Architektur zur mehrstufigen Angriffserkennung in Hochgeschwindigkeits-Backbone-Netzen

Mario Golling, Robert Koch und Lars Stiemert
Munich Network Management Team (MNM-Team)
Universität der Bundeswehr München
Werner-Heisenberg-Weg 39
D-85577 Neubiberg
{mario.golling, robert.koch, lars.stiemert}@unibw.de

Abstract: Die globale Vernetzung und die Durchdringung des alltäglichen Lebens durch Informations- und Kommunikationstechnologien, sowie die zunehmende Anzahl von Angriffen, die bisweilen auch unter Beteiligung ahnungsloser Nutzer durchgeführt werden (Bot-Netze) führen dazu, dass Angriffe auf IT-Infrastrukturen längst keine zu vernachlässigende Begleiterscheinung des Internets mehr sind. Angriffe wie der auf das Spamhaus Project, das 2013 durch einen Distributed Denial of Service Angriff mit mehr als 300 Gbps attackiert wurde und in der Konsequenz auch einige Backbone Provider an die Grenze Ihrer Leistungsfähigkeit brachte, zeigen eindrücklich, dass Angriffe auch auf Backbone Provider große Auswirkungen haben können. Systeme zur Angriffserkennung arbeiten historisch betrachtet zumeist auf Basis sogenannter Deep Packet Inspection, bei welcher der Paketinhalt auf das Vorhandensein spezieller Muster überprüft wird. Dies ermöglicht zwar detaillierte Analysen, ist aber aufgrund der mangelnden Skalierbarkeit in Zeiten immer schneller werdender Anbindungen, gerade für Backbone-Provider, finanziell wie auch technisch nicht praktikabel. Spezifische rechtliche Beschränkungen verschärfen diese Problematik zusätzlich. Die vorliegende Publikation stellt deswegen einen mehrstufigen Ansatz zur Angriffserkennung speziell für Backbone Provider vor, bei welchem mehrere Verfahren wie unter anderem Flow-basierte Angriffserkennung, Protokoll-basierte Angriffserkennung, Deep Packet Inspection und Geolokalisation kombiniert werden.

1 Einleitung und Problemstellung

Die Informations- und Kommunikationstechnik (IKT) hat sich zu einem wesentlichen Bestandteil des alltäglichen Lebens entwickelt. Die globale Vernetzung und die stetig voranschreitende Durchdringung des privaten wie öffentlichen Sektors eröffnet ungeahnte Möglichkeiten und fördert Innovationen ebenso wie die Wirtschaft als Ganzes. Einhergehend mit dem Bedeutungszuwachs des Internets nehmen allerdings auch die Anzahl der Angriffe in den letzten Jahren stetig zu - sowohl in quantitativer, als auch in qualitativer Ausprägung. Um den zunehmenden Bedrohungen entgegenzuwirken haben sich zur Detektion von Angriffen zahlreiche Lösungen etabliert, wie insbesondere Systeme

zur Angriffserkennung (*engl. Intrusion Detection Systeme; IDSs*). Aktuelle Systeme arbeiten hier vorwiegend nach dem Prinzip der Deep Packet Inspektion (DPI), bei der eine Angriffserkennung durch Analyse des kompletten Paketinhaltes (auf das Vorhandensein typischer Indikatoren) stattfindet. Während sich DPI-basierte Systeme aufgrund ihrer im Vergleich zu verhaltensbasierten Systemen besseren Fehlalarmraten, sowie der detaillierten Untersuchungsmöglichkeiten des Datenverkehrs als Standard-Sicherheitssysteme in Access Netzen etabliert haben, ist ihr Einsatz in Netzen mit höheren Verbindungsgeschwindigkeiten (größer 10 Gigabit) mit sehr hohen Kosten verbunden bzw. technisch schwer realisierbar. Zusätzlich bestehen bei DPI zahlreiche rechtliche Bedenken hinsichtlich der Privatsphäre und des Datenschutzes, ebenso wie der juristischen Zuständigkeit.

Insbesondere wenn Angriffe verteilt durchgeführt werden, kann ihr Gesamtvolumen die jeweiligen Systeme überlasten. So wurde zum Beispiel das Spamhaus-Projekt von Distributed Denial of Service (DDoS)-Angriffen Anfang 2013 mit mehr als 300 Gbps Verkehr belegt - genug, um einzelne Knotenpunkte des Internets zu überlasten. Zusätzlich zu DDoS-Attacken stellen v.a. Würmer und Botnetze besondere Herausforderungen für Backbone-Provider dar, da auch sie dazu neigen, eine große Menge an Ressourcen zu blockieren [Arb]. Im Rahmen dieser Publikation wird der Begriff Backbone Provider verwendet, um Netze mit Geschwindigkeiten höher als 10 Gbps und ohne eine Verbindung zu spezifischen Endsystemen zu bezeichnen. Die Kenntnis des geographischen Ursprungs eines Angriffes kann heutzutage von großer Bedeutung sein. So hat der Sicherheitsdienstleister Mandiant kürzlich im Rahmen einer Studie festgestellt, dass ein großer Teil aller Angriffe auf Behörden der USA auf den näheren Umkreis eines einzigen Gebäudes in Shanghai/China einschränkbar ist [Man13].

Dieser Problematik Rechnung tragend wird im Rahmen dieser Publikation ein mehrstufiger Ansatz zur Angriffserkennung speziell für Backbone-Provider vorgestellt, indem mehrere Verfahren wie unter anderem Flow-basierte Angriffserkennung, Protokoll-basierte Angriffserkennung, DPI und Geolokalisation kombiniert werden.

Hierzu wird in Abschnitt 2 ein Überblick über vorhandene Verfahren - sowohl im Bereich der Angriffserkennung, als auch im Bereich der Geolokalisation gegeben. Anschließend wird in den Abschnitten 3 und 4 die mehrstufige Architektur sowie die prototypische Implementierung vorgestellt. Im letzten Teil dieser Arbeit erfolgt ein kurzes Resümee sowie ein Ausblick auf zukünftige Arbeiten.

2 Stand der Wissenschaft und Technik

Im folgenden Abschnitt erfolgt zunächst ein kurzer Überblick über Verfahren zur Angriffserkennung. Analog dazu werden danach im zweiten Teil vorhandene Ansätze zur Geolokalisation vorgestellt und es wird kurz darauf eingegangen, inwiefern diese vorteilhaft in den Prozess der Angriffserkennung integriert werden können.

2.1 Angriffserkennung

Gemäß des National Institute of Standards and Technology (NIST) wird Angriffserkennung respektive Intrusion Detection allgemein als Prozess zur Überwachung und Analyse von Ereignissen in Netzen oder Computersystemen verstanden, bei dem Vorkommnisse auf abweichende Verhaltensweisen hinsichtlich der Verletzung von Sicherheits-, Nutzungsrichtlinien oder -praktiken untersucht werden [SM10].

2.1.1 Vorhandene Ansätze zur Angriffserkennung

Im Bereich der Angriffserkennung haben sich über die Jahre verschiedene Formen von IDSs herausgebildet. Eine der grundlegenden Unterscheidungen hierbei ist die Differenzierung in hostbasierte Systeme und solche Systeme, bei denen die Erkennung nicht auf dem Computersystem erfolgt, sondern mittels Sensoren im Netz. Netzbasierte IDS (NIDS) lassen sich ebenfalls noch weiter unterteilen und werden im Folgenden basierend auf der ISO/OSI-Ebene, auf der die Angriffserkennung durchgeführt wird, kurz vorgestellt:

Angriffserkennung auf Basis der Auswertung des Paketinhaltes: Der bereits vorgestellte DPI-Ansatz stellt den gebräuchlichsten Vertreter von NIDSs dar. Charakteristisch für DPI ist, dass hier der gesamte Inhalt jedes Paket auf das Vorhandensein von Auffälligkeiten untersucht wird. In der Praxis erfolgt hierbei im Regelfall ein Abgleich der zu untersuchenden Datenpakete zu vorher gewonnenen Signaturen.

Angriffserkennung unter Auswertung statistischer, bzw. protokollspezifischer Informationen: Neben der DPI-basierten Angriffserkennung auf Schicht 7 des ISO/OSI-Referenzmodells kann aber auch eine Auswertung auf Schicht 4, d.h. eine Auswertung des Nachrichtenkopfs (*engl. Header*) erfolgen. Aufgrund der Tatsache, dass nur Header untersucht werden, sind diese Ansätze auch in der Lage, hohe Datenraten zu verarbeiten. Hierbei zeichnen sich *Protokoll-basierte IDSs* dadurch aus, dass sie das dynamische Verhalten und den Zustand des Protokolls bzgl. des durch den Standard vorgesehenen Ablaufs hin untersuchen. Problematisch hierbei ist, dass Standards oftmals nicht alle Aspekte des Protokollablaufs festlegen (bspw. Start von Sequenznummern - zufallsbasierter Anfangswert oder Null, etc.) und Hersteller sich bei der Implementierung nicht immer komplett an den Standard halten; dies hat maßgeblichen Einfluss auf die Fehlalarmraten eines entsprechenden IDS' und kann nur durch die Untersuchung und Berücksichtigung der spezifischen Abweichungen verbessert werden. *Verhaltensbasierte IDSs* hingegen beruhen auf Modellen wie bspw. dem Satz von Bayes, um bösartige Pakete im Netz zu identifizieren. Als Folge sind statistische IDS in der Lage, ihr Systemverhalten dynamisch anzupassen und damit ihre eigene Regeln zu modifizieren. Statistische Auswertungen sind grundsätzlich sowohl auf Schicht 4, als auch auf Schicht 7 des ISO/OSI-Modell möglich, wobei im Zuge dieser Arbeit der Begriff nur für Schicht 4-basierte Systeme Verwendung findet.

Angriffserkennung auf Basis aggregierter Header-Informationen: Anstelle der Auswertung von *allen* Headern kann eine Angriffserkennung auch auf Basis aggregierter Verkehrsdaten (Flows) erfolgen [SSS+10]. RFC 7011 [CTA13] definiert einen Flow als Menge von IP Paketen mit gemeinsamen Eigenschaften, die innerhalb eines bestimmten Zeitrahmens erfasst werden. Diese Art der Auswertung ermöglicht eine Analyse, welche rechtliche Bedenken weitgehend ausräumt, da die eigentlichen Paketinhalte nicht herangezogen werden. Weiterhin ist aufgrund der reduzierten Datenmenge der Flows eine sehr effiziente Auswertung möglich; andererseits müssen die Flows zu den Paketströmen erst generiert werden, was eine Verzögerung zu anderen Detektionsverfahren mit sich bringt. Während bei DPI die Inhalte sofort betrachtet werden, muss für die Generierung der Flow-Daten erst eine bestimmte Anzahl an Paketen übertragen und berücksichtigt werden.

Bewertung und Eignung für Backbone-Provider: Für Backbone-Provider ist eine Angriffserkennung basierend auf Flows derzeit sowohl rechtlich, als auch vom Aufwand her betrachtet die einzig praktikable Möglichkeit. Viele Backbone-Provider setzen ohnehin Flow-basierte Komponenten im Rahmen der Netzüberwachung und des -managements ein. Diese Datenquellen können direkt für die Flow-basierte Angriffskennung mit genutzt werden. Flow-basierte Angriffserkennung hat andererseits den Nachteil, dass nicht alle Arten von Angriffen und bösartigem Verhalten erkannt werden können. Folgende vier Kategorien können gut erkannt werden: (i) (Distributed) Denial of Service DDoS (ii) Netz-Scans (iii) Würmer sowie (iv) Bot-Netze [SSS+10]. Da dies jedoch genau die Gefahren sind, die einen Backbone-Provider interessieren (bspw. die Detektion eines DoS und das Ergreifen von Gegenmaßnahmen) [Arb], ist eine Flow-basierte Detektion als ausreichend zu bezeichnen.

2.2 Geolokalisation

Geolokalisation bezeichnet die Zuordnung einer logische Adresse, beispielsweise der IP eines Hosts, zu einer physikalischen respektive geografischen Position. Das Einsatzspektrum ist hierbei breit gefächert und umfasst neben zielgerichteter Werbung beziehungsweise Contentpräsentation auch die Verwendung im Rahmen der Strafverfolgung, wenn es um die juristische Zuständigkeit oder den Ursprung eines Deliktes mit dem Tatmittel Internet geht.

2.2.1 Vorhandene Ansätze zur Geolokalisation

Im Forschungsgebiet der Geolokalisation von IP-Adressen haben sich diverse Ansätze herausgebildet. Nach Endo et. al [ES10] lassen sich alle Verfahren grundsätzlich in zwei wesentliche Kategorien einordnen [KGR13b]:

Verfahren basierend auf aktiven Messungen: Die Ermittlung der möglichen geografischen Position eines Hosts erfolgt über aktive Messungen. Es findet folglich eine direkte

Interaktion mit dem Zielsystem statt. Dazu werden typischerweise Verzögerungswerte (zumeist Round Trip Times) bestimmt und daraufhin versucht, über Vergleiche mit Messungen bekannter Server-Standorte (beispielsweise Webserver oder Router), auf die Position des Zielhosts zu schließen [ZFdRD05].

Semantische Methoden: Anhand semantischer Verfahren werden standortbezogene Informationen zu einer gegebenen Adresse mit Hilfe umfangreicher Datenanalysen ermittelt. Die so erhobenen Daten können anschließend Rückschlüsse auf die tatsächliche physikalische Position des Ziels zulassen. Grundlage hierfür bilden unter anderem die Datenbestände der fünf Regional Internet Registries, sowie Geoservice-Anbieter wie Quova [HFc11]. Diese Ansätze ermöglichen Abfragen in Echtzeit und sind entsprechend für große Datenmengen geeignet. Allerdings sind die Datenbestände zumeist nicht aktuell und folglich ungenau.

Bewertung und Eignung für Backbone-Provider: Im Rahmen der im nächsten Abschnitt vorgestellten Architektur hat Geolokalisation eine hohe Bedeutung. Da, wie bereits erwähnt, einer Studie des Sicherheitsdienstleister Mandiant zufolge ein großer Teil aller Angriffe auf Behörden der USA auf den näheren Umkreis eines einzigen Gebäudes in Shanghai/China einschränkbar ist [Man13], soll Geolokalisation vergleichbar mit Greylisting in E-Mails verwendet werden, um so verdächtigen Pakete (deren Ursprung sich in räumlicher Nähe zu ähnlichen, bereits erkannten, bösartigen Paketen befindet) einen höhere Angriffswahrscheinlichkeit zuzuordnen. Da die rechtlichen Rahmenbedingungen in der Regel länderspezifisch sind, ist die Nutzung von Geolokalisationverfahren für die geografische Zuordnung eines Einbruchversuches zudem ein probates Mittel, um entsprechende (Gegen-)Maßnahmen auch vor länderspezifischen rechtlichen Besonderheiten gegeneinander abzugrenzen [KGR13a].

Bei Betrachtung der finanziellen und technischen Herausforderungen in heutigen Hochgeschwindigkeitsnetzen sind Geolokalisationsverfahren auf Basis von aktiven Messungen vor allem aufgrund des hohen Datenaufkommens nicht praktikabel einsetzbar. Obwohl widersprüchliche Angaben zur Genauigkeit von derlei Ansätze existieren, gehen jüngste Studien [HFc11] davon aus, dass eine Zuordnung auf Landesebene zu 96-98% korrekt ist. Als erweiternde Maßnahme zur Angriffserkennung, um beispielsweise den geographischen Ursprung von Angriffen zu korrelieren, liefern Geo-Datenbanken somit einen kostengünstigen und effektiven Mehrwert.

3 Architektur

Nachfolgend wird auf Basis der Erkenntnisse aus Abschnitt 2 ein mehrstufiger Ansatz zur Angriffserkennung vorgestellt (siehe Abbildung 1), welcher die Vorteile verschiedener Systeme zur Angriffserkennung wie DPI und Flow-basierter IDSs vereint, um so die Fehlalarmraten zu minimieren.

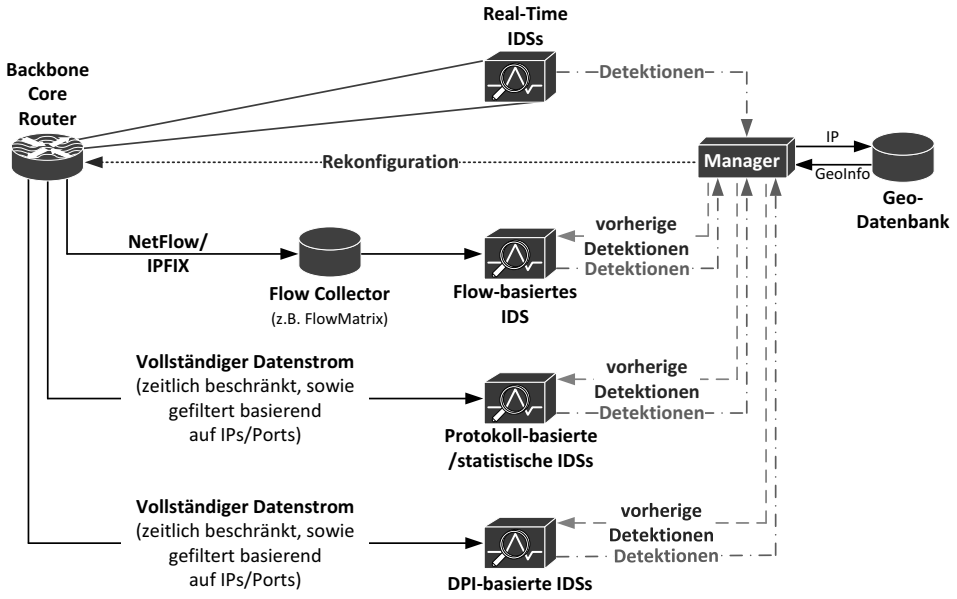

Abbildung 1: Komponenten der Architektur

Grundlegendes Prinzip: Wie in Abbildung 1 dargestellt, besteht die Architektur im Wesentlichen aus einer *Managementkomponente (Manager)*, einem *Core Router* und verschiedenen *IDSs*. Die Managementkomponente ist hierbei das Kernelement der Architektur. Sie steuert alle Interaktionen, kontrolliert die einzelnen IDSs und stellt sicher, dass diese bei Bedarf die nötigen Verkehrsdaten erhalten.

Real-Time IDS: Im Ausgangszustand wird dabei der komplette Datenstrom, der den Core Router passiert, durch ein spezielles Real-Time IDS, welches direkt auf dem Router ausgeführt wird, untersucht. Da hier kein dediziertes Gerät vorhanden ist, sondern dem Router Ressourcen „entzogen“ werden, sind nur sehr einfache Funktionen möglich. Die zentrale Idee hierbei ist, insbesondere gegen (D)DoS-Attacken zu schützen. So wurde bereits gezeigt, dass es sehr gut möglich ist, einen solchen Angriff mit den begrenzten Ressourcen eines Routers mit einer hohen Genauigkeit (selbst bei einer relativ hohen CPU-Auslastung) [HBSP13] zu erkennen. Im Falle des Erkennens eines Angriffes ist das Real-Time IDS in der Lage, selbständig den Router zu rekonfigurieren, um den Datenstrom bspw. durch eine Access Control List oder ein Sinkhole zu blockieren. Darüber hinaus wird auch der Manager unter Nutzung des “Intrusion Detection Message Exchange Formats” (IDMEF, Austauschformat) sowie der „Common Vulnerabilities and Exposures“ (CVE, standardisierte Semantik) und dem „Common Vulnerability Scoring System“ (CVSS, standardisierte Metrik) über den Vorfall informiert.

Flow-basierte IDS: Neben dem Real-Time IDS überwacht auch das Flow-basierte IDS ständig den kompletten Datenstrom des Routers. Angesichts der Tatsache, dass Flow-

Exportformate wie NetFlow und IPFIX die Verkehrsdaten in Flows aggregieren, ist eine derartige Angriffserkennung auch mit vergleichsweise geringen Ressourcen möglich. Zur einfacheren Detektion kann das Flow-basierte IDS zudem vom Manager über bereits vorhandene Detektionsergebnisse informiert werden. Obwohl dies von gegenwärtigen Systemen nicht unterstützt wird, besteht die Grundidee darin, einem IDS so viele Information wie möglich an die Hand zu geben, um so den Prozess der Angriffserkennung so zuverlässig wie möglich zu machen. Sollte das Flow-basierte IDS einen Angriff feststellen, so leitet es die Information an den Manager weiter. Dieser wertet die Information aus und kann seinerseits wiederum andere IDSs (wie protokoll-basierte oder DPI-basierte IDSs) aktivieren und über die vorangegangene Detektion beziehungsweise die Meldungen der jeweiligen IDSs entsprechend steuern und informieren. In diesem Zusammenhang dient das vorgeschaltete Real-Time IDS, (i) um Gegenmaßnahmen ohne hohe Verzögerungen durchzuführen (die Erzeugung von Flows und deren Export verzögert den Prozess der Angriffserkennung), (ii) da vor allem DoS / DDoS-Angriffe eine große Menge an Flow-Daten produzieren, welche die Flow-basierten IDS überlasten können und durch das Real-Time IDS reduziert werden können und (iii) im Regelfall insbesondere DDoS-Attacken hohe Auswirkungen auf den Betrieb des Backbone-Providers haben und deshalb effektiv verhindert werden müssen.

Übrige IDSs: Sollte der Manager eine weitergehende Analyse eines Angriffs initiieren, können die Protokoll-basierten/statistischen IDSs oder DPI-basierte IDSs aktiviert werden. Hierzu veranlasst der Manager eine Rekonfiguration des Routers, um nur den Teil des Datenverkehrs an die jeweiligen Systeme weiterzuleiten, der vorher bereits als verdächtig eingestuft wurde. Analog zu den Flow-basierten IDSs werden diese IDSs im Vorfeld auch über vorherige Alarmmeldungen informiert und melden ihre Analysen an den Manager. Wenn ein Angriff erkannt wurde, wird der Router durch den Manager angewiesen, den entsprechenden Datenverkehr zu blockieren. Sollte ein Angriff nicht bestätigt werden können, wird der Manager dafür sorgen, dass die verschiedenen IDSs (mit Ausnahme des Real-Time IDS sowie des/der Flow-basierte IDSs) den Datenverkehr für eine gewisse Zeit nicht erneut analysieren.

Zum genaueren Verständnis werden die einzelnen Schritte im Detail vorgestellt:

Gewinnung von Indizien: Sobald durch das Real-Time IDS bzw. das Flow-basierte IDS ein Indiz für einen möglichen Angriff entdeckt wurde, wird der entsprechende Datenstrom isoliert betrachtet. Da diese Untersuchung nicht auf der gesamten Nutzlast durchgeführt wird, wird die Privatsphäre der Nutzer respektiert und auf der anderen Seite ermöglicht dies die Verwendung preiswerter IDSs.

Bewertung: Basierend auf dem Alarm des Real-Time IDS, dem Flow-basierten IDS oder dem Prokollbasierten/statistischen IDS und dem entsprechenden CVE kann eine erste Einschätzung über das Ausmaß des Angriff unter Nutzung von CVSS durchgeführt werden; CVSS ist ein Industriestandard, der den Schweregrad der Schwachstellen in Computersystemen beschreibt. Ziel dieser Gewichtung ist das Herstellen einer Prioritätsreihenfolge für den Fall, dass aufgrund von Ressourcenlimitierungen nicht alle gemeldeten Angriffe im Detail untersucht werden können. Zusätzlich zu der CVSS-Gewichtung werden im Rahmen

der Architektur noch weitere (lokale) Kriterien verwendet, um die individuelle Bedrohung zu bewerten. Solche Kriterien sind beispielsweise, ob ein Angreifer in der Vergangenheit schon verdächtig war, oder ob sich das Ausmaß eines Angriffs (der derzeit untersucht wird) drastisch erhöht, bspw. bei Zunahme entsprechender Pakete, oder ob eine hohe Anzahl von ähnlichen Angriffen in der Vergangenheit beobachtet wurde. In diesem Zusammenhang wird auch Geolokalisation verwendet, was ebenfalls ein Bewertungskriterium zur Ähnlichkeit liefert. Dazu werden entsprechend Geo-Datenbanken eingesetzt. Je näher ein bereits erkanntes Indiz zu einem in der Vergangenheit erkannten Angriff ist, desto höher die Gewichtung. Geolokalisation hat hier auch noch einen zweiten Zweck: Abhängig von der Herkunft des Paketes kann ferner geprüft werden, ob evtl. ergriffenen Maßnahmen (z.B. die Anwendung von DPI) im Einklang mit den Gesetzen sind und so ein Provider nicht fälschlicherweise Gegenmaßnahmen ergreift, die für ihn juristische und vertragliche Konsequenzen nach sich ziehen.

Detaillierte Analyse: In Abhängigkeit des detektierten Angriffs und der vorangegangen Wertung können nun spezifische IDSs zur erweiterten Analyse hinzugezogen werden. Dies ist von elementarer Bedeutung, da der Backbone-Provider die Glaubwürdigkeit und Vertraulichkeit gegenüber seinen Kunden riskiert und zugleich die rechtlichen und wirtschaftlichen Konsequenzen durch blockierte oder verworfene Datenströme nicht zu vernachlässigen sind. Aus diesem Grund möchte ein Backbone-Provider sehr sicher sein, bevor er eine Entscheidung wie das Blockieren des Datenstroms trifft. Dies kann auch Bedeuten, dass ein Provider mehrere IDSs (z.B. mehrere verschiedene IDSs, wie bspw. Snort oder BRO) parallel für eine Untersuchung verwendet.

Ergebnisbewertung: Nachdem alle Untersuchungen beendet sind, erfolgt die Korrelation und Bewertung der Ergebnisse, um ein möglichst hohes Maß an Verlässlichkeit gewährleisten zu können, bevor mögliche Gegenmaßnahmen ergriffen werden. Dies ist insbesondere dann relevant, wenn mehrere IDSs zur Untersuchung verwendet wurden.

Reaktion und Gegenmaßnahmen: Der letzte Schritt ist die Einleitung einer Reaktion auf die erfolgte Detektion. Dies kann durch entsprechende Gegenmaßnahmen, wie das Verwerfen von Paketen und/oder der Rekonfiguration des Core Routers, von statten gehen. Zugleich ist eine Weitermeldung an andere Router (beziehungsweise Instanzen) und die lokale Speicherung des Vorfalls möglich.

4 Prototypische Umsetzung

Zur Evaluation der Leistungsfähigkeit der Architektur wird diese derzeit prototypisch umgesetzt. Der Großteil der Managementkomponente wird aufgrund der Performance in C realisiert; hierbei kommen Open Source Bibliotheken zum Einsatz, um die Entwicklungszeit zu verkürzen. Als Datenbankbackend kommt MySQL zum Einsatz. Durch diverse APIs können Daten wie bspw. CVE importiert werden. In diesem ersten Prototyp werden

als IDSs im Wesentlichen eine speziell für Protokollanalyse angepasste, als auch eine in der Standardkonfiguration befindliche Version von Snort verwendet. Der bereits in erster Version verfügbare Proof of Concept wird derzeit in das Labor des Institutes integriert, die ersten intensiven Tests laufen bereits. Das Institutsnetz besteht hierbei aus den sicherheitstechnisch strikt voneinander getrennten Produktiv-, Forschungs- sowie Büronetzen. Als Geolokalisationslösung kommt hier eine von uns speziell entwickelte Software zum Einsatz, welche IP Adressen auf Landesebene mit einer Genauigkeit von 99.78% erkennt (vgl. [KGR13a, KGR13b]).

Um die vorgestellte Architektur mit dem derzeitigen „State of the Art“ zu vergleichen, werden verschiedene Kriterien, wie die Genauigkeit und die Rate von False Positives, herangezogen. Dabei ist es nicht das Ziel möglichst viele Vorfälle zu detektieren, sondern die False Positives zu reduzieren.

Hierzu wird parallel zu unserer Architektur eine vergleichende Betrachtung mit „State of the Art“-Systemen durchgeführt. Die Anbindungen der einzelnen Komponenten und die zugrundeliegenden Bedingungen, wie zum Beispiel beim Export der Flows, sind in beiden Umgebungen gleich (z.B. zwei identische Cisco Catalyst 6509-E Router).

5 Zusammenfassung und Ausblick

Die globale Vernetzung und die Durchdringung des alltäglichen Lebens durch IKT führen zu einer wachsenden Zahl sicherheitstechnischer Herausforderungen, derer sich auch Backbone-Provider nicht verschließen können. Im Rahmen der vorliegenden Publikation wurde ein mehrstufiger Ansatz zur Angriffserkennung in Hochgeschwindigkeits-Backbone-Netzen vorgestellt. Dieser ermöglicht es, neben den finanziellen und technischen auch rechtliche Aspekte, beispielsweise in Bezug auf den Datenschutz sowie die Privatsphäre, zu berücksichtigen. Obwohl sich die Fähigkeit des Gesamtsystems auf die der Flow-basierenden Verfahren beschränkt, ist die Architektur gerade deswegen für Backbone-Betreiber geeignet. Denn diese Verfahren ermöglichen eine vergleichsweise kostengünstige Integration in bestehende Umgebungen und effektive Behandlung von Angriffen, die von besonderem Interesse für Backbone-Betreiber sind.

Zukünftige Arbeiten werden sich mit der Anpassung und Erweiterung der Architektur befassen, um so eine möglichst weite Verbreitung in unterschiedlichen Netzen und einer automatisierten Anpassung an diese zu ermöglichen. Hierfür sind allerdings mehr Informationen zu den technischen und rechtlichen Gegebenheiten unterschiedlicher Umgebungen von Nöten. Weitere Gedanken befassen sich mit einer noch weitergehenden Integration von Geolokalisationsmechanismen in die vorgestellte Architektur, sowie eine tiefergehenden Betrachtung (*Evaluierung*) der Abhängigkeit zwischen Detektion und Geolokalisation. Dies kann vor allem der länderspezifischen Behandlung von Vorfällen, wie auch der vorgestellten Bewertung derer zuträglich sein.

Danksagung

Diese Arbeit wurde teilweise durch Flamingo, einem Network of Excellence Projekt (ICT-318488) des 7. EU-Forschungsrahmenprogramms der europäischen Kommission, gefördert.

Literatur

[Arb] Arbor Networks. Worldwide Infrastructure Security Report - 2012 Volume VIII. `http://pages.arbornetworks.com/rs/arbor/images/WISR2012_EN.pdf`, zuletzt besucht am 14.04.2014.

[CTA13] Benoit Claise, Brian Trammell und Paul Aitken. Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information. RFC 7011 (Internet Standard), 2013.

[ES10] Patricia Takako Endo und Djamel Fawzi Hadj Sadok. Whois Based Geolocation: A Strategy to Geolocate Internet Hosts. In *Proceedings of the 2010 24th IEEE International Conference on Advanced Information Networking and Applications*, Seiten 408–413, 2010.

[HBSP13] Rick Hofstede, Vaclav Bartos, Anna Sperotto und Aiko Pras. Towards Real-Time Intrusion Detection for NetFlow and IPFIX. In *Proceedings of the 9th International Conference on Network and Service Management, CNSM'13*, Seiten 227–234, 2013.

[HFc11] B. Huffaker, M. Fomenkov und k. claffy. Geocompare: a comparison of public and commercial geolocation databases - Technical Report. Bericht, CAIDA, May 2011.

[KGR13a] Robert Koch, Mario Golling und Gabi Dreo Rodosek. Advanced Geolocation of IP Addresses. In *International Conference on Communication and Network Security (ICCNS)*, Seiten 1–10, 2013.

[KGR13b] Robert Koch, Mario Golling und Gabi Dreo Rodosek. Geolocation and Verification of IP-Addresses with Specific Focus on IPv6. In *5th International Symposium on Cyberspace Safety and Security (CSS 2013)*, Seiten 1–20. Springer, 2013.

[Man13] Mandiant. APT1 - Exposing One of China's Cyber Espionage Units, 2013. `http://intelreport.mandiant.com/`, zuletzt besucht am 14.04.2014.

[SM10] Karen Scarfone und Peter Mell. Intrusion detection and prevention systems. In *Handbook of Information and Communication Security*, Seiten 177–192. Springer, 2010.

[SSS+10] Anna Sperotto, Gregor Schaffrath, Ramin Sadre, Cristian Morariu, Aiko Pras und Burkhard Stiller. An Overview of IP Flow-Based Intrusion Detection. *IEEE Communications Surveys & Tutorials*, 12(3):343–356, 2010.

[ZFdRD05] Artur Ziviani, Serge Fdida, José F. de Rezende und Otto Carlos M. B. Duarte. Improving the Accuracy of Measurement-based Geographic Location of Internet Hosts. *Comput. Netw. ISDN Syst.*, 47(4):503–523, Marz 2005.