VisiX

Darstellung von komplexen Sicherheitssituationen mit „Visual Internet Sensor Information“

Dem Internet den Puls fühlen

Besonders seit dem 11. September 2001 ist in vielen Bereichen die Nachfrage in puncto Sicherheit so groß wie nie zuvor. Weltweit besteht immer öfter das Interesse Frühwarnsysteme zu schaffen, damit Gefahren und Risiken noch schneller erkannt und bevorstehende Schäden soweit wie möglich reduziert oder gar vollständig abgewendet werden können. Mit dem am Institut für Internet-Sicherheit (ifis) der Fachhochschule Gelsenkirchen entwickelten System VisiX lassen sich bedeutsame Informationen aus einer Fülle an Daten in eine für den Betrachter angemessenen Weise präsentieren. Dabei steht es im Vordergrund, dass dringliche Entscheidungen – insbesondere bei Gefahren – einfacher und schneller als bisher getroffen und komplexe Sachverhalte gegenüber Dritten auf verständliche Art und Weise verdeutlicht werden können.

Im Bereich der IT-Sicherheit wird mit VisiX (Visual Internet Sensor Information) auf Basis raum- und zeitbezogener Soll-/Ist- Abweichungen beispielhaft der aktuelle Zustand des Internets repräsentiert. Dabei ist das Visualisierungssystem jedoch 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“.
Um trotz des immensen Datenverkehrsaufkommens im Internet eine übersichtliche und damit leicht wahrnehmbare Darstellung vom Ist-Zustand zu ermöglichen, werden vom Betrachter besonders relevante Kommunikationsknoten ausgewählt, unter Beachtung der Anonymität analysiert und daraus resultierende Allgemeinzustände visualisiert.

Damit verschiedene Zustände (wie beispielsweise: normal, bedrohlich, kritisch) generiert werden können, wechseln zugrunde liegende Parameter der Kommunikationsknoten beim wiederholten Überschreiten von individuellen Grenzwerten 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 die betroffene Datenquelle gelenkt. Damit jedoch auch zwischen unterschiedlichen Anwendungsfällen schnell gewechselt werden kann, lassen sich diese in Form persönlicher Profile vollständig speichern, laden und löschen. Für weiterführende Analysen mit anderen Systemen besteht außerdem die Möglichkeit, ausgewählte Parameter eines Kommunikationsknotens in ein unabhängiges Format zu exportieren.
Um bei der Präsentation der Daten auf die individuellen Wünsche des Anwenders einzugehen, verfügt das Visualisierungssystem über mehrere Darstellungskomponenten. Diese erlauben einerseits einen schnellen und einfachen Gesamtüberblick über den Zustand eines Netzwerkes (minimierte Ansicht der Datenquellen) und andererseits die Überwachung individuell ausgewählter Parameter der Kommunikationsknoten (maximierte Ansicht der Datenquellen).

Darüber hinaus können einzelne Kommunikationsparameter sowohl im Detail (Detail-

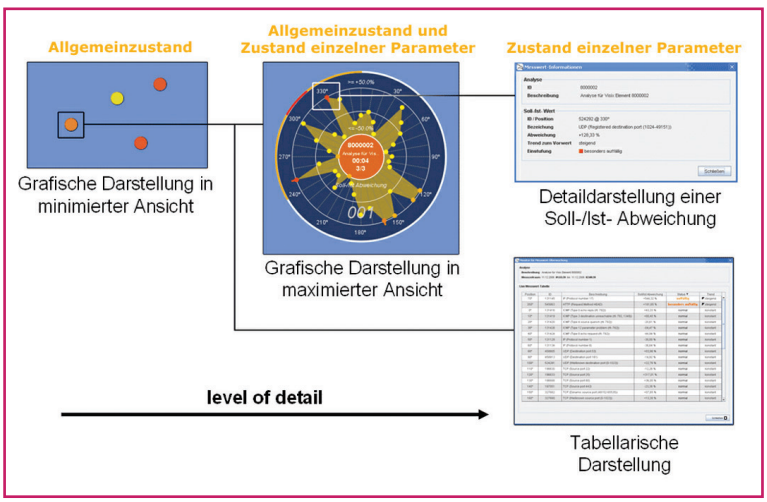

Bild 1: Informationsdarstellung nach dem Prinzip: „details on demand“

darstellung einer Soll-/Ist-Abweichung) als auch exakte Werte korrespondierender Kommunikationsparameter (tabellarische Darstellung) so genau verglichen werden, wie es grafische Darstellungen zumeist nicht ermöglichen.

Flexible Benutzerschnittstelle

Um Ursachen wie Spam-Attacken oder böswillige Malware-Angriffe bereits frühzeitig zu erkennen, soll das Visualisierungssystem komplexe Strukturen einfach veranschaulichen. Mithilfe flexibler Zustandsindikatoren lassen sich infolgedessen Präventivmaßnahmen schaffen und Risiken gezielter minimieren. So kann zum Beispiel auf Basis einer erhöhten Soll-/Ist- Abweichung die Verbreitung eines neuen Computerwurms rechtzeitig erkannt und anschaulich visualisiert werden. Auf diese Weise lässt sich eine drohende Gefahr für die Informationsgesellschaft schneller eindämmen.

Die Benutzerschnittstelle besteht aus einem zweigeteilten Basisfenster. Bild 2 zeigt einen exemplarischen Anwendungsfall des Systems. Das links dargestellte Panel repräsentiert das Interaction-Panel und ist Grundlage für die Visualisierung der Zustandsinformationen. Das rechte Panel enthält Interaktionselemente zur Konfiguration des Systems.
Damit ein Anwendungsfall visualisiert werden kann, hat der Anwender einerseits die Möglichkeit, eine bekannte Szene mit allen individuellen Einstellungen über das Profilmanagement zu laden oder andererseits eine Visualisierungsgrundlage auszuwählen und die Datenquellen mit dem Zeigegerät auf dem Interaction-Panel zu positionieren.

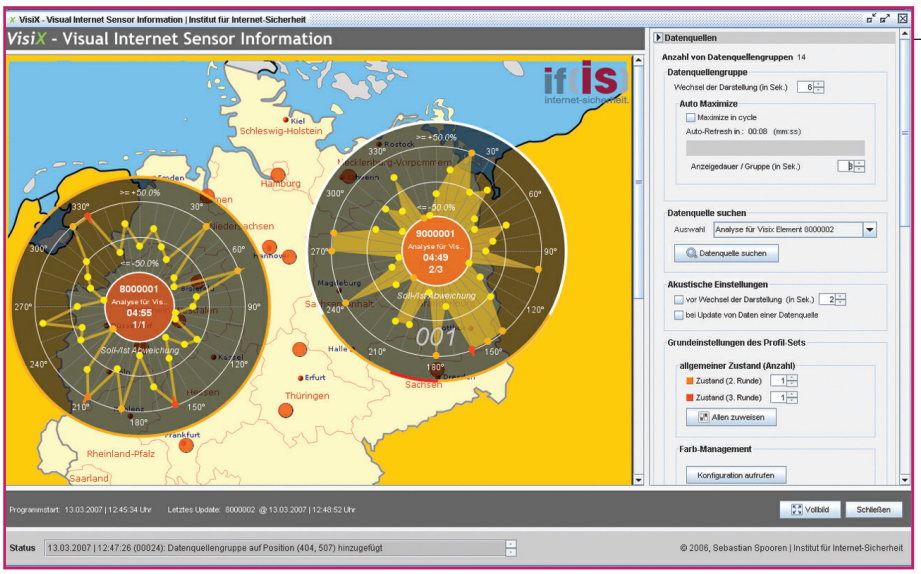

Bild 2: Beispielhafte Darstellung ausgewählter Kommunikationsknoten über die Benutzerschnittstelle

Damit bei der Darstellung eines Kommunikationsknotens die Details einzelner Parameter vom Betrachter schnell erfasst werden können, existiert unter anderem auch die Darstellung eines Kommunikationsknotens in maximierter Ansicht.

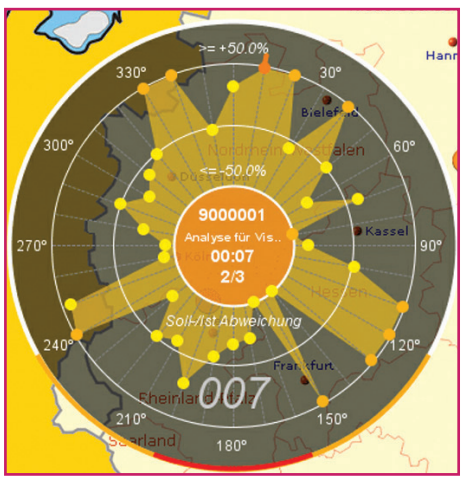

Bild 3: Grafische Darstellung einer Datenquelle mit Kommunikationsparametern

Bild 3 zeigt die Darstellung einer Datenquelle mit den Zuständen und Werten ihrer zugrunde liegenden Kommunikationsparameter. Das Zentrum der im Bild gezeigten halbtransparenten Darstellungskomponente stellt den Ort der Messdatenerhebung dar.

Der Anwender wählt dazu im Vorfeld eine Visualisierungsgrundlage aus und positioniert die Datenquelle 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. Die Gradeinteilung bei der Darstellungskomponente grenzt die verschiedenen Kommunikationsparameter klar und deutlich voneinander ab, damit der Betrachter einzelne Kommunikationsparameter anhand ihrer Gradzuordnung schnell aufzeigen und darüber hinaus auch mit dessen Hilfe schnell wieder finden kann.

Die Ausprägung einer Abweichung wird dabei über die Radiusposition kodiert. Dazu kann jeder Datenquelle ein individueller Schwellwert zugeordnet werden. Weicht ein 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 und analog dazu auf der inneren Schale abgebildet. Nur die Soll-/Ist- Abweichungen, die auf der inneren und äußeren Schale abgebildet werden, wechseln, wenn sie beim nächsten Datenupdate wiederum aufgrund der Ausprägung ihrer Abweichung auf der gleichen Schale liegen, ihren Zustand. Eine Trenddarstellung (siehe Bild 3 bei 10 Grad) verdeutlicht, ob der Abweichungsgrad vom Ist- gegenüber Sollwert abgenommen oder zugenommen hat.

Damit eine spezifische Datenquelle gegenüber anderen Datenquellen schnell identifiziert werden kann, wird neben einer eindeutigen Identifikationsnummer auch eine individuelle Datenquellenbeschreibung angezeigt. Da die Quellen ihre Daten nicht zu festen Zeitpunkten erfassen, das Zeitintervall zwischen den Erhebungen der Messdaten dennoch meist identisch ist, informiert eine Countdown-Anzeige bis zum nächsten Datenupdate mit einer geschätzten Zeitangabe.

Fazit

Das am (ifis) entwickelte Visualisierungssystem für komplexe Sicherheitssituationen hilft, wichtige Sachverhalte durch geeignete Visualisierungstechniken effizient darzustellen. Zudem unterstützt es bei der Entscheidungsfindung. 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 wirkt. Klare Vorteile werden mit dem System nicht nur hinsichtlich einer übersichtlichen Darstellung von komplexen Sachverhalten (Sicherheitssituationen) erzielt, sondern auch durch die Möglichkeit, Detailinformationen auf Abruf zu erhalten eingeräumt. 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. Eine Schnittstelle für den Datenexport bietet außerdem die Möglichkeit für weiterführende Analysen.

Prof. Dr. Norbert Pohlmann,
Dipl.-Inform. (FH) Sebastian Spooren
spooren@internet-sicherheit.de

Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen,
Fachbereich Informatik
www.internet-sicherheit.de

Literatur:

Bertin, J. (1982): Grafische Darstellungen und die grafische Weiterverarbeitung der Information. In: De Gruyter
Cleveland, W.S. (1985): Visualizing Data. In: Hobart Press
Geroimenko V.; Chen, C. (2003): Visualizing the Semantic Web – XML based Internet and Information Visuali-zation. In: Springer Verlag
Ipanema Technologies (2006): Multidimensionale Performance-Überwachung in Echtzeit. In: unicat communi-cations
Spooren, S. (2007): Entwicklung eines profilgestützten Visualisierungssystems zur Darstellung von raum- & zeitbezogenen Soll-/Ist- Abweichungen, Diplomarbeit; Institut für Internet-Sicherheit, FH-Gelsenkirchen