Gefahrenpotenzial visualisieren

Erfassung und Visualisierung des Malware-Aufkommens im World Wide Web

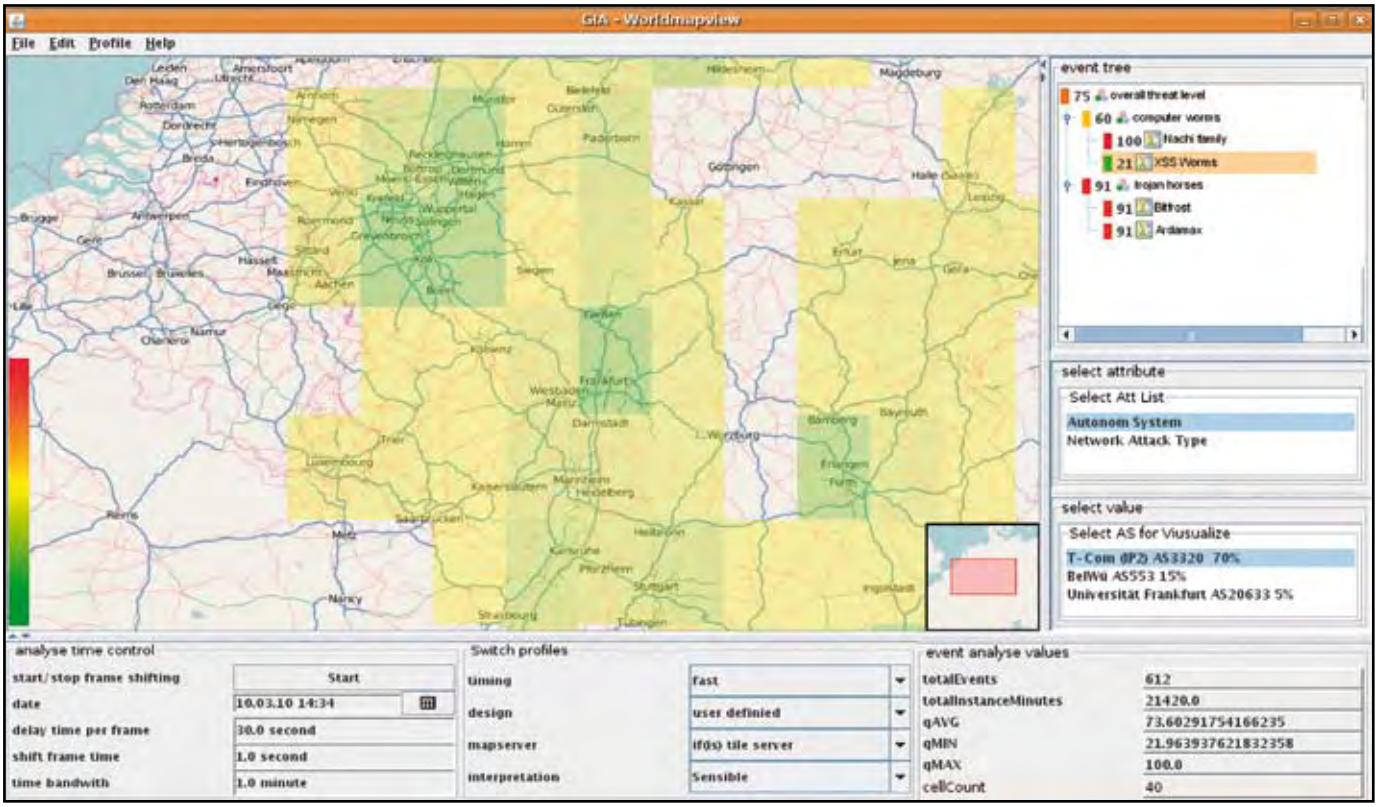
Um Malware und Netzangriffe in Zukunft noch besser erkennen und schneller reagieren zu können, haben Mitarbeiter vom Institut für Internet-Sicherheit ein spezielles Auswertungssystem entwickelt. Dieses System dient zur Erfassung und Visualisierung des aktuellen und vergangenen von Malware und Netzangriffen ausgehenden Gefahrenpotenzials. Über eine für den Anwender dargestellte Weltkarte kann die Bedrohungslage im World Wide Web auf einen Blick erschlossen werden. Eine interaktive Weltkarte ermöglicht dem Anwender sowohl eine globale Darstellung der Gefährdung über verschiedene Ländergrenzen hinweg sowie die Möglichkeit, auch lokale Analysen auf Städte-Ebene durchzuführen. Erfasste Informationen können im weiteren Verlauf verwendet werden, um Warnmeldungen zu generieren, aktuelle Trends zu erkennen oder sicherheitsrelevante Einstellungen zukünftig automatisch zur Optimierung der Sicherheitssoftware vorzunehmen.

Warum brauchen wir eine globale Sicht auf die Bedrohungen im WWW?

Die Auftrittshäufigkeit sowie die verschiedenen Arten von Malware (wie Viren, Würmer und Trojaner) nehmen seit geraumer Zeit stark zu. Das liegt auch an den optimierten Verbreitungsstrategien der Schädlinge. Es gibt viele Schutzmaßnahmen, mit deren Hilfe das Risiko, von diesen Gefahren betroffen zu werden, minimiert werden kann. Gerade bei der klassischen Virenbekämpfung werden operative Maßnahmen zum Schutz des Systems meist direkt an dem physikalischen Rechner durchgeführt. Insbesondere handelt es sich bei diesen lokal installierten Sicherheitsanwendungen um Antivirenprogramme, Desktop-Firewallsysteme und lokale Spam-Filter.

Diese Sicherheitsanwendungen stellen meist die letzte Barriere vor einem sicheren Befall mit Schadsoftware dar. Das vom Institut für Internet-Sicherheit entwickelte globale Instanzen-Auswertungssystem (GIA) kann über eine anonyme Messung der Ereignisse solcher Sicherheitsanwendungen Rückschlüsse auf die aktuell ausgehende Gefährdung ziehen. Ein Beispiel dafür ist ein versuchter Virenangriff, der vom System erfolgreich abgewehrt wurde. Die gewonnenen Informationen werden dem Anwender des Auswertungssystems auf einer interaktiven Weltkarte für weitere Analysen bereitgestellt. Gewonnene Forschungsergebnisse über die aktuellen Trends von Malware-Aufkommen können langfristig in neue Sicherheitsprodukte einfließen, um besser und zielgerichteter gegen die Bedrohungen vorgehen zu können.

Abbildung 1: Anwendungsoberfläche des Auswertungssystems



Wie kann eine globale Sicht auf das Gefährdungspotenzial erzielt werden?

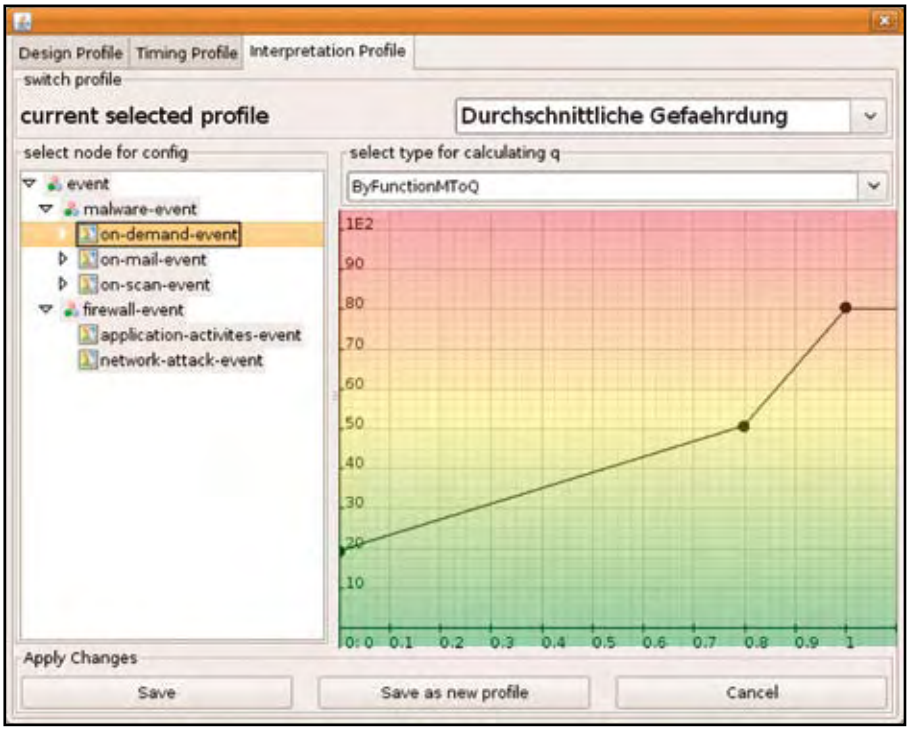
Moderne Antivirensoftware mit aktuellen Signaturen verfügt meist über eine hohe Erkennungsrate von mehr als 95%. Somit ist davon auszugehen dass die meisten Malware-Angriffe auf Systeme mit installierter aktueller Antivirensoftware erkannt werden. Wären diese Rechner nicht von den installierten Sicherheitslösungen geschützt, würden sämtliche Angriffe zu einem Befall des Systems führen.Tritt in einer Region eine ungewöhnlich hohe Anzahl von erkannten Angriffen auf, ist davon auszugehen, dass gleichartige, ungeschützte Systeme in dieser Region unmittelbar von den Schädlingen betroffen sind. Das Auswertungssystem erfasst die erkannten Malware-Angriffe und wertet diese zu einem Gefährdungspotenzial aus.

Zu diesem Zweck werden verschiedene Ereignisse, über verhinderte Angriffe, vom System logisch in eine Baumstruktur gegliedert. Die Gliederung kann je nach Einstellung sowohl nach Art der erfassten Software wie auch nach konkreten Familien von Schadsoftware erfolgen. Für jede dieser Kategorien kann der Analyst eine Funktion angeben, welche das Verhältnis zwischen der Häufigkeit des Auftretens eines solchen Ereignisses und der darzustellenden Gefährdung angibt. Abb. 2 zeigt beispielhaft eine Funktion, die die Ereignisse abbildet, die von einem On-Demand-Virenscanner gemeldet worden sind. Die X-Achse gibt hierbei die relative Häufigkeit pro Zeit und die Y-Achse die hieraus resultierende Gefährdung an.

Die resultierende Gefährdung aus einer erkannten Angriffsart kann sich auch aus den berechneten Bedrohungen der Unterarten zusammensetzen. Auf welche Art die Gefährdung berechnet wird, wird mittels eines kleinen Symbols im Anschluss an den Namen der Angriffsart dargestellt.

Die Gefährdung, die in dem betrachteten Zeitraum von den verschiedenen Bedrohungsarten ausgeht, wird innerhalb einer interaktiven Weltkarte visualisiert. Diese ermöglicht mit Hilfe einer freien Navigation und Zoomfunktionalität sowohl lokale wie auch globale Auswertungen. Die jeweilige Gefährdung einer Region wird über farbige Flächen auf der Karte dargestellt, die sich automatisch an die jeweilige Zoomstufe anpassen. Grüne Bereiche weisen eine geringe, gelbe eine mittlere und rote eine hohe Gefährdung auf. Das verwendete Kartenmaterial, welches zum Rendern der virtuellen Karte verwendet wird, kann vom Anwender nach eigenen Bedürfnissen angepasst werden. Standardmäßig wird die freie Weltkarte von OpenStreetMap zur Darstellung der Weltkarte verwendet. Die OpenStreetMap-Community bietet einerseits einen Dienst zur Verwendung der eigenen zentralen Weltkarte, andererseits auch die Weitergabe aller gesammelten Rohdaten zur Generierung von eigenem Kartenmaterialien an. Für das Auswertungssystem können somit spezielle Karten gerendert werden, die vom Detaillierungsgrad und den darzustellenden Objekten genau auf die Anforderungen des GIAs ausgelegt sind. Grünflächen wie Wälder und Bäume sollte zum Beispiel nicht farblich auf der Weltkarte dargestellt werden, da sonst die gefärbten Flächen der Visualisierung nur schlecht oder gar nicht erkannt werden können.

Abbildung 2: Die zu visualisierende Gefährdung kann frei als Funktion zur Auftrittshäufigkeit einer Angriffsart definiert werden



Wie funktioniert die Trenderkennung?

Über die Zeit-Steuerung lässt sich der zu betrachtende Zeitraum der Analyse festlegen. Über diese Konfiguration ist es sowohl möglich, die aktuellen 5 Minuten in Echtzeit wie auch den gesamten ersten Monat des letzten Jahres zu betrachten. Die dargestellte Gefährdung steht immer im Verhältnis zur dargestellten Zeit, so dass die Werte der 5-Minuten-Messung durchaus mit denen der Monats-Betrachtung verglichen werden können. Eine Animation über die Zeit ist ebenfalls einstellbar. Bei Aktivierung des Startbuttons (siehe Abb. 1. unten links) schreitet der zu visualisierende Zeitraum nach einem definierten Intervall um eine bestimmte Zeiteinheit voran. Ähnlich wie die animierte Darstellung von Hochs und Tiefs in Wetterfilmen werden Änderungen über die Zeit auf der Weltkarte auch in bewegten Bildern dargestellt. Innerhalb weniger Augenblicke kann so der geographische Verlauf der Verbreitung einer ganzen Viren-Familie intuitiv verständlich erkannt werden.

Welchen Mehrwert bringt die Messung für den Anwender der Sicherheitslösungen?

Das System wird zur Zeit weiterentwickelt, um zukünftig dem Anwender der Sicherheitsanwendungen aktuelle Tipps zur Optimierung der eigenen Sicherheitsstruktur zu geben. Zum Beispiel könnte bei akuter Gefahr durch einen Zero-Day-Exploit dem Anwender dazu geraten werden, die Heuristik und Verhaltenserkennung der verwendeten Antiviren-Lösung höher zu setzen. Sobald Signaturen gegen diese akute Gefahr ausgeteilt werden, könnte der Anwender die Einstellung wieder zurücksetzen.

Können verschiedene Einstellungen zwischen Experten ausgetauscht werden?

Die Auswertungssoftware bietet Sicherheitsexperten je nach eigenem Schwerpunkt ein hohes Maß an Freiheiten bei der Gestaltung von eigenen Analysen. Alle Konfigurationen liegen im XML-Format vor und können beliebig zwischen den Benutzern des Systems ausgetauscht und verglichen werden. Somit besteht die Möglichkeit, gemeinsam eine geeignete Interpretation des Gefahrenpotenzials von Ereignissen zur ständigen Optimierung zu erarbeiten.

Alle Einstellungen der Software sind in verschiedene Profile untergliedert. Jedes Profil bietet die Möglichkeit, Konfigurationen unabhängig von den anderen zu speichern und zu verwalteten.

Der Benutzer ist in der Lage, verschiedene Sichten durch „Mixen" seiner vorhandenen Profile zu generieren. So kann der Benutzer mit jeweils zwei Klicks den dargestellten Zeitbereich, die Funktionen zur Berechnung des Gefahrenpotenzials (siehe Abb. 2), die zu verwendende Weltkarte sowie die Darstellung der Visualisierung ändern. Die Profileinstellungen werden in Abb. 1 unter der Weltkarte dargestellt.

Wie können Daten von verschiedenen Sicherheitslösungen erfasst werden?

Abb. 3 zeigt die beteiligten Komponenten des Systems. Auf der linken Seite wird ein Arbeitsrechner (Client), auf dem verschiedene Sicherheitsanwendungen (Instanzen) installiert sind, stellvertretend für viele Clients dargestellt. Auf diesem befindet sich eine Client-Applikation, die als Schnittstelle zwischen den verschiedenen Instanzen (lokale Sicherheitslösungen) und dem Server des Auswertungssystems dient. Diese Anwendung kann sowohl als eigenständige Variante oder aber direkt innerhalb der Sicherheitslösung implementiert sein. Zur Erfassung der Messdaten greift der Client auf eine instanzabhängige Schnittstelle der jeweiligen Sicherheitslösung zu. Hierbei kann es sich um einen passiven Zugriff auf Logdateien oder um eine aktive Kommunikation mit den beteiligten Sicherheitslösungen handeln. Das System ist somit in der Lage, Informationen von verschiedenen Herstellern zu erfassen und zu analysieren. Über einen Webservice findet der sichere und anonyme Informationsversand vom Client zum Server statt. Der Webservice definiert die Informationsstruktur der auszutauschenden Daten. Die Schnittstelle ist so flexibel, dass das Auswertungssystem auch Verwendung in Bereichen finden kann, die außerhalb der Messung und Auswertung von Sicherheitsanwendungen liegt. Prinzipiell können alle Ereignisse mit einem Zeit- und einem Ortsbezug vom System verarbeitet werden.

Nachdem die Daten über aufgetretene Ereignisse zentral an die Datenbank des Servers versendet wurden, kann diese Wissensdatenbank zur Analyse der Daten von verschiedenen Auswertungssystemen genutzt werden.

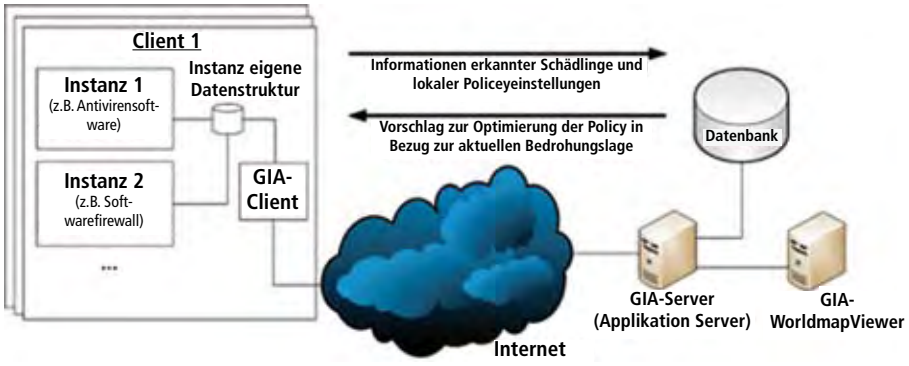
Fazit

Das am Institut für Internet-Sicherheit entwickelte globale Instanzen-Auswertungssystem ist als flexibles Ereigniskorrelationssystem zu sehen, welches besonders auf die effiziente Darstellung von Orts- und Zeit-bezogenen Informationen ausgelegt ist. Bei den zu erfassenden Datensätzen handelt es sich ausschließlich um anonyme nicht personenbezogene Informationen.

Zurzeit findet das System sein Einsatzgebiet in der Erfassung und Analyse von potenziellen Malware-Angriffen. Informationen über besonders gefährdete Regionen können nach einer anschließenden Ursachenforschung direkt in die Entscheidungsfindung konkreter Aktionen einfließen. So könnte zum Beispiel die gezielte Sensibilisierung der Bevölkerung einer Region oder die Aufstockung der Sicherheitsmaßnahmen, die ein bestimmter ISP zum Schutze seine Kunden aufbringt, als effiziente Maßnahme zur Erhöhung der Sicherheit identifiziert werden. Um möglichst aussagekräftige Ergebnisse zu liefern, sollte das System Informationen von möglichst vielen verschiedenen Sicherheitslösungen erfassen. Den Anbietern dieser Lösungen bietet das Auswertungssystem zusätzlich Informationen über die Verbreitung und Nutzung der eigenen Software.

Das System wird zur Zeit erweitert, um zukünftig dem Anwender von Sicherheitslösungen eine Hilfestellung zur Optimierung der eigenen Konfigurationseinstellungen zu bieten. ■

Abbildung 3: Architektur des Auswertungssystems



Prof. Dr. Norbert Pohlmann
Informatikprofessor für Verteilte Systeme und Informationssicherheit, Leiter des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen (www.internet-sicherheit.de)

Andreas Schnapp
ist wissenschaftlicher Mitarbeiter des Instituts für Internet-Sicherheit im Forschungsschwerpunkt Botnetze und Websecurity