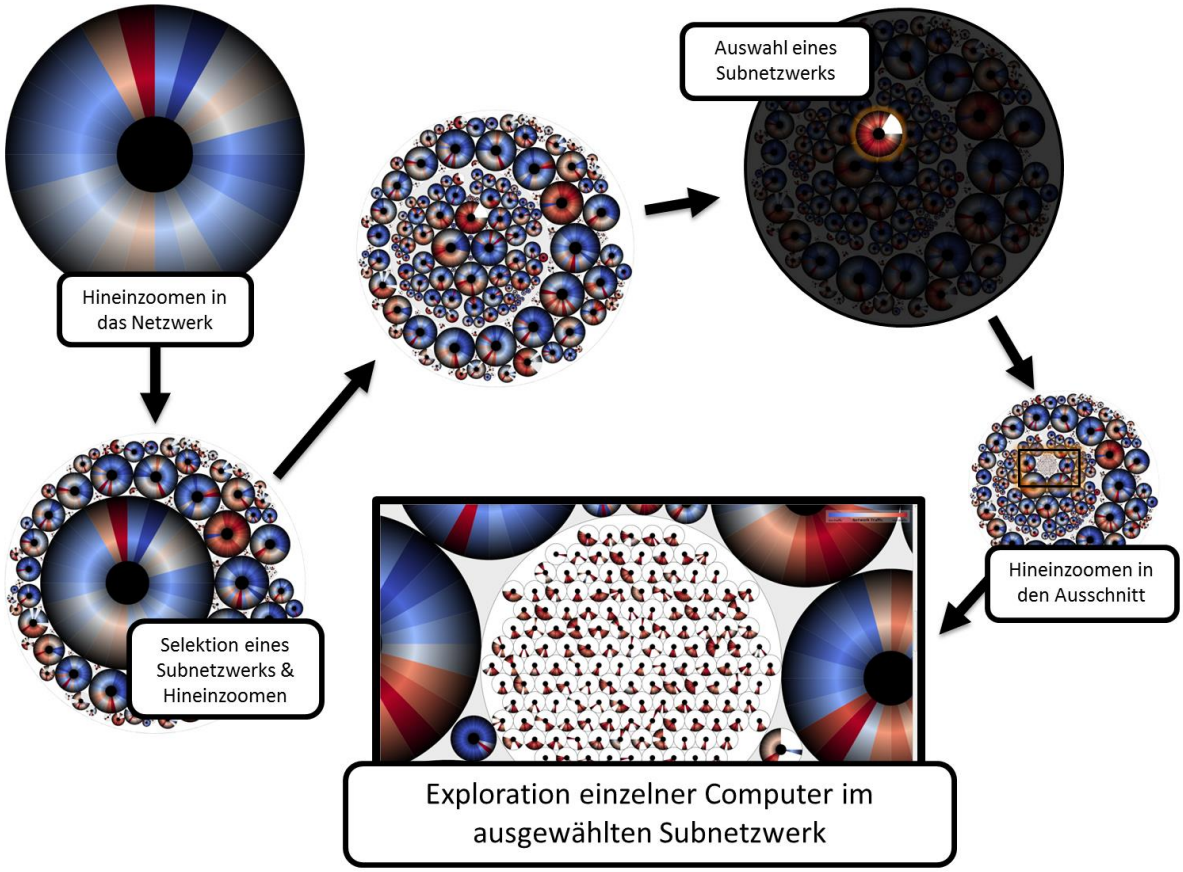

Abbildung 6: Workflow für die visuelle Exploration eines großen Netzwerks. Im ersten Schritt ist nur eine einzelne Clock-Repräsentation dargestellt. Diese zeigt den Datenverkehr des gesamten Netzwerks. Durch weitere Interaktion kann hierarchisch in interessante Teilnetzwerke hinabgestiegen werden, um schließlich im letzten Schritt den zeitlichen Datenverkehr einzelner Computer zu betrachten.

Auf gleicher Weise lassen sich allerdings auch verdächtige Rechner identifizieren, die sich z.B. aufgrund des Datenverkehrsmusters massiv von anderen Rechnern in ihrem Subnetzwerk unterscheiden oder besonders hohes Datenvolumen verursachen. Durch die interaktive Exploration durch An- und Abschalten der Aggregationsfunktion der einzelnen Clocks, wie in Abbildung 7 angedeutet, lassen sich Aktivitätsmuster vergleichen und visuell korrelieren.

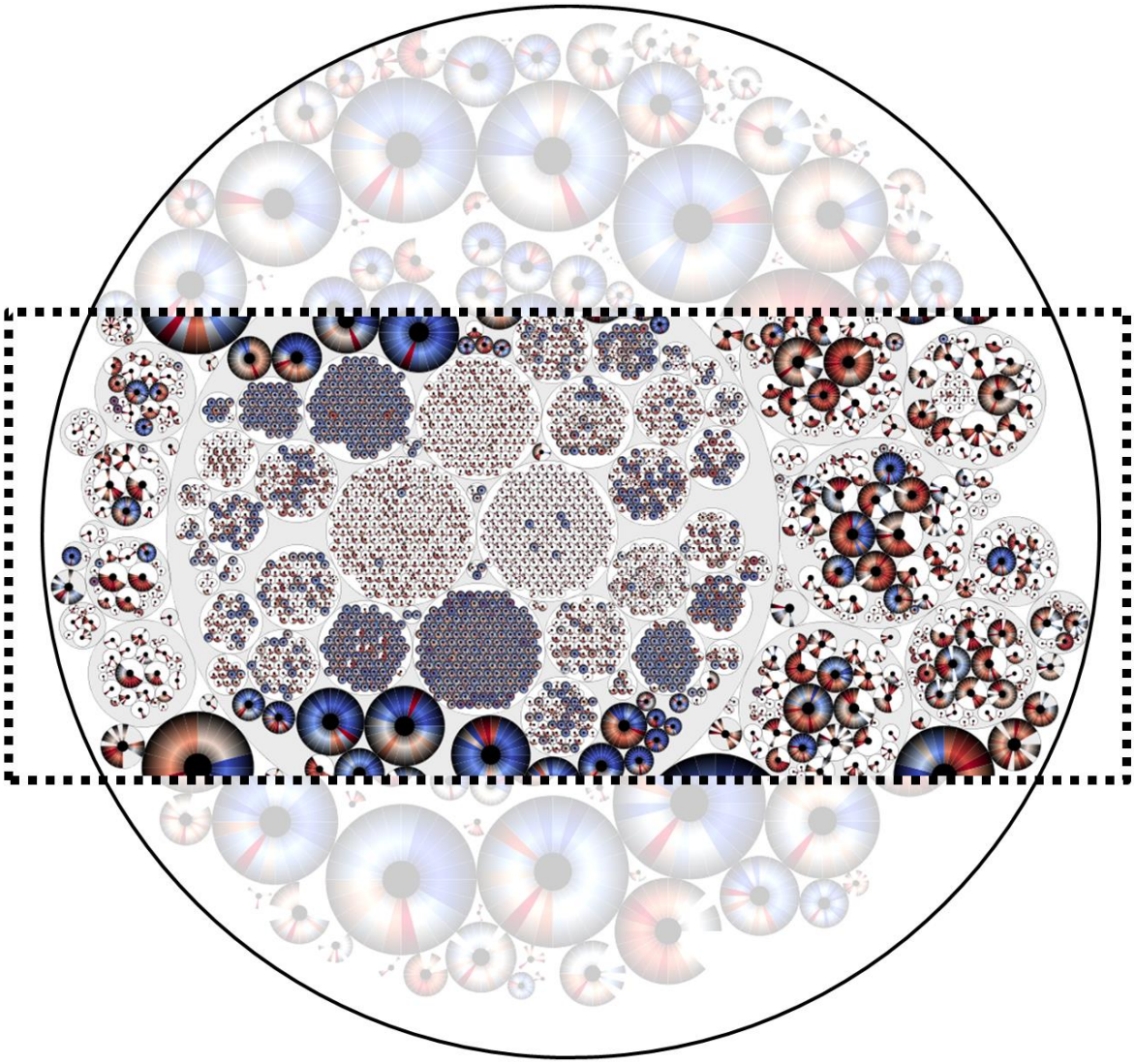

Abbildung 7: Der zirkuläre Treemap-Algorithmus ordnet die Clocks kreisförmig an und gruppiert diese z.B. anhand ihrer IP-Adresse. Das eingezeichnete Rechteck wurde manuell hinzugefügt und zeigt eine tiefere Hierarchieebene.

5. Zusammenfassung und Ausblick

Der dynamische Zuwachs an Informationen und die Zusammenführung von verschiedenen Datenquellen stellt eine große Herausforderung für die Netzwerksicherheit dar. Die Möglichkeiten der skalierbaren Speicherung und Verarbeitung haben sich in den letzten Jahren durch moderne skalierbare Systeme deutlich verbessert. Herausforderung ist es allerdings weiterhin in diesen Datenmengen, Auffälligkeiten zu identifizieren und Erkenntnisse zur Verbesserung der Informationssicherheit zu gewinnen. In unserer Arbeit stellten wir das Forschungsgebiet *Visual Analytics* vor und beschrieben anhand zweier Visualisierungssysteme, wie es Analysten ermöglicht durch die Kombination von analytischen Methoden mit neuartigen interaktiven Visualisierungstechniken, gerade solche großen und komplexen Datenmengen zu explorieren. Im vor-

liegenden Kontext haben wir zwei Forschungsarbeiten vorgestellt. Bei Visual Firewall [1] stand die visuelle Konfiguration von Firewall-Regeln im Vordergrund. Diese Kombination von herkömmlichen, computer-lesbaren Konfigurationsdateien mit einer visuellen Repräsentation trägt dazu bei, dass der Anwender ein besseres Verständnis von komplexen Zusammenhängen erhält. Somit hilft das Tool z.B. Konfigurationsfehler zu vermeiden oder bereits vorhandene Konfigurationen durch visuelle Analyse inhaltlich prüfen zu können. Diese Erkenntnisse über Zusammenhänge und das Vermeiden von Fehlern trägt dazu bei, die allgemeine Netzwerksicherheit zu verbessern.

Ebenso wurde ClockMap [2] vorgestellt um den Netzwerkverkehr von Tausenden Computern über die Zeit hinweg visuell zu explorieren. Durch die skalierbare Darstellungsweise und Integration von Hierarchieebenen können so auch sehr große Computernetzwerke mit einer Vielzahl von Subnetzwerken analysiert werden. Die vielfältigen Interaktionsmöglichkeiten ermöglichen dem Nutzer die Analyse zu steuern und relevante Fragestellungen zielgerichtet zu bearbeiten.

Es wurde somit gezeigt, dass es durch den Einsatz solcher Visual Analytics Tools dem Anwender möglich wird, Hintergrundwissen in die Analyse einfließen zu lassen und schlussendlich Erkenntnisse aus großen Datenmengen zu gewinnen. Diese enge Verbindung von Mensch und Computer durch visuelle Repräsentationen trägt somit entscheidend zur Verbesserung der Informationssicherheit bei und stärkt schlussendlich das Vertrauen in die Sicherheit.

Referenzen

[1] F. Mansmann, T. Göbel and W. Cheswick. **Visual Analysis of Complex Firewall Configurations**. *Proceedings of the 9th International Symposium on Visualization for Cyber Security, ACM, 2012.*

[2] F. Fischer, J. Fuchs and F. Mansmann**. ClockMap: Enhancing Circular Treemaps with Temporal Glyphs for Time-Series Data.** *Proceedings of the Eurographics Conference on Visualization (EuroVis 2012), 2012.*

[3] D. A. Keim, F. Mansmann, J. Schneidewind and H. Ziegler. **Challenges in Visual Data Analysis**. *Information Visualization (IV 2006), IEEE Press, 2006.*

[4] C. Kintzel, J. Fuchs and F. Mansmann. **Monitoring Large IP Spaces with ClockView.** *Proceedings of the 8th International Symposium on Visualization for Cyber Security, ACM, 2011.*