

Datenschutzkonforme Kommunikationsanalyse zum Schutz der IT-Infrastruktur

Nahezu jedes Unternehmen ist bereits schon einmal mit Hackerangriffen und den mehr oder minder gravierenden Folgen konfrontiert gewesen. Eine neue Methode sich gegen diese Angriffe zu wappnen bietet das Internet-Analyse-System. Durch die gezielte Überwachung der Datenströme im Internet soll zukünftig die Reaktionszeit und somit der Schutz des Internetverkehrs verbessert werden.

Mittwochmorgen, es ist 7:30 Uhr. Heinrich M. ist auf dem Weg zu seinem Arbeitsplatz. Er ist im Auto unterwegs, doch benutzt er heute ausnahmsweise nicht die Autobahn, sondern die Schnellstraße. Heinrich M. hat nämlich heute Morgen, bevor er zu seiner Anfahrt startete, im Radio gehört, dass es auf seiner Autobahn aufgrund von kleinen Reparaturarbeiten zum Stau kommt. Herr M. freut sich, denn über die Bundesstraße schafft er es, trotz des Staus auf der Autobahn pünktlich zur Arbeit zu kommen.



Abbildung 1: Stau auf der Autobahn

Um 8:15 Uhr kommt Herr M. an seinem Arbeitsplatz an. Er schaltet den Computer an, loggt sich ein und startet seinen Internet-Browser. Aber er bekommt nur eine Fehlermeldung. Auch nach dem zweiten und dritten Versuch wird keine Verbindung aufgebaut. Herr M. ärgert sich!

Den Stau konnte Herr M. einfach umgehen, weil er vorgewarnt wurde. Ein ausgeklügeltes Überwachungssystem kontrolliert die Hauptverkehrsadern und schickt Warnmeldungen an die entsprechenden Stellen, um Verkehrsumleitungen zu starten und um ein größeres Verkehrschaos zu vermeiden.

Das Internet-Analyse-System, welches zurzeit am Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen in Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik entwickelt wird, übernimmt genau diese Aufgabe auf den Datenbahnen des Internets. An ausgesuchten Knotenpunkten und Hauptschlagadern werden Sonden installiert, die den Infor-

mationsfluss beobachten, analysieren und auswerten. Kommt es zu Anomalien, beispielsweise zu erhöhten Datenmengen durch gezielte Hackerangriffe, schlägt das Internet-Analyse-System Alarm und Gegenmaßnahmen können eingeleitet werden. Somit wird eine globale Sicht auf das Internet erreicht, ähnlich einem Hubschrauber, der über der Autobahn kreist.

Die Messwerte des Internet-Analyse-Systems sind dabei datenschutzrechtlich absolut unbedenklich. Es werden zum Beispiel keine IP-Adressen erfasst. Zusätzlich werden die erfassten Daten ohne Zusammenhang untereinander gespeichert. Beobachtet werden vor allem die anonymisierten Headerdaten der Protokolle auf verschiedenen Netzebenen. Diese Daten werden gesammelt, kategorisiert und grafisch übersichtlich dargestellt. Einzelne Datensätze sind nicht erkennbar, Anomalien werden über die Häufigkeit von bestimmten Parametern erkannt.

Einsatz des Internet-Analyse-System

Das Internet-Analyse-System setzt Sonden ein, die den Netzwerkverkehr an Kommunikationsleitungen unterschiedlicher Netze passiv abgreifen und Kommunikationsparameter auf verschiedenen Kommunikationsebenen zählen. In einem Auswertungssystem werden die Kommunikationsparameter unter verschiedenen Gesichtspunkten ausgewertet. Ein Client zeigt die gesammelten Daten übersichtlich an.

Die Aufgaben des Internet-Analyse-Systems lassen sich in die Analyse von lokalen Kommunikationsdaten in definierten Teilnetzen des Internets und die Erstellung einer globalen Sichtweise auf das Internet durch die Zusammenführung der vielen lokalen Sichten aufteilen.

Die Funktionen des Internet-Analyse-Systems erstrecken sich über die vier Teilbereiche Musterbildung, Beschreibung des Ist-Zustandes, Alarmierung und Prognostizierung.

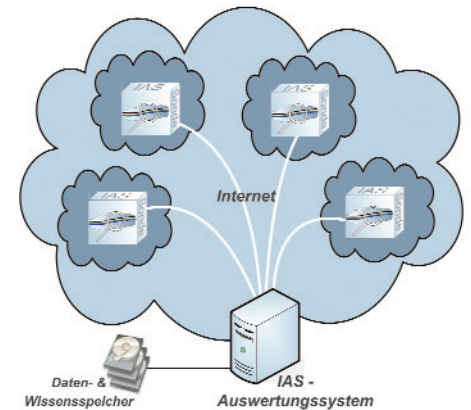


Abbildung 2: Internet-Analyse-System

Durch die Musterbildung soll erreicht werden, dass durch eine umfangreiche Analyse des Internetverkehrs Zusammenhänge und Technologietrends erkannt werden können, die eine unterschiedliche Sichtweise auf das Internet ermöglichen. Auf der Grundlage dieser Wissensbasis werden in aktuellen Messwerten Anomalien gesucht und die Ursachen für die Zustandsänderungen analysiert und interpretiert. Dabei ist es wichtig herauszufinden, ob die Zustandsanomalien natürlichen Ursprungs sind, wie beispielsweise durch den Einsatz einer neuen Technologie, oder ob ein mutwilliger Angriff zu Grunde liegt. Falls eine mutwillige Attacke vorliegt, werden die Muster identifiziert, die den Angriff charakterisieren.

Durch die Identifizierung dieser Muster kann bei einem zukünftigen Auftreten der Attacke eine Warnmeldung generiert werden, die es erlaubt, schnell und angemessen zu reagieren.

Die Darstellung des Internet-Zustands, ähnlich einer Wetter- oder Staukarte, ist eine weitere wichtige Funktion des Systems. Nur so kann eine globale Sicht gewährleistet werden. In der Entwicklung befinden sich Darstellungen, die es erlauben, die wichtigsten Parameter auf einen Blick zu erkennen.

Durch die Untersuchung und Analyse der berechneten Profile, Technologietrends, Zusammenhänge und Muster wird es durch

einen Evolutionsprozess der gewonnenen Ergebnisse möglich sein, Prognosen über Zustandsänderungen des Internets zu treffen. Auf diese Weise können Angriffe und wichtige Veränderungen bereits frühzeitig erkannt und die Schadenswirkung prognostiziert werden [2].

Prinzip der Rohdatenerfassung

Abbildung 3 verdeutlicht das Prinzip der Rohdatenerfassung durch die Sonden. Sie gliedert sich in drei Teile. Links befindet sich schematisch das Internet.

Es sind Pakete dreier unterschiedlicher An-

wird sofort nach der Kommunikationsparameter-Auswertung physikalisch, irreversibel und spurlos von der Sonde gelöscht [2]. Eine Wiederherstellung des Kontexts eines Paketes oder auch nur eines Kommunikationsparameters ist weder möglich, noch notwendig. In konfigurierbaren Zeitabständen können die gesammelten Zählerstände der Sonden als Rohdaten an das Rohdaten-Transfer-System übertragen werden. Hierbei handelt es sich ausschließlich um vollständig anonyme Informationen.

Das Rohdaten-Transfer-System fungiert als Server, mit dem sich die Sonden verbinden

können, um ihre Rohdaten für einen definierten Zeitraum zu übertragen. Es handelt sich hier um eine unidirektionale Verbindungsmöglichkeit. Das bedeutet, ein Verbindungsaufbau ist nur von der Sonden-Seite aus möglich. Eine

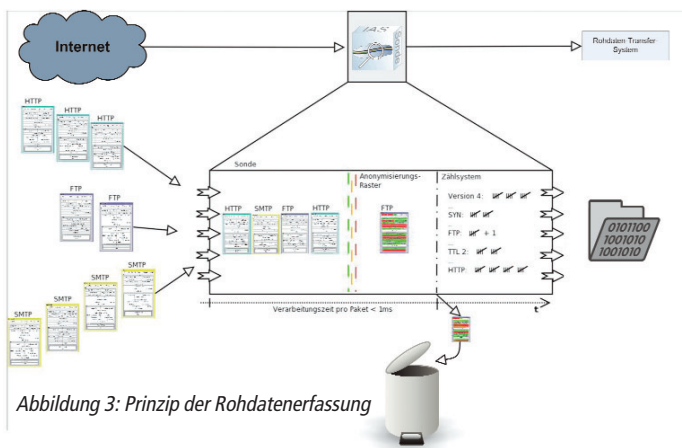


Abbildung 3: Prinzip der Rohdatenerfassung

wendungsitzungen dargestellt. Zusammengehörige HTTP-Pakete, eine FTP-Sitzung und eine SMTP-Sitzung. In der Mitte der Abb. 3 befindet sich die Sonde. Die Pakete der drei Anwendungen werden in ihrer zufälligen Reihenfolge nacheinander von der Sonde passiv abgegriffen und ausgewertet. Das abgegriffene Paket wird durch mehrere Analyseklassen geschleust, die jeweils für ein bestimmtes Protokoll zuständig sind. Es werden fest definierte Kommunikationsparameter in den Protokoll-Headern ausgewertet, die nicht datenschutzrechtlich relevant sind. Je nachdem, wie die Headerinformationen des Paketes ausgefüllt sind, werden die im Zählsystem zugeordneten Zähler erhöht. Ähnlich einer Strichliste wird die Häufigkeit bestimmter Headerinformationen festgehalten. Beispielsweise wird in der Abb. 3 die Registrierung des FTP-Paketes durch die Inkrementierung des FTP-Zählers festgehalten. Bei den Rohdaten handelt es sich also um Aggregate von Zählern, das heißt, um Zähler von aufgetretenen Kommunikationsparametern auf den verschiedenen Kommunikationsebenen über einen definierten Zeitraum. Das Paket, in Abb. 3 ein FTP-Paket,

Sonde kann die Rohdaten an ein oder mehrere Rohdaten-Transfer-Systeme übertragen. Beispiel einer typischen Konfiguration ist, dass alle 5 Minuten die Rohdaten zum Beispiel in einer Größe von 40 KByte an das eigene und ein zentrales Rohdaten-Transfer-System gesendet werden.

Da die Rohdaten nur eine statistische Formulierung der eigentlichen Kommunikationsdaten sind, würde es auch ausreichen, wenn nicht jedes Paket betrachtet wird, sondern beispielsweise nur jedes zehnte Paket. Dieser Aspekt kann bei sehr hohen Kommunikationsdatenraten eine pragmatische Lösung sein, ohne dass dabei – statistisch gesehen – ein anderes Ergebnis generiert werden würde.

Nutzen des Internet-Analyse-Systems

Sondenbetreiber mit eigenem Auswertungssystem werden bei auftretenden Problemen vom Internet-Analyse-System informiert und können die umfangreichen Hilfsmittel des Systems bei den Analysen von Problemen nutzen. Eine übersichtliche Darstellung des aktuellen Zustandes des ei-

genen Systems und ein aufschlussreiches Reportingsystem stellen die Basis für einen zuverlässigen Netzbetrieb dar.

Ist das eigene System Bestandteil eines zentralen Auswertungssystems, werden Probleme bei einem Teilnehmer rechtzeitig weitergegeben, so dass alle frühzeitig Gegenmaßnahmen ergreifen können.

Ausblick

Das Internet-Analyse-System ist in der Lage, kontinuierlich statistische Daten zu sammeln, die den Internetverkehr widerspiegeln. Anhand dieser Daten können Muster, Trends und weitere Informationen abgeleitet werden.

Durch die Analyse der Ergebnisse unterschiedlicher Sonden ist es möglich, eine globale Sichtweise des Internets darzustellen und Warnstufen im Fall von Problemen, wie beispielsweise infrastrukturellen Ausfällen oder Angriffen zu definieren. Weitere Analysen der Rohdaten erlauben die Prognosen von Trends in der Benutzung von Protokollen, Netzwerkdiensten und Angriffen.

Für ein umfangreiches IT-Frühwarnsystem lässt sich das Internet-Analyse-System beispielsweise noch mit einem Verfügbarkeitssystem und Logdaten-Auswertungssystem erweitern.

Es gilt also, dieses System flexibel und flächendeckend einzusetzen, damit genau wie im Stau auf der Autobahn, eine globale Sicht auf die Strukturen und Gefahren des Internets möglich wird.

Weitere Informationen: Institut für Internet-Sicherheit

<https://www.internet-sicherheit.de/internet-fruehwarn.html>

Prof. Dr. Norbert Pohlmann, norbert.pohlmann@informatik.fh-gelsenkirchen.de
Dipl.-Inform. (FH) Marcus Proest, marcus.proest@internet-sicherheit.de
Institut für Internet-Sicherheit, Fachhochschule Gelsenkirchen, Neidenburger Str. 43, 45877 Gelsenkirchen, www.internet-sicherheit.de

Literatur

[1] S. Dierichs, N. Pohlmann: „Netz-Deutschland“, iX - Magazin für professionelle Informationstechnik, Heise-Verlag, 12/2005.

[2] N. Pohlmann, M. Proest: „Messverteilung: Die globale Sicht auf das Internet“, iX - Magazin für professionelle Informationstechnik, Heise-Verlag, 2/2006.