Prefix-Hijacking im Internetrouting

Monitoring, Analyse und Mitigation

Dissertation

zur Erlangung des Doktorgrades
Doctor Rerum Naturalium (Dr. rer. nat.)

vorgelegt von

Matthias Wübbeling
aus Herdecke

vorgelegt an der
Rheinischen Friedrich-Wilhelms-Universität Bonn
Mathematisch-Naturwissenschaftliche Fakultät

im Promotionsfach
Informatik

Bonn, 13. Juni 2019

Angefertigt mit Genehmigung der Mathematisch-Naturwissenschaftlichen
Fakultät der Rheinischen Friedrich-Wilhelms-Universität Bonn

1. Gutachter: Prof. Dr. Michael Meier

2. Gutachter: Prof. Dr. Matthew Smith

Tag der Promotion: 11. Oktober 2019

Erscheinungsjahr: 2019

Für Lissy!

Für Papa!

Danksagung
Ich danke meiner Frau Elisabeth für ihre unendliche Geduld, ihre Unterstützung und Motivation. Ich danke meinen Kindern für die inspirative Ablenkung zu Tages- und Nachtzeiten. Ich danke allen in der Familie für jegliche Unterstützung, die ich erhalten habe. Ich danke meinem Doktorvater Michael Meier für die konstruktiven Gespräche und die Freiheiten in der Gestaltung meiner Arbeiten. Ich danke meinen Kollegen für die vielen intensiven Fachgespräche, Diskussionen und Reviews meiner Arbeit, insbesondere Arnold Sykosch, Felix Boes und Timo Malderle. Ich danke Thomas Trimborn für unschätzbare Stunden an Entwicklung und Fehlersuche und die sehr hohe Einsatzbereitschaft.

Zusammenfassung

Die vorliegende Arbeit betrachtet IT-Sicherheitsaspekte des Internetroutings und verbessert etablierte Ansätze zur Entdeckung, zur Klassifikation und zur Untersuchung der Folgen von Anomalien im Internetrouting und entwickelt darüber hinaus das Konzept und zeigt die Erprobung einer effektiven Gegenmaßnahme auf.

Dabei steht das Border-Gateway-Protokoll (BGP), das die weltweite Kommunikation zwischen Computersystemen über das Internet erst ermöglicht, im Fokus der Betrachtung. Ausgehend von Computernetzwerken im militärischen Kontext und in Forschungseinrichtungen in den 1980er Jahren, entwickelte sich das Internet zu einem weltumspannenden Netzwerk von Computernetzwerken, das aus der zivilen Gesellschaft nicht mehr wegzudenken ist. Während moderne Anwendungen Haushaltsgeräte miteinander vernetzen und der Austausch von individuellen Erlebnissen den Takt in der modernen Gesellschaft vorgibt, sind die grundlegenden Mechanismen dieser Vernetzung in den letzten Jahren unverändert geblieben.

Als Netzwerk von Computernetzwerken ist das Internet ein dynamischer Zusammenschluss sogenannter Autonomer Systeme (AS), also Computernetzwerken von Unternehmen, Forschungseinrichtungen sowie Regierungs- und Nicht-Regierungs-Organisationen. Um Datenpakete zwischen zwei Endgeräten unterschiedlicher AS auszutauschen, müssen auf den unteren Ebenen des eingesetzten TCP/IP-Protokollstacks notwendige Erreichbarkeitsinformationen ausgetauscht und regelmäßig aktualisiert werden. Für den Austausch dieser Erreichbarkeitsinformationen im Internet wird BGP verwendet.

Die mit BGP ausgetauschten Erreichbarkeitsinformationen bestehen aus einem IP-Adressbereich (Prefix) und dem AS-Pfad, den ein Paket auf dem Weg zum Ziel durch andere AS zurücklegen muss. Dabei ist in BGP keine Validierung der ausgetauschten Erreichbarkeitsinformationen vorgesehen. Jedes AS kann damit im Grunde beliebige Informationen in das Internetrouting einbringen oder bei der Weiterleitung bestehende Informationen manipulieren. Falsche Erreichbarkeitsinformationen haben unterschiedliche Ursachen, etwa Fehler in der Routing-Hardware, Konfigurationsfehler in der Administration oder gezielte Angriffe. Aus falschen Erreichbarkeitsinformationen resultieren Routinganomalien unterschiedlicher Kritikalität, bis hin zur Nicht-Erreichbarkeit von Prefixen oder der Übernahme von Prefixen durch Angreifer. Diese Übernahme fremder Prefixe durch einen Angreifer nennt man Prefix-Hijacking, also die Entführung eines IP-Adressbereichs. Es gibt keine globale Sicht auf das Internetrouting, so dass eine globale Erkennung von Prefix-Hijacking ohne weiteres nicht möglich ist. Vielmehr besitzt jedes AS eine ganz eigene Sicht auf das Internet, bedingt durch die mit den Nachbarn ausgetauschten Erreichbarkeitsinformationen. Für einen Überblick müssen diese lokalen Sichten zunächst zu einer globalen Sicht zusammengefasst werden.

Da Prefix-Hijacking mit der eingesetzten Version von BGP einfach realisiert werden kann, sind weitere Maßnahmen notwendig, um die Schutzziele der IT-Sicherheit im Internetrouting umzusetzen. Präventive Maßnahmen, wie die nachträgliche Absicherung der Erreichbarkeitsinformationen über Protokollerweiterungen oder zusätzliche Protokolle sind bisher nicht flächendeckend eingesetzt und daher ohne Erfolg. Für Prefix-Besitzer bleibt das kontinuierliche Monitoring der eigenen Prefixe im Internet als Maßnahme zur Gewährleistung der IT-Sicherheit.

Die vorliegende Arbeit analysiert zunächst die Datenlage zur Umsetzung eines effektiven Monitorings des Internetroutings und berücksichtigt dabei die in der Literatur genutzten Routingarchive unterschiedlicher Anbieter. Durch die Hinzunahme weiterer Quellen, wie Internetknotenpunkten oder sogenannten Looking-Glass-Diensten, werden die in den Routingarchiven enthaltenen Informationen angereichert und die globale Sicht verbessert. Anschließend folgt die Revision der etablierten Methode zur Abschätzung einer Prefix-Hijacking-Resilienz für AS und die Herleitung einer verbesserten Formel zur Folgenab-

schätzung. Daraufhin wird eine effektive Gegenmaßnahme vorgestellt, die mit der Unterstützung von Partner-AS die Reichweite der legitimen Erreichbarkeitsinformationen ermöglicht und damit eine Mitigation von Prefix-Hijacking zumindest grundsätzlich möglich macht. Durch die vorgestellten Ansätze zur Verbreiterung der Datenbasis, zur Verbesserung der Analyse von Prefix-Hijacking-Folgen und dem Ansatz zur Mitigation von Prefix-Hijacking durch die Prefix-Besitzer, lassen sich verbesserte Maßnahmen zur Sicherstellung der IT-Sicherheits-Schutzziele umsetzen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Die vorliegende Arbeit betrachtet IT-Sicherheitsaspekte des Internetroutings und verbessert etablierte Ansätze zur Entdeckung, zur Klassifikation und zur Untersuchung der Folgen von Anomalien im Internetrouting und entwickelt darüber hinaus das Konzept und zeigt die Erprobung einer effektiven Gegenmaßnahme auf.

Im Zentrum der Betrachtung steht dabei das *Border-Gateway-Protokoll* (BGP), dass bereits frühzeitig der De-facto-Standard zum Austausch von Erreichbarkeitsinformationen im Internet wurde. Seit Beginn der zivilen Nutzung an Universitäten und Forschungseinrichtungen in den 1980er Jahren hat sich das Internet zur Infrastruktur alltäglicher Kommunikation im geschäftlichen und privaten Bereich entwickelt. Da zunächst die Vernetzung im Vordergrund stand, hatten IT-Sicherheitsaspekte bei der Entwicklung der Techniken und Protokolle keine hohe Relevanz. Viele Anwendungsprotokolle des Internets wurden in den letzten Jahren weiterentwickelt und um IT-Sicherheitsaspekte erweitert. Diese Protokolle laufen im Gegensatz zu BGP jedoch auf den Computern der Anwender, die einfacher zu aktualisieren sind als die Router im Kernbereich des Internets. Daher wurden die vorgeschlagenen Erweiterungen von BGP bisher nicht flächendeckend umgesetzt.

Aufgrund der Relevanz für die Gesellschaft, wird das Internet vom Ministerium des Innern in Deutschland im Bereich „Informations- und Kommunikationstechnologie“ indirekt als kritische Infrastruktur eingestuft [19, 20]. Andere kritische Infrastrukturen, wie Banken, Energiekonzerne oder Medien- und Kultureinrichtungen, sind ebenfalls zu großen Teilen von der Funktionalität des Internets abhängig und unterstreichen die Bedeutung des Internets.

In der Struktur ist das Internet, als Verband physikalischer Computernetze (im weiteren Verlauf auch Netze genannt), grundsätzlich nicht hierarchisch – obwohl sich durch eine Klassifizierung anhand der Größe und Marktstellung beteiligter Netze eine Hierarchie darstellen lässt. Ein Autonomes System (AS), als kleinste abstrakte Einheit des Internets, ist ein physikalisches Netz unter einer bestimmten administrativen Domäne, wie einem Internet-Diensteanbieter (ISP), einem Unternehmen oder einer Universität. Durch physikalische Netzverbindungen mit anderen Autonomen Systemen wird es Teil des globalen Internets.

Die Kommunikation zwischen Computern (weiterhin auch Teilnehmer genannt) aus verschiedenen Netzen basiert auf dem Internet-Protokoll (IP in den Versionen 4 und 6, kurz IPv4 und IPv6), welches die Adressierung der Teilnehmer festlegt und die Grundlage für das Routing der Datenpakete bildet. Jeder Netz-Teilnehmer erhält eine eindeutige IP-Adresse aus dem Adressraum des zugehörigen AS. Solche Adressräume werden einem AS durch eine zuständige übergeordnete Verwaltungsorganisation zugeteilt, um doppelte Nutzung von IP-Adressen zu verhindern. Adressräume lassen sich bis zu einer gewissen Größe in Unteradressräume aufteilen, was eine feingliedrige Unterteilung des gesamten zur Verfügung stehenden IP-Adressbereichs (2^{32} IPv4-Adressen und 2^{128} IPv6-Adressen) erlaubt.

Um von jedem Teil des Internets erreichbar zu sein, müssen alle AS ihre eigenen IP-Adressbereiche bekanntgeben. Die Bekanntgabe des Besitzes erfolgt an alle Nachbar-Netze – also AS, mit denen eine physikalische Netzverbindung besteht – die diese Bekanntgabe wiederum an die ihrigen Nachbarn weiterleiten. Jedes AS pflegt eine Tabelle mit Routen, also all den anderen AS zwischen dem AS selbst und dem Besitzer (oder Ursprungs) -AS eines Adressbereichs, um Datenpakete an den Empfänger weiterleiten zu können. Daher gibt es keine globale Sicht auf das Internetrouting sondern jedes AS besitzt eine ganz eigene Sicht auf das Internet und auf die Wege, über die Datenpakete weitergeleitet werden.

Die Weitergabe der Bekanntgaben von AS zu AS erfolgt in den meisten Fällen ohne weitere Prüfung der enthaltenen Informationen. Dieses implizite Vertrauen zwischen allen Autonomen Systemen ist dabei eine große Bedrohung für

die Routingsicherheit im globalen Internet. Ein Fehler bei der Bekanntgabe eigener Routen kann somit leicht zu großflächigen (sowohl netztopologischen als auch geografischen) Konnektivitätsproblemen führen. In der Geschichte des Internets gibt es einige Vorfälle, die als Folge von Fehlkonfiguration die Nicht-Erreichbarkeit von großen IP-Adressbereichen in Teilen der gesamten Welt verursachten. Der Begriff der Fehlkonfiguration wird dabei werteneutral genutzt, so dass auch gezielte Manipulation – also Angriffe auf die Routingebene des Internets – als Fehlkonfiguration betrachtet werden. Die Folgen für das globale Routing im Internet werden allgemein als Anomalien bezeichnet.

Im Forschungskontext von Routinganomalien im Internet werden regelmäßig die folgenden übergeordneten Forschungsfragen thematisiert:

- Welche Daten bilden eine Ground-Truth (im Sinne eines Realitätsabgleichs) für Internetrouting und folgt die akademische Praxis dieser Ground-Truth?
- Welche Daten lassen sich für eine Vermessung der Internets verwenden und welche Aussagen für den Zustand des Internetroutings können davon abgeleitet werden?
- Wie lassen sich die Folgen von Prefix-Hijacking abschätzen und ist es möglich, allgemeine Aussagen auf Basis der Verbindungen zwischen Autonomen Systemen zu treffen?
- Kann Prefix-Hijacking verhindert werden bzw. lassen sich die Folgen für betroffene Autonome Systeme minimieren?

In dieser Arbeit werden die folgenden in diesen Kontext eingebetteten konkreten Forschungsfragen beantwortet:

- Wie sind die Informationen in Routingarchiven organisiert und wie lassen sich diese zur Erkennung von Anomalien im Internetrouting nutzen? (Vgl. Kapitel 4)
- Welche effizienten Möglichkeiten gibt es, neben öffentlich verfügbaren Routingarchiven, um weitere Daten über das Internetrouting zu sammeln (Monitoring), um die Überwachung der Schutzziele zu verbessern? (Vgl. Kapitel 5)
- Wie lässt sich die Sicherheit Autonomer Systeme im Bezug auf BGP-Routinganomalien quantifizieren? (Vgl. Kapitel 6)

- Gibt es effektive Gegenmaßnahmen, um Angriffe auf das Internetrouting abzuwehren und wie lassen sich diese realisieren? (Vgl. Kapitel 7)

Die Arbeit ist wie folgt strukturiert: Um diese Forschungsfragen zu beantworten, gibt 2 einen Überblick über die benötigten Grundlagen für das Verständnis der Forschungsfragen. Kapitel 3 gibt einen Einblick in Routinganomalien und daraus resultierende Folgen für die Erreichbarkeit von Autonomen Systemen. Kapitel 4 stellt den akademischen Konsens zur Datenbasis dar und diskutiert den damit möglichen Realitätsabgleich. Kapitel 5 demonstriert effektive Möglichkeiten zur einfachen Erweiterung der Datenbasis mit zusätzlichen und aktuellen Datenquellen. Kapitel 6 zeigt Ungenauigkeiten bei der bisher genutzten Formel zur Berechnung von Prefix-Hijacking-Resilienz und definiert eine verbesserte Formel die der Dynamik des Internetroutings gerecht wird. In Kapitel 7 wird eine effektive Maßnahme gegen Prefix-Hijacking vorgeschlagen und gezeigt, wie die Folgen abgeschwächt werden können, um die Kommunikation mit betroffenen Systemen zu ermöglichen. Kapitel 8 fasst die Ergebnisse dieser Arbeit zusammen und gibt einen Ausblick auf offene Fragestellungen und Arbeiten auf Basis der Ergebnisse dieser Arbeit.

2 IT-Sicherheit und Internetrouting

Die meisten Prozesse der heutigen westlichen Gesellschaft sind maßgeblich auf die Unterstützung durch Computer angewiesen. Um die Sicherheit für diese computergestützten Prozesse sicherzustellen, bietet die IT-Sicherheit Rahmenbedingungen, Prozesse, Methoden und Techniken. Die globale Vernetzung über das Internet erlaubt die Verteilung von Informationen an nahezu jeden beliebigen Punkt der Welt innerhalb kurzer Zeit. Damit Datenpakete im Internet zugestellt werden können, ist ein globales Routing erforderlich, was die Adressierung jedes Endpunkts erlaubt und so die Kommunikation zwischen Endpunkten ermöglicht. In diesem Kapitel werden die grundlegenden Begriffe der IT-Sicherheit und des Internetroutings eingeführt und erläutert.

2.1 IT-Sicherheit

IT-Systeme (auch Rechner; engl. computer) werden sowohl für die Speicherung von Daten als auch für die Verarbeitung dieser Daten genutzt. Durch Aggregation unterschiedlicher Daten und Interpretation der Daten können dabei neue Daten entstehen, die ebenfalls gespeichert und für weitere Verarbeitungsvorgänge genutzt werden. Zur dauerhaften Speicherung werden Datenträger wie Disketten, Festplatten, CD/DVD-Roms oder USB-Sticks verwendet. Um Daten zur Speicherung oder weiteren Verarbeitung an einen anderen Ort zu bringen, können die Datenträger physikalisch an diesen Ort transportiert werden. [40, 137]

Um den Transport von Daten zu beschleunigen, werden Computer über Daten-Netze miteinander verbunden. Diese physikalische Verbindung zwischen Computern erlaubt die Kommunikation zwischen verbundenen Geräten und somit die Übertragung von Daten von einem Computer zu einem oder mehreren anderen. Dabei können Computer auch stellvertretend (transitiv) Daten weiterleiten, was eine direkte physikalische Verbindung von Kommunikationspartnern überflüssig macht. Je nach Größe und Entfernung der Computer wird unterschieden zwischen lokalen Netzen (Local Area Network; LAN), regionalen oder überregionalen Netzen (Wide Area Network; WAN) oder dem Internet als einem Netz von Netzen. Das Internet als weltumspannendes Netz von Computernetzen ermöglicht heute die beliebige Kommunikation zwischen verschiedenartigen Endgeräten. [108, 137]

Die englischen Begriffe *safety* und *security* werden im deutschen mit *Sicherheit* übersetzt. Bezogen auf die IT-Sicherheit müssen sowohl Safety- als auch Security-Aspekte für IT-Systeme betrachtet werden[1]. Dabei bezieht sich Safety auf die Funktionssicherheit, also die Tatsache, dass ein System unter den Bedingungen, denen es ausgesetzt ist, in dem vorgesehenen Umfang funktioniert und dabei keine unvorhergesehenen Risiken für Leib und Leben oder die Umgebung auftreten bzw. auf diese adäquat reagiert werden kann. Security bedeutet Informationssicherheit und bezieht sich darauf, dass bei einem (im Sinne von Safety) funktionierenden System der Prozessablauf selbst und die in diesen Prozess eingebundenen Daten nicht unberechtigt eingesehen, verändert oder gelöscht werden. Die beiden Bereiche Safety und Security sind nicht trennscharf zu differenzieren, da sie sich gegenseitig beeinflussen. Wird mangels Informationssicherheit ein Prozess unberechtigt verändert, so kann dies gravierenden Einfluss auf die Safety-Eigenschaften des Systems haben. Neben Safety und Security umfasst IT-Sicherheit in der Literatur auch die Bereiche *Datensicherheit* (engl. data protection) sowie *Datenschutz* (engl. privacy). Streng genommen handelt es sich dabei aber um Security-Aspekte, da insbesondere die unberechtigte Einsicht und Veränderung von Daten verhindert werden soll. [9, 40, 46]

[1] Im weiteren Verlauf der Arbeit werden hauptsächlich die Security-Aspekte der IT-Sicherheit betrachtet. Daher wird IT-Sicherheit im Folgenden mit dem englischen Security gleichgesetzt.

Im folgenden Abschnitt 2.1.1 werden zunächst die übergeordneten Schutzziele der IT-Sicherheit vorgestellt. Anschließend stellt Abschnitt 2.1.2 die Gefährdungen dieser Schutzziele dar und Abschnitt 2.1.3 präsentiert mögliche Schutzmaßnahmen. Abschließend thematisiert Abschnitt 2.1.4 Methoden zur Überwachung dieser Schutzmaßnahmen.

2.1.1 Schutzziele

Die praktische Relevanz von IT-Sicherheit ergibt sich anhand definierter und allgemein akzeptierter Schutzziele [40] sowie auch individueller und anwendungsfallbezogener Schutzziele [144]. Diese können sich direkt oder indirekt beeinflussen, zueinander im Widerspruch stehen oder sich gegenseitig ausschließen. In dieser Arbeit sind die Schutzziele bezogen auf die Speicherung und Verarbeitung von Daten auf Computern sowie die Übertragung auf andere Computer. Im Vordergrund stehen dabei die folgenden übergeordneten Schutzziele der IT-Sicherheit [144]:

Vertraulichkeit - Informationen werden vor unbefugter Einsichtnahme geschützt. Das Schutzziel der Vertraulichkeit gewährt die Geheimhaltung einer Information gegenüber unberechtigten und unbefugten Benutzern. Um dieses Schutzziel zu erreichen, müssen unterschiedliche Aspekte des Zugriffs auf Daten betrachtet werden. Bei der Speicherung von Informationen auf einem Datenträger muss das Betriebssystem den *technischen Zugriff* auf die Daten durch eine geeignete Zugriffskontrolle sicherstellen. Neben dem technischen Zugriff eines Benutzers über das Betriebssystem kann aber auch ein *physischer Zugriff* auf die Festplatte des Computers erfolgen, um die darauf gespeicherten Informationen mit anderen Mitteln auszulesen. Existiert nicht für beide Aspekte eine Zugriffskontrolle oder befinden sich die Daten außerhalb des eigenen Kontrollbereichs kann die Vertraulichkeit etwa durch Verschlüsselung sichergestellt werden. Verschlüsselung lässt sich also insbesondere beim Versand von Informationen zur Sicherstellung der Vertraulichkeit nutzen. [40, 43]

Integrität - Nachträgliche Änderungen der Informationen sind nachweisbar. Das Schutzziel der Integrität stellt sicher, dass gespeicherte Informationen in der Form erhalten bleiben, wie sie zum Zeitpunkt der Speiche-

rung waren. Eine Änderung der Daten lässt sich ähnlich dem Schutzziel der Vertraulichkeit durch eine entsprechende Zugriffskontrolle verhindern. Selbst, wenn eine Änderung der Informationen zwischenzeitlich möglich ist, soll diese Änderung nicht unbemerkt vom Empfänger der Informationen bleiben. Viele Dateisysteme speichern zu diesem Zweck die letzten Zugriffszeiten auf Dateien. Befinden sich Informationen außerhalb des eigenen Kontrollbereichs können Änderungen an Informationen nicht zuverlässig mit Zeitstempeln erfolgen. Prüfsummen eignen sich sowohl lokal als auch bei der Übertragung von Informationen, um die Integrität von Informationen sicherzustellen. Allerdings ist dabei zu beachten, dass auch die Prüfsummen selbst nicht unbemerkt veränderbar sein dürfen. [40, 43]

Zurechenbarkeit - Gespeicherte Informationen und übertragene Informationen können einem Besitzer, bzw. einem Sender und einem Empfänger zugeordnet werden. Das Schutzziel der Zurechenbarkeit erlaubt den Urheber von Informationen eindeutig zu bestimmen. In einem Dateisystem auf einem Datenträger gespeicherte Informationen werden beim Speichern immer einem Benutzer zugeordnet. Der Urheber einer Information bzw. der Absender und der Empfänger einer Nachricht sind eindeutig identifizierbar. Nachrichten in Computernetzen werden grundsätzlich mit einem Absender und einem Empfänger versehen. [40, 43]

Anonymität, als ein untergeordnetes Schutzziel der Vertraulichkeit, steht in direktem Widerspruch zur Zurechenbarkeit und der Angabe von Absender und Empfänger. Um Anonymität zu gewährleisten, werden Absender und Empfänger einer Nachricht in der Form verändert, dass die Zurechenbarkeit zu einer Person nicht mehr ohne weiteres möglich ist, während die anderen Schutzziele möglichst nicht beeinträchtigt werden. Gelegentlich wird Zurechenbarkeit auch als Teilaspekt der Integrität verstanden [43]. Für die Betrachtung von IT-Sicherheit beim Internetrouting im Rahmen dieser Arbeit ist eine separate Betrachtung aber durchaus sinnvoll.

Verfügbarkeit - Ressourcen und Dienste stehen grundsätzlich für Benutzer zur Verfügung. Das Schutzziel der Verfügbarkeit beabsichtigt den Zugriff

auf Informationen und die Nutzung von Diensten ohne Einschränkungen. Gespeicherte Informationen sind damit stets verfügbar. Das Schutzziel der Verfügbarkeit wird sowohl von technischen Fehlern (Nicht-Verfügbarkeit durch fehlerhafte Hard- oder Software) als auch durch physische Ereignisse, etwa durch Elementareinwirkungen (Brand oder Überschwemmung) ebenso wie Stromausfälle oder Diebstahl, bedroht. Damit lässt es sich sowohl den Safety- als auch den Security-Aspekten zuordnen. [40, 43]

Die vier genannten Schutzziele ergänzen sich gegenseitig, widersprechen sich aber auch in gewissem Maße (vgl. Abschnitt 2.1.3). So ist etwa die Zurechenbarkeit selbst nur durch die Speicherung zusätzlicher Informationen möglich, nämlich über den Urheber oder Absender der Information. Diese zusätzlichen Informationen müssen für sich genommen ebenfalls den Schutzzielen genügen. Insbesondere muss das Schutzziel der Integrität gewährleistet sein. Wäre nachträglich eine unbemerkte Änderung der Urheberschafts- oder der Absender-Information möglich, ist die Zurechenbarkeit selbst nicht mehr gewährleistet.

2.1.2 Gefährdung der Schutzziele

Die genannten Schutzziele sind unterschiedlichen Gefährdungen ausgesetzt. Das Bundesamt für Sicherheit in der Informationstechnik benennt im aktuellen IT-Grundschutz-Kompendium 47 elementare Gefährdungen [24]. Aus der Summe der tatsächlichen Gefahren für ein System ergibt sich eine Bedrohungslage oder ein Risiko für dieses System. „Eine Bedrohung (engl. threat) des Systems zielt darauf ab, eine oder mehrere Schwachstellen oder Verwundbarkeiten auszunutzen, um einen Verlust der Datenintegrität, der Informationsvertraulichkeit oder der Verfügbarkeit zu erreichen, oder [sic!] um die Authentizität von Subjekten zu gefährden“ [40]. Dabei ist eine Schwachstelle „eine Schwäche eines Systems oder [ein] Punkt, an dem das System verwundbar werden kann“ [40]. Das Risiko einer Bedrohung für ein System ist „die Wahrscheinlichkeit (oder relative Häufigkeit) des Eintritts eines Schadensereignisses und die Höhe des potentiellen Schadens, der dadurch hervorgerufen werden kann“ [40]. Um Bedrohungen abzuwehren und das Risiko zu minimieren, müssen also entsprechende Maßnahmen getroffen werden, um die Schutzziele zu erreichen.

2.1.3 Schutzmassnahmen

Schutzziele sind nicht nur *technisch* sondern auch *physisch* entsprechenden Gefährdungen ausgesetzt. Um die Schutzziele trotz dieser Risiken zu erreichen, müssen Sicherheitsanforderungen eines Systems und geeignete technische, physische und organisatorische Maßnahmen definiert und realisiert werden. Die Ursache dafür ist, dass die Systeme die geforderten Maßnahmen zur Einhaltung der Schutzziele nur teilweise selbst umsetzen können. Brandschutz oder eine unterbrechungsfreie Spannungsversorgung sind etwa physische Maßnahmen, die ein System selbst nicht sicherstellen kann. Bei organisatorischen Maßnahmen handelt es sich zumeist um Richtlinien für Benutzer. [40, 43] Häufig sind organisatorische Maßnahmen technisch nicht ohne weiteres umsetzbar.

> **Beispiel: Organisatorische Maßnahmen**
> Eine mögliche organisatorische Maßnahme ist das Verbot der privaten Nutzung von Social-Media-Konten in Unternehmen, wobei die dienstliche Nutzung notwendig ist. Technisch ist es nicht ohne weiteres möglich, den Zugang zu Social-Media-Plattformen zu unterbinden, da dies auch die dienstliche Nutzung beeinträchtigen würde. Somit bleibt nur, das Verbot der privaten Nutzung als organisatorische Maßnahme umzusetzen.

Alle Maßnahmen lassen sich unterscheiden in *präventive* und *reaktive* Maßnahmen. Eine unterbrechungsfreie Spannungsversorgung wäre damit eine präventive Maßnahme, die Zuhilfenahme eines Stromgenerators, um die Versorgung darüber hinaus sicherzustellen, eine reaktive Maßnahme.

Für jedes Schutzziel lassen sich geeignete Maßnahmen zum Erreichen dieses Schutzziels benennen. Dabei gibt es Maßnahmen, die einem Schutzziel zuträglich, einem anderen Schutzziel jedoch abträglich sind. So lässt sich keine umfassende Sicherheit unter Berücksichtigung aller Schutzziele erreichen. Bei der Umsetzung von Maßnahmen müssen also Kompromisse hinsichtlich der Schutzziele getroffen werden.

> **Beispiel: Widersprüche zwischen Schutzzielen**
> Es ist möglich, einen Datenträger mit Informationen in einem Safe sicher vor unberechtigtem Zugriff oder der Veränderung zu schützen. Da der Datenträger jedoch nicht gleichzeitig in einem System vorhanden sein kann, um dort

> verwendet zu werden, ist das Schutzziel der Verfügbarkeit nicht zeitgleich erreicht. Würde nun der Datenträger über eine Maßnahme zur Erfüllung der Verfügbarkeit wieder in ein System eingebaut, sind in dem Moment die Maßnahmen zur Sicherstellung der Vertraulichkeit oder Integrität wieder deutlich abgeschwächt worden. Es sind also weitere Maßnahmen nötig, etwa die Zugriffskontrolle über das Betriebssystem.

2.1.4 Überwachung der Schutzmassnahmen

Ein Angriff gegen ein Schutzziel ist der Versuch, die existierenden Maßnahmen eines Systems zu manipulieren bzw. zu umgehen und so das Schutzziel zu verletzen. Schutzziele können aber auch versehentlich durch Konfigurationsfehler oder Fehler in Hard- und Software gefährdet werden. Ebenso ist es möglich, dass Maßnahmen zur Risikominimierung selbst fehlerhaft sind oder umgangen werden können. Einmalig durchgeführte Maßnahmen zur Risikominderung führen also nicht zwangsläufig zum dauerhaften Erreichen eines Schutzziels. [40]

Maßnahmen zur Zugriffskontrolle etwa sind nur so lange erfolgreich, bis es einem Angreifer gelingt, einen Fehler zu entdecken und auszunutzen. Um diesem Umstand Rechnung zu tragen, ist es notwendig, die Einhaltung der Schutzziele und die Effektivität der dafür eingesetzten Maßnahmen kontinuierlich zu überwachen. Ein solcher Prozess der Überwachung nennt sich *Monitoring* und lässt sich in unterschiedlichen Ausprägungen betreiben. Monitoring ermöglicht eine Reaktion auf den Wegfall einzelner (meist) *präventiver* Maßnahmen in Form weiterer *reaktiver* Maßnahmen zur Kompensation des Sicherheitsverlusts. Dabei sind die reaktiven Maßnahmen von der unmittelbaren Gefahr und der individuellen Gewichtung der Schutzziele abhängig. Erkennt das Monitoring einen Fehler in der Konfiguration eines Systems oder einen Hard- oder Softwarefehler rechtzeitig, können diese Fehler im besten Fall einfach und ohne große Beeinträchtigungen korrigiert werden. Wird ein gezielter Angriff erkannt und war dieser erfolgreich, müssen je nach Schutzbedarf auch drastische Maßnahmen gewählt werden, bis hin zum Abschalten des Systems.

Grundsätzlich sind noch weitere Ebenen zur Sicherstellung der Schutzziele denkbar. Denn auch die Systeme zur Überwachung der Schutzmaßnahmen un-

terliegen selbst auch den Schutzzielen. So ließen sich auch die zur Überwachung eingesetzten Systeme selbst wieder überwachen. Solche zusätzlichen Ebenen der Überwachung sind jedoch nicht weit verbreitet.

2.2 Internetrouting

Maßgeblich für die weitere Betrachtung ist das Internet in seiner Form als strukturelle und technische Verbindung von Netzen, die als administrativ und technisch eigenständig anzusehen sind. Abschnitt 2.2.1 gibt einen Einblick in die gewachsene Struktur des Internets und daraus resultierende Kategorien der teilnehmenden Netze. Für die Kommunikation im Internet müssen Datenpakete von einem Absender zu einem oder mehreren Empfängern geleitet werden. Dabei werden die Datenpakete über verschiedene Router unterschiedlicher Teilnehmer bis zum Empfänger weitergeleitet. Der Weg, den die Pakete dabei zurücklegen, wird *Route* oder *Pfad* eines Pakets genannt. Ein einzelner Router auf diesem Pfad ist ein *Hop*. Bei diesem *Routing* genannten Vorgang stehen neben der Zuverlässigkeit hauptsächlich Leistungsaspekte bei der Auswahl geeigneter Pfade im Vordergrund. Darüber hinaus müssen Absender und Empfänger (eindeutig) adressierbar sein, um eine Kommunikation zu gewährleisten. Der Abschnitt 2.2.4 stellt die Adressierung mittels IP-Adressen und die Konzepte von Routingverfahren vor. Anomalien im Internetrouting führen allgemein zu verschiedenen Verbindungsproblemen und beeinträchtigen die Sicherheit der Kommunikation im Internet. Dabei gibt es unterschiedliche Ursachen für *Routing-Anomalien*. Die Folgen reichen von einer Beeinträchtigung der Verbindungsqualität über Vertraulichkeitsverlust bis hin zu Nichterreichbarkeit.

2.2.1 Das Internet

Tanenbaum definiert das Internet in einem Satz als „Bezeichnung für eine Ansammlung von Netzen (Netzverbund), die den gesamten Globus überspannen und unter dem Internet-Protokoll (IP) laufen“ [137]. Ein *Autonomes System* ist das organisatorisch kleinste Element dieses Verbunds (vgl. Abschnitt 2.2.2). Dabei beschränkt sich das verbindende Element dieses Netzverbunds auf den Konsens über den Austausch von Paketdaten des Internet-Protokolls und den Austausch von *Erreichbarkeitsinformationen* (engl. Network Layer Reachability

Information; NLRI) nach dem *Border-Gateway-Protokoll* (BGP). Dabei werden Verbindungen individuell oder an dafür vorgesehenen Internetknotenpunkten geschlossen (vgl. Abschnitt 2.2.3). Die große Anzahl an Verbindungen zwischen AS ermöglicht die Weiterleitung von Datenpaketen zwischen beliebigen Kommunikationspartnern, selbst wenn einzelne Verbindungen zeitweise oder dauerhaft wegfallen.

2.2.2 Autonome Systeme

Ein AS ist ein Computernetz, das unter der administrativen Domäne einer Organisation (dem AS-Betreiber) steht und damit eigenständig agiert. Als Computernetz ermöglicht es den darin enthaltenen Computern (Teilnehmern) die Kommunikation. Durch eine Verbindung mit anderen AS (engl. *peering*), die wiederum unter einer eigenen administrativen Domäne stehen, werden die Kommunikationsmöglichkeiten der Teilnehmer erweitert. So lassen sich auch Kommunikationspartner in anderen AS adressieren. Wie Daten innerhalb eines AS ausgetauscht werden und welche Pfade die Pakete wählen obliegt allein dem Betreiber des AS. Lediglich die Organisation der Kommunikation über AS-Grenzen hinweg ist übergeordnet festgelegt. Dabei können AS eigenständig Routing-Richtlinien (engl. routing *policies*) festlegen, wie Datenpakete mit anderen AS ausgetauscht werden.

Die ersten Autonomen Systeme bei der Gründung des Internets als National Science Foundation Network (NSFNet) waren Computernetze von militärischen und zivilen Forschungseinrichtungen sowie Universitäten in den USA [47]. Heutzutage betreiben darüber hinaus viele Universitäten, Organisationen und Unternehmen eigene AS.

Ein Autonomes System besteht in der Regel selbst wieder aus voneinander getrennten Netzbereichen, die jedoch unter einer gemeinsamen administrativen Domäne, z.B. der IT-Abteilung eines Unternehmens oder dem Rechenzentrum einer Universität, stehen. Zwischen den voneinander getrennten Netzbereichen innerhalb eines AS werden Datenpakete mittels Routern von einem Netzbereich in den anderen vermittelt. Für den Austausch der Erreichbarkeitsinformationen können AS-intern andere Routingprotokolle verwendet werden, als in der Kommunikation mit anderen AS. Dies ermöglicht eine bessere Optimierung

für den internen Datenverkehr, da alle relevanten Teile des Netzes aufeinander abgestimmt werden können.

Die physikalischen Verbindungen zwischen mehreren AS bilden nun die Struktur des Internets. Für die Kommunikation zwischen AS ist eine *AS-Nummer* (ASN) notwendig, die bei einer regionalen Internet-Registrierungsstelle beantragt werden kann. ASN werden, ebenso wie öffentliche IP-Adressbereiche, unter der federführenden Organisation der *American Registry for Internet Numbers* (ARIN), durch vier weitere regionale Registrierungsstellen (engl. *Regional Internet Registries*, RIR) vergeben: dem *Réseaux IP Européens Network Coordination Centre* (RIPE NCC), der *Latin American and Caribbean Internet Addresses Registry* (LACNIC), der *Internet Numbers Registry for Africa* (AFRINIC) und dem *Asia Pacific Network Information Centre* (APNIC). Dabei bleibt die Eigenständigkeit der AS gewährleistet, so dass nur der Austausch von Erreichbarkeitsinformationen zwischen AS geregelt wird. Bei der Wahl von Peering-AS oder der Durchsetzung von Policies haben RIR keinen Einfluss.

Eine ASN ist die Voraussetzung für die eigenständige Teilnahme am Internet und die Zuweisung öffentlicher, global erreichbarer IP-Adressbereiche. Je mehr direkte Verbindungen zu anderen AS bestehen, umso mehr IP-Adressbereiche sind direkt erreichbar. Verbindungen mit anderen, nicht direkt verbundenen AS, können indirekt über die verbundenen AS hergestellt werden. Die direkte und indirekte Erreichbarkeit AS-externer IP-Adressbereiche und die Vermittlung von Datenpaketen werden in Abschnitt 2.2.4 thematisiert.

2.2.3 Peeringbeziehungen und Internetknotenpunkte

Peering hat eine ökonomische und eine technische Komponente. Zwei AS werden *Peers*, indem sie mindestens eine physikalische Netzverbindung zwischen ihren Routern etablieren, über die sie Datenpakete ihrer Teilnehmer austauschen. Grundlage einer technischen Peeringbeziehung ist in der Regel ein Vertrag zwischen den jeweiligen AS-Betreibern über den Umfang des Peerings. Peering ist damit ein wirtschaftlicher und technischer Geschäftsvorfall bei der Administration eines AS. Peeringbeziehungen lassen sich in unterschiedliche Kategorien aufteilen:

Peering Zwei AS, AS 1 und AS 2, haben eine *Peer-to-Peer*-Beziehung (P2P), wenn sie die Daten ihrer eigenen Teilnehmer untereinander austauschen. Durch eine solche Beziehung können die Teilnehmer von AS 1 nicht nur untereinander, sondern auch mit den Teilnehmern von AS 2 kommunizieren. Je nach Menge der ausgetauschten Daten und der Größe der beteiligten AS werden solche Peeringbeziehung gleichberechtigt oder vertraglich auf einer Geschäftsbeziehung basierend geschlossen. Je nachdem in welche Richtung und wie viele Daten zwischen Peers ausgetauscht werden, können Ausgleichszahlungen festgelegt werden. Peering ist nicht transitiv. Hat AS 1 ein weiteres Peering-AS, AS 3, folgt daraus nicht, dass auch AS 2 die Teilnehmer von AS 3 erreichen kann. [100]

Eine besondere Form von P2P-Beziehungen sind Sibling-to-Sibling-Beziehungen (S2S). Diese S2S-Beziehungen entstehen, wenn zwei Autonome Systeme desselben AS-Betreibers, etwa von Tochter- oder Schwesterunternehmen eine P2P-Verbindung unterhalten. In solchen Fällen gibt es häufig andere Regelungen bei der Weiterleitung des Datenverkehrs zwischen den AS, so dass auch transitives Peering möglich ist. Da es sich bei S2S um Spezialfälle handelt, die ohne zusätzliches Wissen über die Organisation der beteiligten AS nicht als solche erkannt werden können, werden S2S-Beziehungen nur selten näher betrachtet (vgl. Beispiel 6.2.1).

Transit Zwei AS, AS 1 und AS 2, haben eine Anbieter-Kunden-Beziehung (engl. *provider to customer*, P2C), wenn AS 1 die Pakete von AS 2 nicht nur für die Erreichbarkeit der eigenen Kunden sondern auch transitiv für die Kunden anderer AS weiterleitet. AS 1 als *(Transit-) Provider* ermöglicht AS 2 also die transitive Kommunikation mit allen AS, mit denen AS 2 selbst kein Peering unterhält. Dabei besteht zumeist keine Einschränkung bei den transitiv erreichbaren AS, der Anbieter stellt damit die Verbindung des Kunden zum restlichen Teilnehmerkreis des Internets dar. Alle Pakete, die AS 2 nicht direkt an eigene Peers übergeben kann, werden dann über AS 1 und eventuell weitere Transit-Provider oder Peers an die Empfänger weitergeleitet. Auch die Erreichbarkeit der Teilnehmer des Transit-Providers ist über die Transit-Beziehung sichergestellt. Die Anbieter von Transit werden auch *Upstream* oder *Carrier* genannt. Ein AS ist *multiho-*

med [77], wenn es mindestens 2 P2C-Beziehungen zu unterschiedlichen Upstreams unterhält. [100]

Im Allgemeinen werden die Teilnehmer eines Kunden-AS im Bezug auf Peering als Teilnehmer des Anbieter-AS verstanden. Das bedeutet, dass bei einer P2P-Beziehung zwischen AS 1 und AS 2 sowie einer P2C-Beziehung zwischen AS 1 und AS 3 die Teilnehmer von AS 2 über die Peeringbeziehung auch die Teilnehmer von AS 3 erreichen. Durch die transitiven und direkten Beziehungen aller Autonomen Systeme, die Teilnehmer am Internet sind, ist es möglich weltweit jedes am Internet angeschlossene Gerät zu erreichen. Im Hinblick auf die Beziehungen existiert für AS-Pfade das Paradigma der Tal-Freiheit (engl. *valley-free paradigm*). Dieses besagt, dass kein AS Daten zwischen seinen Upstream-Providern vermittelt. Das hat ökonomische Gründe: das AS würde in einem solchen Fall den ersten Upstream-Provider für den Empfang der Daten bezahlen und bei der Weitergabe dann auch den zweiten Upstream-Provider für den Versand derselben Daten noch einmal bezahlen.

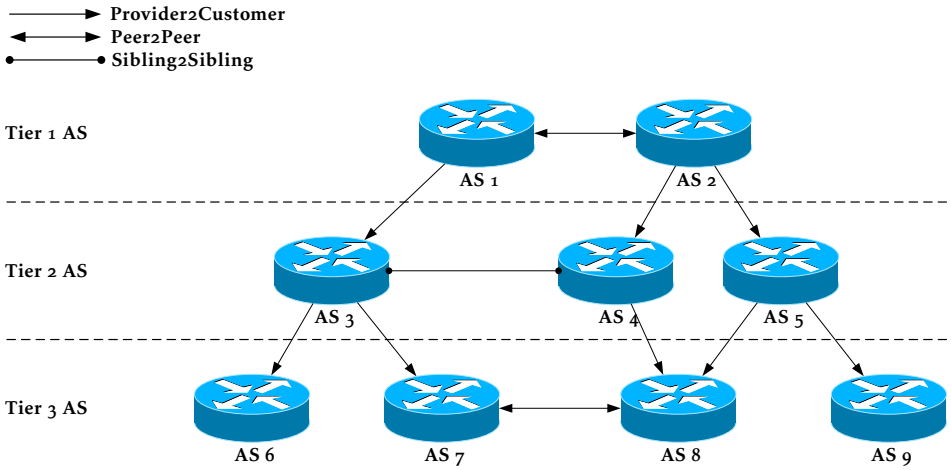

Abbildung 1: *Beispielgraph zur hierarchischen Ordnung des Internets*

Betrachtet man das Internet als Graphen und die Peeringbeziehungen der AS untereinander als Relation, lässt sich eine Ordnung auf diesem Graphen erzeugen. Es hat sich außerhalb der Wissenschaft eine Ordnung mit drei Stufen etabliert, die unterschiedliche Faktoren wie die Anzahl der Peerings oder die globale Präsenz der AS einbezieht. Abbildung 1 zeigt an einem Beispielgraphen eine entsprechende Ordnung. Dabei liegen Anbieter über ihren Kunden und

Peers jeweils auf einer Ebene. Wissenschaftlich wird diese Ordnung zwar referenziert, allerdings lässt sich diese Ordnung nicht ohne weiteres mathematisch definieren (in dieser Arbeit wird daher eine andere Ordnungsrelation verwendet, vgl. Abschnitt 6.2.1). Grundsätzlich ist im Internet nämlich auch Peering zwischen AS unterschiedlicher Ebenen möglich.

Auf der obersten Ebene liegen solche AS, die so gut mit anderen AS vernetzt sind, dass sie keine Upstream-Provider benötigen, um alle anderen Teilnehmer am Internet zu erreichen. Es entsteht eine Clique auf der obersten Ebene des Internets, deren Mitglieder allgemein als Tier-1 AS bezeichnet werden. Dabei handelt es sich aktuell um große und global agierende Organisationen, deren Netze den gesamten Globus umspannen. Eine Ebene darunter befinden sich die sogenannten Tier-2 AS. Dabei handelt es sich um große überregionale und zum Teil internationale Netze, häufig betrieben von größeren Telekommunikationsunternehmen, für die der Zugang zum Internet selbst ein Geschäftsfeld ist. Diese erreichen einen Teil aller Internet-Teilnehmer über unmittelbare Peers, den Rest über ihre Beziehungen mit Tier-1 AS. Kunden solcher Tier-2 AS sind regionale oder lokale Netze von Organisationen, die wiederum als Tier-3 bezeichnet werden. Solche Tier-3 Kunden bieten teilweise auch selbst Transit an, allerdings ist dies meist nicht der Hauptgeschäftszweig der Organisation. Die Anzahl der direkt verbundenen AS ist geringer und meist auf andere regionale oder lokale AS beschränkt. [77, 139]

Die technische Komponente bei der Betrachtung von Peeringbeziehungen sind die Router unterschiedlicher AS, die miteinander verbunden werden. Router innerhalb eines AS, welche über Verbindungen zu Routern anderer AS verfügen, werden *Border-* oder *Gateway-Router* genannt. Teilnehmer eines AS müssen Datenpakete unbekannter Zielnetze lediglich an diese Gateway-Router weiterleiten, die ihrerseits, auf Basis der etablierten Peeringbeziehungen, den nächsten Router eines anderen AS auf dem Weg zum Zielnetz wählen.

Die Router befinden sich dabei in räumlicher Nähe und sind über einen Switch netzwerktechnisch miteinander verbunden. Einige Rechenzentren bieten dafür *Co-Location* oder *Housing* genannte Dienstleistungen an. Dabei wird der Platz für Kunden-Hardware vermietet und zumeist auch ein Upstream zum Internet mit angeboten. Das Rechenzentrum ist damit ein *Point-of-Presence* für die Kun-

den. Im Unterschied zu klassischen Hosting-Providern bleibt die Hardware also im Besitz und unter der Kontrolle des Kunden. Peering lässt sich zwischen Kunden des Rechenzentrums etablieren, eine Verbindung erfolgt entweder direkt oder über die Switch-Infrastruktur des Rechenzentrums.

Ein wichtiger Faktor für die Reichweite und Anzahl von Verbindungen zwischen AS sind Internetknotenpunkte. Ein Internetknotenpunkt (engl. Internet eXchange Point (IXP); auch Commercial Internet eXchange (CIX) oder Network Access Point (NAP)) „ist ein Ort, wo mehrere ISPs ihre Netze miteinander verbinden“ [100]. Im Gegensatz zu klassischen Co-Location-Rechenzentren handelt es sich bei IXPs um Carrier-neutrale Rechenzentren, der Upstream ist also nicht (oder nicht unbedingt) Bestandteil der Dienstleistung. Kunden mieten ebenfalls einen Platz für eigene Hardware (Co-Location) und eine Netzanbindung an die Switches des IXPs. Peering und Verträge über Transit werden dann mit anderen Kunden des IXPs ausgehandelt. Während im amerikanische Modell IXPs immer eigene Co-Location-Rechenzentren betreiben, mieten europäische IXPs für eine größere Reichweite auch Platz in klassischen Co-Location-Rechenzentren anderer Betreiber. Sie erweitern damit die Liste ihrer Points-of-Presence und ermöglichen so zusätzliche (Carrier-neutrale) Anbindungen der übrigen Kunden an das Internet. [100] Eine weitergehende Betrachtung von IXPs findet in Abschnitt 5.4 statt.

2.2.4 Internetrouting

Während AS innerhalb des Internets als kleinste organisatorische Einheit betrachtet werden, müssen auch innerhalb eines AS die Datenpakete bis zu den Endpunkten weitergeleitet werden. In solchen (lokalen) Netzwerken werden Datenpakete entweder direkt zugestellt, wenn alle Kommunikationsteilnehmer in einer Kollisionsdomäne liegen, oder über Router von einer Kollisionsdomäne in eine andere weitergeleitet. Größere Netzwerke haben in den meisten Fällen mehrere Kollisionsdomänen, so dass ein Paket über mehrere Router (Hops) bis zum Ziel weitergeleitet wird. Um eine effiziente Weiterleitung innerhalb des AS zu ermöglichen, können interne Routingprotokolle, etwa Open Shortest Path First (OSPF) [94] oder Routing Information Protocol (RIP) [90] genutzt werden. Diese stellen innerhalb des AS sicher, dass keine Kreise entstehen und immer eine möglichst kurze oder kosteneffiziente Route zum Ziel gefunden wird. Jeder

Router muss dabei Informationen über den Aufbau und mögliche Kosten der Verbindungen des Netzwerks besitzen. Diese internen Routinginformationen werden ebenfalls in der Routingtabelle hinterlegt und für jedes Datenpaket abgefragt. Dabei sind alle Endpunkte (Hosts) eindeutig adressierbar (heutzutage meist mit einer IP-Adresse gemäß dem Internet Protokoll) und mindestens einem Router zugeordnet, der in derselben Kollisionsdomäne liegt. Beim Versand eines Pakets genügt also die Kenntnis eines Ziel-Routers. Dieser wird das Paket dann an den adressierten Endpunkt zustellen.

Die einzelnen IP-Adressen der Endpunkte eines jeden AS werden nach wie vor für die Adressierung verwendet, allerdings spielen diese für das Routing der Pakete zwischen unterschiedlichen AS keine Rolle. Vielmehr werden beim Internetrouting ganze IP-Adressbereiche (Prefixe) adressiert und entsprechend den AS zugeordnet. Für jedes im Internet gültige Prefix ist in der Routingtabelle eines Gateway-Routers das Ziel-AS hinterlegt. Als Kern des Internets (engl. core) wird ein AS betrachtet, wenn es die komplette Routingtabelle, also ohne Standardgateway zu einem Upstream-Provider, bei Routingentscheidungen berücksichtigt [80].

Das Internetprotokoll

Das Internet-Protokoll ist ein Protokoll der Vermittlungsschicht gemäß des ISO/OSI-Referenzmodells und das Basisprotokoll des TCP/IP-Protokollstacks. Es wurde entwickelt, um über Kollisionsdomänen hinweg Computer als Endpunkte adressieren zu können. Jeder Endpunkt erhält im IP-Protokoll eine eindeutige IP-Adresse. Die Länge dieser IP-Adresse in Bit unterscheidet sich je nach Protokoll-Version. IP definiert darüber hinaus einen Paket-Header, der den gesendeten Nutzdaten vorangestellt wird. In diesem Paket-Header werden unterschiedliche Parameter für das Paket definiert, unter anderem auch die IP-Adresse des Absenders und des Empfängers. Gemeinsam mit den Nutzdaten wird aus dem Header ein IP-Paket, welches die Kommunikation zwischen Computern, identifizierbar über die IP-Adressen im IP-Header, ermöglicht.

Beim klassenlosen Routing zwischen Domänen (Classless InterDomain Routing; CIDR) werden IP-Adressen zu Subnetzen zusammengefasst. Jedes Subnetz erhält eine Netzadresse (Prefix) basierend auf der Anzahl der gemeinsamen

ersten Bits einer IP-Adresse. Diese ersten Bits sind für alle IP-Adressen eines Subnetzes gleich, alle darauf folgenden Bits beschreiben die Host-Adresse. Subnetze werden in der Notation <Netzadresse>/<Prefixlänge> beschrieben und bilden eine hierarchische Struktur. Ausgehend vom Least Significant Bit werden immer zwei Subnetze zum nächstgrößeren Subnetz (mit einer um 1 kleineren Prefixlänge) zusammengefasst. Die im Internet gängigen Prefixe haben eine Länge zwischen 8 und 24 Bit für IPv4 sowie zwischen 32 Bit und 48 Bit für IPv6. Prefixe können kürzer oder länger als diese Werte sein, diese werden aber von den meisten AS ausgefiltert und sind daher effektiv nicht nutzbar. [11]

Das Border-Gateway-Protokoll (BGP)

Interne Routingprotokolle organisieren das Routing innerhalb Autonomer Systeme (engl. intra AS routing). Aus unterschiedlichen Gründen sind diese Protokolle nicht für den Austausch von Erreichbarkeitsinformationen zwischen AS (engl. inter AS routing) geeignet. Um ein einheitliches Protokoll im Internet zu verwenden und zusätzliche Merkmale wie Peer-Authentifikation, Policies oder eine einfache Weitergabe in das Intra-AS-Routing hinein zu ermöglichen, wurde BGP 1989 entwickelt [139]. Seit 1994 existiert die Version BGP-4 [113], die heute als de-facto-Standard für den Routenaustausch im Internet verwendet wird. Alternative Vorschläge wie das Protokoll für Inter-Domain-Policy-Routing (IDPR) [135] oder das Resource Reservation Protocol (RSVP) [22] konnten sich nicht etablieren [139]. Daher wird im Rahmen dieser Arbeit ausschließlich BGP-4 berücksichtigt.

Obwohl BGP als Layer-5-Protokoll grundsätzlich unabhängig von der Transport-Schicht entworfen wurde, basiert es heute auf TCP [68] und nutzt TCP-Port 179 zur Kommunikation [139]. BGP definiert einen Zustandsautomaten wie in Abbildung 2 und entsprechende Nachrichten der Peeringpartner als Transitionen. Ein solcher Zustandsautomat existiert für jede BPG-Verbindung eines Border-Routers. Lediglich im Zustand *Established* kann eine Verbindung zwischen AS für den Austausch von Datenpaketen genutzt werden. Die übrigen Zustände werden lediglich beim Aufbau der Verbindung durchlaufen, bis die Verbindung erfolgreich aufgebaut wurde. Probleme beim Verbindungsaufbau oder der Abbruch einer bestehenden Verbindung führen immer wieder in den *Idle*-Zustand, aus dem heraus eine neue Verbindung aufgebaut werden kann.

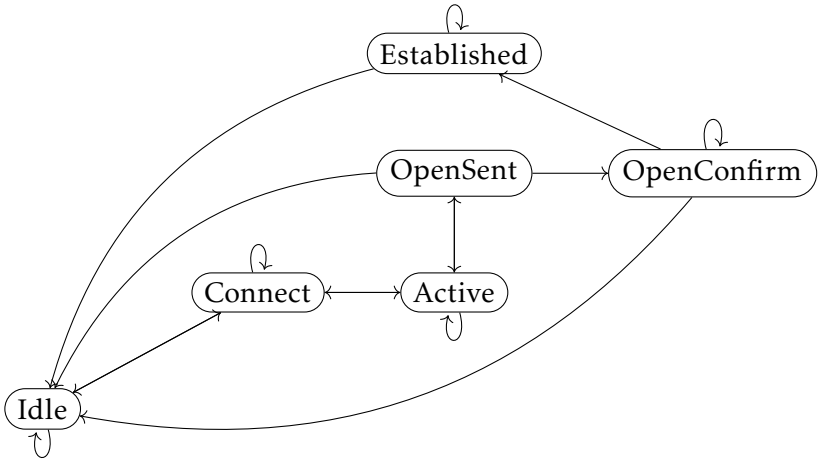

Abbildung 2: *BGP-Zustandsautomat*

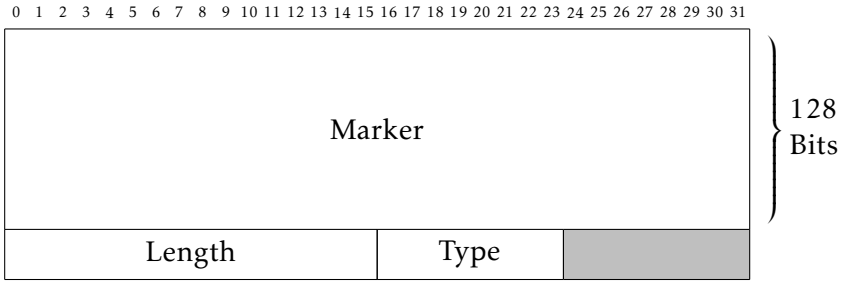

Abbildung 3: *BGP-Protokollheader*

Der Header des BGP-Pakets beginnt wie in Abbildung 3 zunächst mit einem 128 Bit langen Marker (diese Bits sind in den Nachrichten alle auf 1 gesetzt und dienen der Synchronisierung [114]), anschließend folgen die Länge der Nachricht und der Nachrichtentyp. Die vier Nachrichtentypen in BGP sind „open“, „update“, „notification“ und „keepalive“. Eine Erweiterung der Nachrichtentypen ist zwar möglich, hat bisher aber noch nicht stattgefunden.

Open - Die Open-Nachricht wird direkt nach dem Aufbau der TCP-Verbindung von beiden Routern ausgetauscht und enthält unter anderem die eigene AS-Nummer, einen Timeout inaktiver Verbindungen und kann optional auch Informationen zur Authentifikation beinhalten.

Update - Die Update-Nachricht transportiert widerrufene Prefixe (engl. Withdrawn routes), angekündigte Prefixe (engl. Network Layer Reachability Information; NLRI) und den zugehörigen AS-Pfad.

Notification - Die Notification-Nachricht wird genutzt, um Fehlerzustände zu kommunizieren, bevor die BGP-Verbindung beendet wird.

Keepalive - Um zu verhindern, dass eine Verbindung entsprechend dem Timeout aus der *Open*-Nachricht beendet wird, werden leere Keepalive-Nachrichten übertragen.

Da BGP heute der de-facto-Standard ist, benötigt jedes an das Internet angebundene AS einen Router, der BGP-Informationen austauschen kann. Um im Internet erreichbar zu sein, informiert ein AS alle direkten Nachbarn mit der Update-Nachricht über seine eigenen Prefixe (Announcement). Das ankündigende AS wird damit zum Ursprung (engl. origin) des Prefixes und wird zur Quelle (engl. source) des Announcements.

Erhält ein AS ein Announcement von einem Nachbarn wird das Prefix und der AS-Pfad in einer Eingangsdatenbank gespeichert. Auf Basis aller Pfade für ein Prefix wird in einem Auswahlprozess entsprechend der Filter und Policies der beste Pfad ausgesucht und in die Routingtabelle übernommen. Anschließend wird die eigene AS-Nummer dem besten Pfad angehängt und das Announcement an alle weiteren Nachbarn weitergeleitet. So traversiert ein Announcement durch das gesamte Internet, bis jedes AS einen Pfad zum Prefix in der Routingtabelle gespeichert hat.

Ähnlich verhält es sich beim Zurückziehen von angekündigten Prefixen (Withdrawals). Der einzige Unterschied ist dabei das Feld der Update-Nachricht, in dem die Prefixe übermittelt werden. Da es unterschiedliche Felder in der Update-Nachricht gibt, ist es möglich, sowohl Withdrawals als auch Announcements zeitgleich zu senden. Dabei ist es bei Updates von Erreichbarkeitsinformationen nicht nötig, eine Route zunächst zu widerrufen und dann erneut anzukündigen. Das Announcement eines bereits bekannten Prefix impliziert einen Withdrawal der zuvor gesendeten Route zum Origin.

Die Konvergenzzeit, also die Dauer, die ein Announcement benötigt, um von jedem AS im Internet berücksichtigt zu werden, beträgt im Internet eine bis

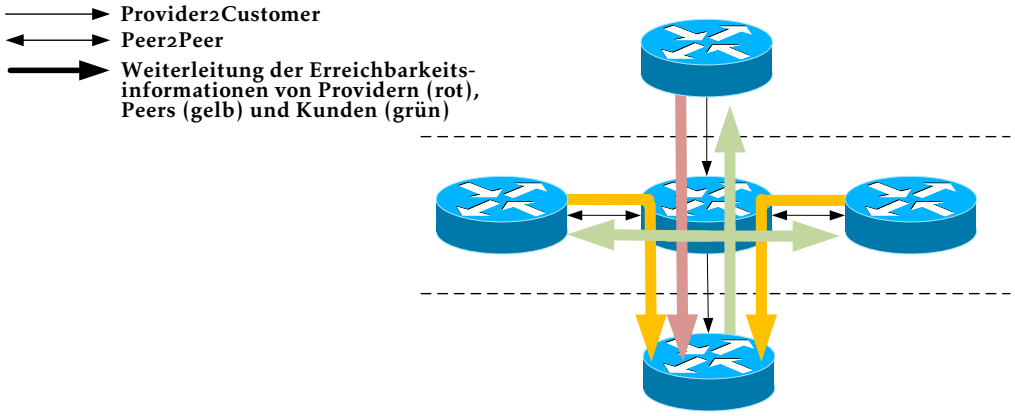

Abbildung 4: *Routingpolicy basierte Weiterleitung der Announcements*

fünfzehn Minuten [34, 78]. Dabei werden Announcements abhängig von den Geschäftsbeziehungen (Routingpolicies), wie in Abbildung 4 dargestellt, weitergeleitet [89]. Eingehende Announcements eigener Kunden werden an alle Peers weitergeleitet, da es sich um eine Transit- bzw. Upstreambeziehung handelt. Die Weitergabe ist notwendig, um die Erreichbarkeit der eigenen Kunden im gesamten Internet sicherzustellen. Eingehende Announcements von Peer-to-Peer-Verbindungen werden ausschließlich an eigene Kunden weitergereicht, da ansonsten eine Transit- oder Upstreambeziehung entsteht. Eingehende Announcements von einem Upstream werden ausschließlich an die eigenen Kunden weitergeleitet. Anhand der Weiterleitung eines Announcements lassen sich mit diesen Regeln Geschäftsbeziehungen zwischen AS ableiten [50].

2.3 IT-Sicherheit im Internetrouting

Ein funktionierendes und fehlertolerantes Internetrouting ohne große technische Hürden ist die Grundlage für den Erfolg des Internets in seiner heutigen Form. In den frühen Jahren des Internets gab es eine überschaubare Anzahl Autonomer Systeme und die Betreiber kannten sich untereinander. Wie bei fast allen Protokollen im Netzwerkbereich wurde daher auch für BGP auf explizite Sicherheitsmechanismen im Protokolldesign verzichtet. Zwar gibt es ein Feld für die Authentifikation in der „Open“-Nachricht von BGP, allerdings authenti-

fiziert dieser nur die TCP-Verbindung zwischen Peers[2]. Eine Möglichkeit zur Absicherung von Origin- oder AS-Pfad-Informationen in den Update-Nachrichten ist nicht vorgesehen. BGP impliziert daher ein gegenseitiges Vertrauen aller am Internet teilnehmenden Autonomen Systeme. Aufgrund der Größe des Internets (mehr als 60.000 AS im Jahr 2018) ist gegenseitiges Vertrauen heute nicht mehr angebracht [10].

Beim Design von Routingprotokollen und -Algorithmen wurden Aspekte des Safety-Begriffs berücksichtigt. Insbesondere die Ausfallsicherheit (engl. failsafe) und die Fehlertoleranz (engl. fault tolerance) sind im Routingkontext sichergestellt. Im Fokus der Sicherheitsargumente steht dabei die Kommunikation zwischen Teilnehmern, also die Sicherstellung der Weiterleitung von Paketen von einem Teilnehmer zum anderen. Wenn eine Verbindung zwischen zwei Routern ausfällt, gibt es aufgrund der großen Vernetzung untereinander viele alternative Routen zur Sicherstellung der Kommunikation, das gilt auch für BGP-Routing [54, 114].

Der folgende Abschnitt 2.3.1 wendet die Schutzziele der IT-Sicherheit auf die Elemente des Internetroutings an und zeigt mögliche Bedrohungen dieser Schutzziele auf. Der anschließende Abschnitt 2.3.2 definiert Routinganomalien allgemein und Abschnitt 2.3.3 präsentiert im Kontext Internetrouting anwendbare Angreifermodelle. Abschließend zeigt Abschnitt 2.3.4 mögliche Ansätze zum Monitoring der Schutzmaßnahmen.

2.3.1 Schutzziele und Bedrohungen

Betrachtet man die Schutzziele der IT-Sicherheit aus 2.1.1 wird damit das Schutzziel der Verfügbarkeit (im Sinne von Safety) bereits im Design der Routingprotokolle adressiert. Im Folgenden werden die Schutzziele im Hinblick auf Internetrouting betrachtet. Dabei müssen verschiedene Facetten des Internetroutings betrachtet werden. Auf der einen Seite steht dabei BGP als Protokoll zum Austausch von Erreichbarkeitsinformationen (engl. control plane), auf der

[2] BGP als Zustandsautomat hat sich als widerstandfähig gegen Angriffe gezeigt [143]. Da BGP auf TCP basiert, gelten die Verwundbarkeiten von TCP zunächst auch für BGP. Dieser Umstand wurde mit dem Authentifikations-Feld im Header gewürdigt, dieser verhindert die Verbindung mit einem nicht authentifizierten Angreifer, der mittels IP-Spoofing eine Verbindung aufbauen möchte. [143]

anderen Seite die auf diesen Erreichbarkeitsinformationen basierenden Routingentscheidungen und über diese Routen ausgetauschten Informationen (engl. data plane).

Verfügbarkeit

Verfügbarkeit mit Bezug auf Security-Aspekte betrachtet die Bedrohung der Verfügbarkeit als Folge gezielter Angriffe (etwa Denial-of-Service), die aufgrund von Protokolleigenschaften aber auch -implementierungen möglich sind. Darunter fallen für BGP etwa Angriffe gegen die TCP-Verbindung, wie bei Reset-Angriffen aber auch gefälschte Erreichbarkeitsinformation [95]. Auch Angriffe gegen die Routerhardware [41] stellen eine Bedrohung dar und können Störungen im Internetrouting verursachen.

Vertraulichkeit

Das Schutzziel der Vertraulichkeit lässt sich für das Routing selbst nicht festlegen, da die Informationen öffentlich verfügbar sein müssen. Für die Gewährleistung der Erreichbarkeit aller Teilnehmer, lassen sich die Zuordnungen von Prefixen zu AS und die AS-Pfade (und damit auch zu einem gewissen Teil die Nachbarschaftsbeziehungen Autonomer Systeme) nicht vertraulich behandeln. Abgesehen von der unmittelbar technischen Ebene des Internetroutings gibt es allerdings Anforderungen an die Vertraulichkeit. So sind die Geschäftsbeziehungen zwischen AS und auch die eingesetzten Policies und Filterregeln häufig als Geschäftsgeheimnisse zu betrachten und damit vertraulich [50]. Mittelbar betrifft Routing auch die Vertraulichkeit der über das Internet ausgetauschten Informationen. Die Route von Paketen durch das Internet lässt sich von den Kommunikationsteilnehmern zwar ein Stück weit nachvollziehen [6] aber nicht beeinflussen. Pakete werden also nicht (ohne weiteres) nachvollziehbar über Autonome Systeme geleitet, die als nicht vertrauenswürdig betrachtet werden. Die Absicherung der übertragenen Inhalte muss also unabhängig vom Routing sichergestellt werden. Es ist aber möglich, eine solche Absicherung durch Manipulationen des Internetroutings anzugreifen (vgl. Abschnitt 2.3.3).

Integrität

Die Integrität der über BGP ausgetauschten Erreichbarkeitsinformationen kann nicht direkt durch das BGP-Protokoll oder damit ausgetauschte Daten sichergestellt werden. Das bedeutet, dass sowohl die Origin-Informationen eines Announcements als auch der AS-Pfad auf dem Weg durch das Internet verändert werden können, ohne dass eine solche Veränderung für den Empfänger ersichtlich ist. Damit ist es leicht möglich, falsche Informationen zu verbreiten und damit das Internetrouting zu stören.

Um die Integrität von Erreichbarkeitsinformationen sicherzustellen gibt es Ansätze auf Basis von Public-Key-Infrastrukturen [73, 84, 140, 142]. Diese ermöglichen über zusätzliche Maßnahmen wie ressourcenbasierte Signaturen der Announcements die Überprüfung der Informationen. Dabei unterscheiden sich die Ansätze im Hinblick auf das Vertrauen in Wurzel-Zertifizierungsstellen und eingesetzte Verfahren bzw. den Umfang der signierten Informationen. Allen Ansätzen gemein ist die Problematik, dass es häufig nicht möglich ist, diese Funktionen auf Routern nachzurüsten und ein zusätzlicher Computer für die Prüfung der Signaturen benötigt wird. Aufgrund der so entstehenden Hürde beim Einsatz dieser Signaturverfahren ist die Verbreitung gering [98]. Einen umfassenden Schutz der Integrität für das gesamte Internetrouting bringen diese Ansätze aber nur dann, wenn im Grunde alle AS daran teilnehmen. Lychev et al. [85] zeigen sogar, dass bei einem partiellen Einsatz dieser Techniken das Risiko sogar höher sein kann.

Mittelbar beeinflusst ein Mangel an Integrität auch das Schutzziel der Vertraulichkeit. Über gefälschte Erreichbarkeitsinformationen können Pakete gezielt umgeleitet werden, so dass die Vertraulichkeit nicht mehr gewährleistet ist.

Zurechenbarkeit

Die Zurechenbarkeit von Erreichbarkeitsinformationen ist auf den ersten Blick durch die Angabe von Origin-Informationen und AS-Pfaden gewährleistet. Eine Zurechenbarkeit ergibt sich damit anhand der AS-Nummern die in den Announcements festgehalten sind. Diese Eigenschaft wird genutzt, um Routingtabellen zu füllen und Routingentscheidungen zu treffen. Routingtabellen selbst ermöglichen auch die Zurechenbarkeit von Paketen im Internet. Da Pakete zwei

IP-Adressen enthalten, eine für den Absender und eine für den Empfänger des Pakets, lassen sich über die Routingtabellen auch die zugehörigen Autonomen Systeme identifizieren. Somit ist es möglich, den Ursprung eines Pakets einem AS zuzurechnen.

Allerdings können sowohl die ausgetauschten Erreichbarkeitsinformationen als auch die Angaben in den IP-Paketen selbst gefälscht sein (IP-Spoofing). Um die Zurechenbarkeit zweifelsfrei zu halten, müssen also auch Maßnahmen zur Sicherung der Integrität dieser Informationen umgesetzt werden.

2.3.2 Routinganomalien

Routinganomalien sind auftretende Störungen im Routing von Paketen. Dabei wird zunächst nicht unterschieden, ob es sich dabei um Routing innerhalb von Autonomen Systemen handelt, oder um das globale Internetrouting. Anomalien müssen dabei nicht zwingend eine Verletzung von Schutzzielen der IT-Sicherheit bedeuten. Auch eine (lokale) Überlastung von Verbindungen durch sachgemäßen Gebrauch und damit verbundene Umleitungen von Paketen sind Routinganomalien.

Für diese Arbeit werden nur solche Anomalien betrachtet, die den Austausch von Erreichbarkeitsinformationen über BGP betreffen und die diskutierten Schutzziele der IT-Sicherheit unmittelbar oder mittelbar beeinträchtigen. Eine Übersicht über die betrachteten Anomalien erfolgt in Kapitel 3.

2.3.3 Angreifermodell

Um die Maßnahmen zum Erreichen der Schutzziele für das Internetrouting zu bewerten, müssen Annahmen über potentielle Angreifer getroffen werden. In der Literatur gibt es Ansätze für ein Angreifermodell in Netzwerkumgebungen wie MANETs [33, 104] und auch den Versuch, ein Angreifer-Modell für sichere Routingprotokolle zu formalisieren [60]. Hollick et al. [60] unterscheiden dabei zwischen passiven und aktiven Angreifern. Passive Angreifer können die Informationen erhalten, die sie aus den von ihnen kontrollierten Geräten auslesen können. Das Dolev-Yao-Modell [38] definiert einen (aktiven) Angreifer gegen

Public-Key-Infrastrukturen und berücksichtigt daher auch Angreifer in Netzwerkumgebungen. Aktive Angreifer können in beiden Modellen sowohl in den Austausch von Nachrichten in der Control-Plane als auch in der Data-Plane eingreifen, Nachrichten erstellen, manipulieren oder löschen. Dabei werden in den Modellen im Grunde die gleichen Eigenschaften eines Angreifers definiert:

1. Manipulation von Informationen - Ein Angreifer kann Inhalte eines Pakets auf der Control-Plane und auf der Data-Plane ändern. Da er selbst Teilnehmer ist, kann er auch eigene Nachrichten an Teilnehmer senden. So kann er etwa gefälschte Erreichbarkeitsinformationen einschleusen.
2. Mitlesen von Kommunikationsinhalten - Ein Angreifer kann Inhalte von Paketen mitlesen, speichern und Muster ableiten. Andere Teilnehmer können auch gezielt Nachrichten an den Angreifer senden.
3. Angriffe auf Weiterleitung - Ein Angreifer kann die Weiterleitung von Paketen beeinflussen und Pakete verwerfen, verzögern oder umleiten.
4. Der Angreifer kann sich beim Versand von Nachrichten als jeder andere Teilnehmer des Netzwerks ausgeben.

Die Ziele der Angreifer korrespondieren dabei mit den Schutzzielen der IT-Sicherheit. Ausgehend von diesem allgemeinen Angreifermodell finden spezifische Anpassungen an die jeweilige Netzwerkumgebung (beispielsweise MANETs, LANs, etc.) statt. Zu diesen Anpassungen gehören auch die Unterscheidung eines Innen- bzw. Außentäters sowie die Anzahl koordinierter Angreifer und die Größe der Angriffsfolgen (lokal oder global). Hollick et al. nennen als weiteres Ziel eines Angreifers noch Angriffe auf die Anonymität und Standorte anderer Teilnehmer[3] [60]. Für die Klassifikation der Angriffe gegen Routing allgemein unterscheiden Hollick et al. nicht mehr allein die Control-Plane und die Data-Plane sondern teilen die Control-Plane nochmal auf in die Bereiche „Routing“ und „Topology“ [60]. Der Routingdienst übernimmt dabei den Austausch von Erreichbarkeitsinformationen, der Topologiedienst beinhaltet die Routingtabelle und Erkundungen der Nachbarschaftsverbindungen (engl. neighbor discovery) bzw. der Netzwerktopologie allgemein. In BGP sind Informationen zur Netzwerktopologie (AS-Pfade) Teil der Announcements und

[3] Nach der in dieser Arbeit genutzten Definition der Schutzziele ist Anonymität dem Schutzziel der Vertraulichkeit untergeordnet.

damit der Erreichbarkeitsinformationen. Ein für BGP spezialisiertes Angreifermodell müsste eine solche Unterscheidung nicht treffen, wobei der Angriff auf die Routingtabelle eines Routers (als Teil von „Topology“) weiterhin ein valides Angriffsszenario ist.

Weitere Angriffsmöglichkeiten

Neben den Angriffen auf die ausgetauschten Erreichbarkeitsinformationen gibt es auch Angriffe gegen den im Protokoll beschriebenen Ablauf und gegen die Router, die BGP implementieren [72, 95].

Da BGP de-facto auf TCP basiert, eignen sich alle Angriffe gegen TCP grundsätzlich auch für Angriffe auf die TCP-Verbindungen der Border-Router. In den meisten Fällen sind diese Angriffe dazu geeignet, die Verfügbarkeit einzuschränken. Ein AS, dessen BGP-Verbindung nachhaltig Ziel von Angriffen ist, hat keine Möglichkeit, am Austausch von Erreichbarkeitsinformationen, und damit am Internet teilzunehmen. [95]

Eine große mittelbare Gefahr geht von den Computern aus, die genutzt werden, um die Router zu administrieren. Wenn diese einen Internetzugriff haben und von den Administratoren für weitere Zwecke genutzt werden, ist ein entfernter Angreifer in der Lage, einen mit Schadsoftware infizierten Computer zu nutzen, um Angriffe gegen das Routing des AS durchzuführen. Möglich sind dabei unter anderem die Änderung der Konfiguration von Routern, das Kopieren, Austauschen oder Löschen von eingesetzten Zertifikaten. [72]

Werden Zertifikate für die Absicherung der Erreichbarkeitsinformationen eingesetzt, sind weitere Angriffe denkbar, die sich vor allem gegen die Zertifizierungsstelle richten. Zwar gibt es Maßnahmen, die Angriffe auf Zertifizierungsstellen deutlich erschweren, insbesondere gegen Innentäter oder gegen den Fall, dass die Zertifizierungsstelle selbst der Angreifer ist schützen diese Maßnahmen in der Regel jedoch nicht. Ein Angriff auf die Verfügbarkeit von Zertifizierungsstellen ermöglicht zumindest eine Verzögerung der Updates von Erreichbarkeitsinformationen. [72]

2.3.4 Monitoring

Um Angriffe gegen Infrastrukturen oder gegen Maßnahmen zur Erreichung von Schutzzielen zu erkennen und adäquat reagieren zu können, ist kontinuierliches Monitoring (vgl. Abschnitt 2.1.4) notwendig. Monitoring von Internetrouting muss auf unterschiedlichen Ebenen stattfinden. Jeder Betreiber eines AS muss die eigenen Router sowie ausgewählte Routen beobachten, um bei auftretenden Anomalien oder Angriffen entsprechende Gegenmaßnahmen einzuleiten.

Neben der AS-individuellen Sicht auf das Internetrouting sollte die globale Sicht ebenfalls überwacht und zur Abwehr von Bedrohungen genutzt werden. Dies ist notwendig, da jedes AS immer nur einen Ausschnitt der tatsächlichen Erreichbarkeitsinformationen erhält, basierend auf der tatsächlichen Routenauswahl der Peers. Aufgrund der notwendigerweise inhärent fehlenden Vertraulichkeit von Internetrouting sind die Erreichbarkeitsinformationen öffentlich verfügbar. Sogenannte *Routingarchive* sammeln empfangene Erreichbarkeitsinformationen unterschiedlicher AS und stellen diese zum Download zur Verfügung. Insbesondere für Forschungszwecke werden diese Daten genutzt, ein anderer Zugang, etwa durch den Betrieb eines eigenen Autonomen Systems, ist für Forscher oft nicht einfach möglich. Eine detaillierte Analyse der in diesen Archiven enthaltenen Daten findet sich in dieser Arbeit in Kapitel 4.

Es existieren unterschiedliche Dienstleister, die eine Überwachung der Erreichbarkeitsinformationen für Autonome Systeme anbieten. ORACLE dyn bietet einen Monitoring-Service für unterschiedliche Zwecke im Bereich Internetrouting [12, 103]. BGPMon [102] etwa ermöglicht die Überwachung der Erreichbarkeit eigener Prefixe. Dafür nutzt BGPMon nicht nur die über Routingarchive beziehbaren Informationen sondern sammelt selbst an unterschiedlichen Stellen im Internet eigene Informationen. Monitoring des Internetroutings bildet somit einen Teil der realisierbaren Maßnahmen zur Sicherstellung der Schutzziele der IT-Sicherheit.

2.4 Zusammenfassung

In diesem Kapitel wurden zunächst die Grundlagen und die übergeordneten Schutzziele der IT-Sicherheit dargestellt. Anschließend erfolgte ein Überblick über die Protokolle, die im Internetrouting (sowohl in der Control-Plane als auch in der Data-Plane) verwendet werden. Auf Basis dieser Informationen wurden die Schutzziele der IT-Sicherheit auf das Internetrouting angewendet, Routinganomalien im Allgemeinen erläutert und ein Angreifermodell entwickelt. Abschließend wurden die Möglichkeiten zum Monitoring von Internetrouting als weitere Maßnahme zur Absicherung des Internetroutings erläutert.

2.4.1 Forschungsfragen

Das implizite gegenseitige Vertrauen von AS im Internet führt unmittelbar zu einer Bedrohung der Schutzziele der IT-Sicherheit. Proaktive Maßnahmen müssten dieses gegenseitige Vertrauen adressieren, was vermutlich eine Erweiterung der eingesetzten Protokolle zur Folge hätte. Um dieser Bedrohung mit reaktiven Mitteln zu begegnen, gibt es derzeit hauptsächlich Mittel zum Monitoring der Erreichbarkeit eigener Prefixe und ausgewählter Pfade. Da eine Änderung etablierter Routingprotokolle aufgrund der dezentralen Struktur des Internets schwierig ist, fokussiert die vorliegende Arbeit reaktive Methoden und beantwortet die in der Einleitung erwähnten Forschungsfragen. Dabei basieren die Inhalte zum Teil auf Ergebnissen, die bereits auf Fachkonferenzen (peer-reviewed) veröffentlicht und der Forschungsgemeinschaft zur Verfügung gestellt wurden:

- **M. Wübbeling**, T.Elsner und M. Meier. Inter-AS Routing Anomalies: Improved Detection and Classification. In: Proceedings of 6th International Conference on Cyber Conflict. P. Brangetto, M. Maybaum, J. Stinissen (Eds.). Tallin. June 2014.
- **M. Wübbeling** und M. Meier. Improved Calculation of AS Resilience Against IP Prefix Hijacking. In: Proceedings of IEEE 41st Conference on Local Computer Networks Workshops. Dubai. Nov. 2016
- **M. Wübbeling** und M. Meier. Reclaim Your Prefix: Mitigation of Prefix Hijacking Using IPSec Tunnels. In: Proceedings of IEEE 42nd Conference on Local Computer Networks. Singapore. Oct. 2017

3 Taxonomie: Routinganomalien

Zusammenfassung des Kapitels Anomalien beeinträchtigen die Stabilität des Routings im Internet. Die unterschiedlichen Ursachen für Routinganomalien liegen dabei sowohl in der Control-Plane als auch in der Data-Plane des Internets. Anomalien können in direkte und indirekte Anomalien sowie Verbindungsfehler unterschieden werden. Direkte Anomalien lassen sich dabei noch weiter in direkte beabsichtigte und direkte unbeabsichtigte Anomalien unterteilen. Multiple-Origin-AS-Konflikte (MOAS-Konflikte) als übergeordnete Klasse von Routinganomalien entstehen in der Control-Plane, wenn zwei AS dasselbe Prefix annoncieren und kein eindeutiges Ziel-AS für die Datenpakete an das betroffene Prefix ermittelt werden kann. Bei MOAS-Konflikten handelt es sich zwar um Anomalien, diese lassen sich jedoch auch für legitime Zwecke, etwa zur Lastverteilung zwischen AS, verwenden. Aus Fehlkonfigurationen oder Angriffen resultierende illegitime MOAS-Konflikte werden als Prefix-Hijacking bezeichnet und bilden den Fokus der vorliegenden Arbeit. Mit Prefix-Hijacking kann ein Angreifer unterschiedliche Ziele verfolgen, die als *Blackholing*, *Imposture* oder *Interception* bezeichnet werden. Dabei ist es für ein betroffenes AS gar nicht ohne weiteres möglich, zu erkennen, dass es Opfer von Prefix-Hijacking ist. Dieses Kapitel führt weiter in die Thematik der Routinganomalien im Internet ein. Es definiert notwendige Begriffe, erläutert die Taxonomie von Routinganomalien in der Literatur und gibt einen Überblick über die Zusammenhänge von MOAS-

Konflikten und Prefix-Hijacking. Abschließend werden anhand von drei unterschiedlichen Fallstudien unterschiedliche Ursachen und Folgen von Prefix-Hijacking aufgezeigt.

Anomalien im Internetrouting führen zu Problemen in der Kommunikation zwischen den Teilnehmern im Internet. Dabei gibt es keine übergeordnete Definition von Routinganomalien sondern je nach Ursache und Wirkung einer Anomalie unterschiedliche Ansätze zur Formalisierung. Der Duden beschreibt eine Anomalie als „Abweichung vom Normalen“ [39]. Als normales Verhalten im Internet kann das betrachtet werden, was etwa von Routingprotokollen wie BGP intendiert wird. Fehler in der Implementierung von BGP führen damit zu einer Art von Routinganomalien im Internet.

Verhalten gilt als normal, wenn es von einer Gruppe von Akteuren als „Norm“ betrachtet wird [123]. Dazu gehört etwa der in den meisten Routern implementierte Algorithmus zur Routenauswahl. Diese Vorgehensweise bei der Routenauswahl ist zwar nicht explizit durch BGP definiert, wird aber von den meisten Herstellern in ähnlicher Weise umgesetzt [139]. Das bedeutet etwa, dass spezifischere Prefixe vor weniger spezifischen Prefixen berücksichtigt werden und dass kürzere AS-Pfade bevorzugt werden. Abweichungen von diesem Verhalten werden ebenso als Anomalie betrachtet. Während die genannten Anomalien ihre Ursache auf der Control-Plane haben, also im Austausch und der Interpretation von Erreichbarkeitsinformationen, können Anomalien im Internetrouting aber auch aus der Data-Plane heraus verursacht werden. Werden mehr Datenpakete über eine Verbindung ausgetauscht, als diese verarbeiten kann, und wird diese Verbindung deshalb instabil, so kann diese nicht mehr beliebig für weitere Datenpakete genutzt werden. Die Datenpakete müssen dann über alternative Pfade in Richtung des Ziels weitergeleitet werden, was auch als Anomalie im Internetrouting betrachtet wird [83].

Routinganomalien im Internet sind also Abweichungen vom intendierten Routingverhalten auf unterschiedlichen Ebenen im Internet. Eine Routinganomalie bedeutet dabei nicht unmittelbar eine Gefahr für die Sicherheit der Kommunikation im Internet. Vielmehr ist die Kritikalität abhängig von der tatsächlichen Ursache und Intention des Verursachers der Routinganomalie. In diesem Kapitel werden Anomalien vorgestellt, die ihre Ursache in der Missachtung von

BGP oder der Normen der AS-Betreiber haben und auf der Control-Plane zu beobachten sind. Anomalien, die in der Data-Plane verursacht werden (engl. traffic anomalies) und die auch als Anomalien im Internetrouting betrachtet werden [83], werden in dieser Arbeit nicht berücksichtigt.

Im folgenden Abschnitt 3.1 werden zunächst unterschiedliche Definitionen und grundlegende Forschungsergebnisse zu Routinganomalien auf der Control-Plane behandelt und eine Taxonomie der BGP-Anomalien aufgezeigt. Anschließend werden in Abschnitt 3.2 Multiple-Origin-AS-Konflikte als übergeordnetes Konzept vorgestellt und in verschiedene Klassen unterteilt. Auf Basis von Multiple-Origin-AS-Konflikten wird in Abschnitt 3.3 Prefix-Hijacking als konkrete Routinganomalie und Bedrohung der IT-Sicherheit diskutiert. Abschließend werden in Abschnitt 3.3.3 drei Fallstudien von Prefix-Hijacking-Vorfällen vorgestellt.

3.1 Grundlagen

Labovitz et al. [79, 80] betrachten Ausfälle als Anomalien im Internetrouting für die Jahre 1997 und 1998. Obwohl die Studie zu einem sehr frühen Zeitpunkt in der Geschichte des Internets stattgefunden hat, gehört sie heute zu den wichtigsten Forschungsarbeiten in diesem Bereich. Als Folgen identifizieren sie Stabilitätsprobleme im Internetrouting, die sich als Paketverlust, erhöhte Netzwerklatenz oder gar einem Verbindungsabbruch darstellen. Dabei untersuchen sie die Anomalien auf die mittlere Betriebsdauer bis zu einem Ausfall (engl. mean time to failure, MTTF) und die Dauer der Anomalie (engl. mean time to repair, MTTR). Labovitz et al. zeigen, dass mehr als 50% der betrachteten Netzwerk-Interfaces eine MTTF von mehr als 40 Tagen haben. Ebenso haben etwa 40% der Fehler eine MTTR von weniger als 10 Minuten, mehr als 80% der Fehler eine MTTR von weniger als 2 Stunden.

Eine Anomalie auf der Control-Plane des Internets kann bereits durch eine oder mehrere BGP-Nachrichten verursacht werden [3, 37, 145]. Dabei wird eine BGP-Nachricht als Anomalie klassifiziert [145], wenn sie entweder:

- eine ungültige AS-Nummer enthält,
- ein ungültiges oder reserviertes Prefix enthält,

- ein Prefix, das von einem nicht legitimierten Ursprung annonciert wird, enthält,
- einen AS-Pfad enthält, dem keine physikalische Verbindung der enthaltenen AS zugrunde liegt oder
- nicht gängigen Routingpolicies entspricht.

Mehrere zusammenhängende BGP-Nachrichten werden als Anomalie klassifiziert [3, 37], wenn sie

- einen unmittelbaren Wechsel in der Frequenz der Nachrichten mit unterschiedlich langen Pfaden aufweisen oder
- für einen gewissen Zeitraum das Routingverhalten maßgeblich verändern, obwohl sich die Struktur des Internets nicht maßgeblich verändert hat.

Musawi et al. [96] haben eine Taxonomie der BGP-Anomalien, also der Anomalien auf der Control-Plane, erstellt und entsprechend Abbildung 5 vier unterschiedliche Klassen definiert. Die Klassen *indirekte Anomalien* und *Verbindungsfehler* haben, wie zu Beginn dieses Kapitels bereits erwähnt, ihre Ursache nicht in der Control-Plane von BGP, sondern führen aufgrund anderer Umstände zu Anomalien im Internetrouting. Daher werden weiterhin nur die beiden Klassen der *direkten unbeabsichtigten Anomalien* und der *direkten beabsichtigten Anomalien* betrachtet.

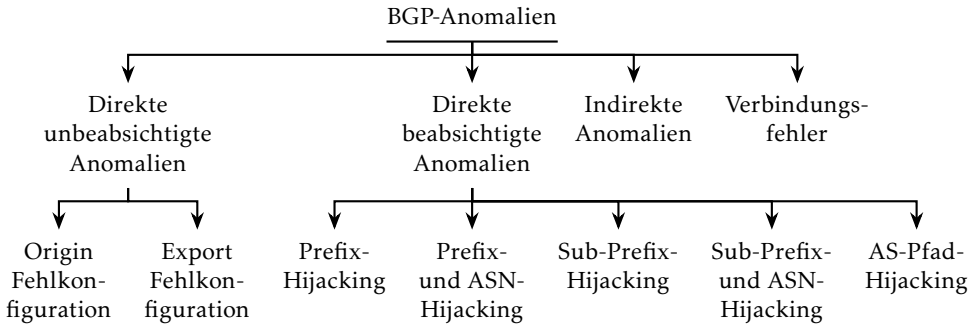

Abbildung 5: *Taxonomie der BGP-Anomalien [96]*

3.1.1 Direkte unbeabsichtigte Anomalien

Mahajan et al. [89] betrachten Fehlkonfigurationen des BGP in Routern durch Administratoren. Dabei unterscheiden sie zwei Arten von Fehlkonfigurationen, die durch Beobachtung der Control-Plane erkannt werden können:

Origin-Fehlkonfiguration - Ein AS annonciert fälschlicherweise einen Prefix. Diese Fehlkonfiguration wird weiter unterteilt in i) fehlende Aggregation von Subnetzen in einen gemeinsamen Prefix, ii) Prefix-Hijacking, also das Announcement des Prefixes eines anderen AS und iii) das Annoncieren von Prefixen, die für den internen Gebrauch gedacht sind.

Export-Fehlkonfiguration - Ein AS leitet Routen weiter, die eigentlich gefiltert werden sollten, etwa zur Sicherstellung des Paradigmas der Tal-Freiheit (vgl. Abschnitt 2.2.2).

Mahajan et al. zählen weitere Arten von Fehlkonfigurationen auf. Dazu gehören das versehentliche Filtern von Routen, die eigentlich weitergeleitet werden sollen oder die fehlerhafte Gewichtung der Routen, so dass Datenverkehr fehlgeleitet wird. Diese Fehlkonfigurationen betreffen aber zumeist nur ein oder zwei AS und sind daher nicht ohne weiteres auf der Control-Plane beobachtbar. [89]

Mahajan et al. führten eine Umfrage unter Administratoren betroffener AS durch, um die Ursachen für Fehlkonfigurationen weiter zu untersuchen. Als häufigen Grund für Fehlkonfigurationen nennen Administratoren etwa die Verwendung alter Konfigurationsdateien in den Routern. Wird die geänderte Konfiguration eines Routers nicht explizit gespeichert, lädt der Router bei einem Neustart die zuletzt gespeicherte Konfiguration. Ein Hinweis auf eine nicht gespeicherte Konfiguration fehlt in den meisten Router-Betriebssystemen. [89]

Als Ursache für versehentliches Prefix-Hijacking geben die Administratoren Tippfehler bei der Konfiguration eigener Prefixe an. Eine weitere Möglichkeit für Prefix-Hijacking sind fehlerhafte Backup-Pfade. Manche AS vereinbaren mit zusätzlichen Upstream-Providern die Möglichkeit zur Annoncierung des eigenen Prefixes, falls der primäre Upstream-Provider nicht erreichbar ist. So

ist es möglich, dass der sekundäre Upstream-Provider während einer vorübergehenden Nichterreichbarkeit des primären Upstream-Providers das Prefix annonciert, diesen aber nicht rechtzeitig wieder zurückzieht. [89]

Prefix-Hijacking intendiert von der Begrifflichkeit eine bösartige Absicht, auch wenn Mahajan et al. Prefix-Hijacking als Folge von Fehlkonfiguration aufzählen. Für eine neutrale Betrachtung solcher Szenarien eignet sich in der Literatur der Begriff mehrfacher Origin-AS (engl. Multiple Origin AS, MOAS). MOAS und Sub-MOAS (bzw. Sub-Prefix) werden in Abschnitt 3.2.1 detailliert beschrieben.

3.1.2 Direkte beabsichtigte Anomalien

Vier der fünf dargestellten Unterkategorien beinhalten das Announcement fremder Prefixe oder Sub-Prefixe sowie fremder AS-Nummern. Vor allem die Sub-Prefix-Hijacking-Anomalien (mit oder ohne AS-Nummern) lassen sich in der Regel nur mit einer sehr umfassenden Datenbasis entdecken [61]. Mit den vorhandenen Daten aus Routingarchiven sind diese Anomalien im Grunde gar nicht zu erkennen, da die Existenz von Subnetzen im globalen Routing ein Effekt des CIDR ist (vgl. Abschnitt 2.2.4). Aus diesem Grund ist Sub-Prefix-Hijacking nicht im Fokus dieser Arbeit.

Bei den mit ASN-Hijacking bezeichneten Klassen handelt es sich eigentlich eher um Topologie-Anomalien in Form von AS-Pfadmanipulationen, weshalb der Begriff Hijacking an dieser Stelle nicht gut geeignet ist. Daher wird im Folgenden zwischen Prefix-Hijacking und AS-Pfadmanipulation unterschieden. Abbildung 6 verdeutlich die beiden Anomalien beispielhaft. Aufgrund der Relevanz von Prefix-Hijacking für diese Arbeit erfolgt eine umfassende Diskussion von Prefix-Hijacking im nächsten Abschnitt 3.2. Im Gegensatz zu Prefix-Hijacking sind AS-Pfadmanipulation, abgesehen von Fehlern in der Routersoftware, nicht versehentlich möglich. Es handelt sich daher fast immer um gezielte Manipulationen der in BGP-Nachrichten enthaltenen AS-Pfade. Das Ziel eines Angreifers ist dabei mit möglichst kurzen Pfaden in den Announcements Datenverkehr für ein gewisses Ziel über sich selbst umzuleiten (vgl. Abschnitt 2.3.3).

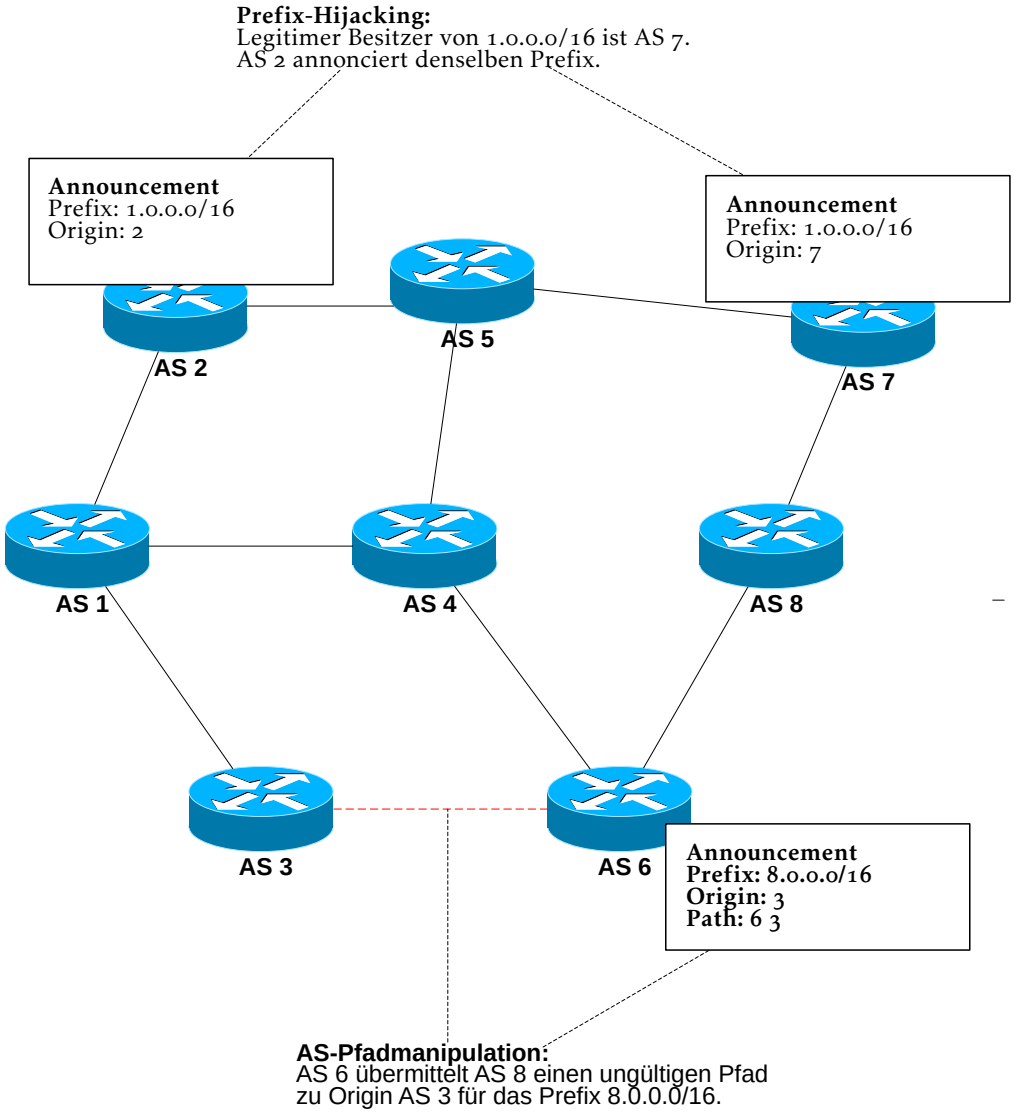

Abbildung 6: *Prefix-Hijacking und AS-Pfadmanipulation*

3.2 Multiple Origin AS (MOAS)

Für jedes Prefix ist ein einzelnes AS als Origin vorgesehen [58]. Beanspruchen im Internet zwei AS dasselbe Prefix für sich, handelt es sich um eine Routinganomalie. Zhao et al. erkennen legitime Gründe für diese Form der Routinganomalie und prägen als erste für diesen Fall den Begriff „Multiple Origin AS“ [151] im Kontrast zu dem negativ bewerteten Begriff des Prefix-Hijacking. Zwei AS, die denselben Prefix annoncieren stehen damit jedoch immer noch in einem Konflikt zueinander. MOAS-Konflikte sind theoretisch leicht zu erkennen: es existieren Routen für dasselbe Prefix mit unterschiedlichem Origin. Schwierigkeiten bei der Erkennung werden in Abschnitt 3.3.2 verdeutlicht. Zhao et al. [151] unterscheiden dabei valide MOAS-Konflikte, wo ein gemeinsames operatives Ziel der AS im Vordergrund steht, von invaliden MOAS-Konflikten, die aus einer Fehlkonfiguration oder einem gezielten Angriff resultieren. Die von Zhao et al. gewählten Begriffe „valid“ und „invalid“ sind in diesem Kontext besser mit *legitim* und *illegitim* übersetzt. MOAS-Konflikte lassen sich also legitim durch Prefixbesitzer nutzen, um eine Art Load-Balancing zu implementieren oder möglichst kurze Wege für Kunden zu bestimmten Diensten anzubieten. Somit ist es schwierig, für erkannte MOAS-Konflikten zu entscheiden, ob diese legitim oder illegitim, also vom Prefixbesitzer intendiert oder Folge eines gezielten Angriffs, sind. Gezielte Angriffe durch MOAS-Konflikte werden zur besseren Unterscheidbarkeit im Folgenden als Prefix-Hijacking bezeichnet.

3.2.1 Sub-MOAS-Konflikte

Annonciert ein AS nur einen Teilbereich des Prefix eines anderen AS, entsteht ein sogenannter Sub-MOAS-Konflikt [61]. Eigentlich handelt es sich dabei nicht um einen Konflikt, sondern vielmehr um eine gewollte Eigenschaft des klassenlosen Internetroutings (CIDR). Somit ist es möglich, viele kleinere Prefix eines AS zu einem größeren Prefix zusammenzufassen (engl. supernetting) [48]. Eine Idee dieser Zusammenfassung ist, die Anzahl der Einträge in Routingtabellen zu reduzieren [48]. Daher gibt es viele legitime Sub-MOAS-Konflikte.

Beispiel: Legitime Sub-MOAS-Konflikte
Ein kleiner Bereich des Prefix eines großen Unternehmens (Sub-Prefix) ist einem einzelnen Geschäftsbereich zugeordnet. Bei einem Verkauf dieses Geschäftsbereichs an einen Mitbewerber soll dieser Sub-Prefix ebenfalls mit an den neuen Eigentümer übertragen werden. Der übergeordnete Prefix bleibt im Besitz des alten Eigentümers und der neue Eigentümer annonciert lediglich diesen spezifischeren Prefix. Da bei der Routenauswahl immer die Routen zu den spezifischeren Prefixen bevorzugt werden, muss der alte Eigentümer die Konfiguration seines AS nicht verändern. Alle Pakete mit einem Ziel innerhalb des übergeordneten Prefix werden an das AS des alten Eigentürmers gesendet, nur für die innerhalb des Sub-Prefix liegenden Adressen werden die Pakete direkt an den neuen Eigentümer gesendet.

Aufgrund der geringen Anzahl verfügbarer IPv4-Adressen im Internet und der großen Nachfrage dieser Adressen in den letzten Jahren, haben viele Organisationen kleine Sub-Prefixe ihrer sehr großen Prefixe verkauft. Dies führt dazu, dass AS mitunter viele kleine Prefixe besitzen, die nicht zusammenhängend sind. Somit lassen sich die Prefixe nicht aggregieren und die Anzahl der Einträge in Routingtabellen steigt kontinuierlich. Eine Änderung in der Konfiguration der großen Prefixe ist für die Erreichbarkeit der kleinen Prefixe nicht nötig, Sub-MOAS-Konflikte haben daher vermutlich häufig eine legitime Ursache.

Neben den legitimen Ursachen gibt es aber auch Fälle von Sub-Prefix-Hijacking, also dem gezielten Announcement eines Sub-Prefix als Angriff auf ein AS. Häufig wird aus einem Sub-Prefix-Hijacking durch Announcements desselben Prefix durch den legitimen Besitzer ein reguläres Prefix-Hijacking (vgl. Abschnitt 3.3 und Abschnitt 3.3.3).

3.2.2 Legitime MOAS-Konflikte

MOAS-Konflikte eignen sich für legitime Zwecke. Soll derselbe Dienst aus unterschiedlichen AS angeboten werden, etwa zur Lastverteilung (engl. load balancing) oder zur Ausfallsicherheit, gibt es unterschiedliche Techniken zur Verteilung der Last. Häufig werden zur Lastverteilung keine MOAS-Konflikte sondern Techniken aus dem Domain-Name-System verwendet [23]. Einem

Domänen-Namen werden dabei mehrere IP-Adressen zugeordnet und anfragende Systeme wählen zufällig eine dieser IP-Adressen für ihre Anfrage aus. Als Alternative zur Lastverteilung mit DNS lassen sich also MOAS-Konflikte legitim zur Lastverteilung auf Basis von IP-Adressen verwenden [89]. MOAS ist damit eine Möglichkeit zur Implementierung von Anycast [1]. Ein bekanntes Beispiel, bei dem Anycast auf Basis von BGP eingesetzt wird, sind DNS-Rootserver [116].

Im Gegensatz zu Sub-MOAS-Konflikten ist bei MOAS-Konflikten nicht eindeutig, zu welchem AS ein Paket an den betroffenen Prefix geleitet werden soll. Die Entscheidung für ein AS im Rahmen der Lastverteilung findet also durch die Routenauswahl implizit statt.

Beispiel: Anycast mit BGP
Es gibt 13 unterschiedliche DNS-Rootserver, die von verschiedenen Organisationen betrieben werden [64]. Das Unternehmen VeriSign betreibt die beiden Rootserver a.root-servers.net (198.41.0.4) und j.root-servers.net (192.58.128.30). Die Prefixe 198.41.0.0/24 und 192.58.128.0/24 werden dabei von 25 bzw. 17 unterschiedlichen Origins annonciert (Stand: April 2019). Das Unternehmen Internet Systems Consortium, Inc. (ISC) betreibt den Rootserver f.root-servers.net mit der IP-Adresse 192.5.5.241. Der von ISC verwendete Prefix 192.5.5.0/24 wird von zwei unterschiedlichen Origins annonciert (Stand: April 2019). [62]

Legitime MOAS-Konflikte können auch das Resultat mehrerer Upstream-Provider sein. Ein AS beauftragt dann mehrere seiner Upstream-Provider mit dem Announcement seines eigenen Prefixes. Damit gibt es ebenfalls Load-Balancing, wenngleich nur auf dem Weg zu dem Besitzer des Prefixes. Ein solches Szenario bietet also Sicherheit beim Ausfall eines Upstream-Providers, nicht aber bei einem Ausfall des Prefixbesitzers. [13]

3.2.3 Illegitime MOAS-Konflikte

Illegitime MOAS-Konflikte resultieren etwa aus einer Fehlkonfiguration (vgl. Abschnitt 3.1) oder einem gezielten Angriff. Insbesondere für den letzten Fall hat sich der Begriff des Prefix-Hijacking etabliert. Eine Einteilung der MOAS-

Konflikte in legitime und illegitime MOAS-Konflikte ist nicht ohne Befragung aller an einem Konflikt teilnehmenden AS möglich. Zhao et al. argumentieren bei der Einteilung von Konflikten über die Dauer eines MOAS-Konflikts, können aber nicht schlussendlich entscheiden, wie Intervalle den unterschiedlichen Ursachen zugeordnet werden können [151]. Der Fokus dieser Arbeit liegt auf Prefix-Hijacking als Angriff auf das Internetrouting. Prefix-Hijacking als illegitimer MOAS-Konflikt wird daher im nachfolgenden Abschnitt gesondert betrachtet.

3.3 Prefix-Hijacking

Mahajan et al. unterscheiden Origin-Fehlkonfigurationen in drei unterschiedliche Kategorien (vgl. Abschnitt 3.1). Prefix-Hijacking ist die einzige der drei Kategorien, die unmittelbar andere AS im Internet beeinträchtigt. Damit beschreibt Prefix-Hijacking gezielte Angriffe gegen AS und stellt somit eine eigene Kategorie der Routinganomalien dar. Beim Prefix-Hijacking annonciert ein AS (Angreifer) das Prefix eines anderen AS (Opfer oder Ziel) und bringt somit dritte AS dazu, Datenverkehr für das Opfer in Richtung des Angreifers weiterzuleiten.

Effektive Gegenmaßnahmen gegen Prefix Hijacking, also die Übernahme eines Prefix durch die Herausgabe entsprechender Erreichbarkeitsinformationen ohne die Zustimmung des eigentlichen Prefixbesitzers, werden nicht auf breiter Basis eingesetzt. Aufgrund von Performanceproblemen auf Internet-Core-Routern und weil Protokollerweiterungen wie S-BGP [73], so-BGP [142] oder RPKI [84] nicht in der Breite eingesetzt werden, gibt es diese Bedrohungen also bis heute ohne wirksamen Schutzmechanismus. Tatsächlich müssten diese Mechanismen zur Prüfung der Herkunft von Erreichbarkeitsinformationen von möglichst allen AS eingesetzt und überprüft werden, um einen effektiven Schutz zu bieten. Bis dahin bleibt das gesamt Routingsystem anfällig gegen gezielte Angriffe. Es genügt schon, wenn ein AS auf dem Pfad zum gewünschten Ziel die erstellten Zertifikate nicht überprüft und ankommende Pakete in Richtung eines Angreifers weiterleitet.

Tritt ein Prefix-Hijacking auf, können die legitimen Prefixbesitzer nur begrenzt reagieren. Als erste Gegenwehr ist es möglich, spezifischere Prefixe zu veröf-

fentlichen (vgl. Abschnitt 3.2.1). Diese Prefixe werden bei der Routenauswahl bevorzugt und ein Angreifer würde auf diesem Wege zunächst keine Datenpakete mehr erhalten. Viele Fälle von Prefix-Hijacking sind zwar grundsätzlich öffentlich bekannt, aber nur wenige werden öffentlich diskutiert. Meist sind es solche, bei denen Prefixe großer Internet-Unternehmen betroffen sind, wie YouTube [119], Google [53] oder Amazon [87].

3.3.1 Ziele eines Prefix-Hijackers

Es gibt unterschiedliche Folgen eines Prefix-Hijacking und damit auch unterschiedliche Ziele eines Angreifers. Zheng et al. [153] listen drei unterschiedliche Ziele eines Angreifers auf:

- Der Angreifer verwirft die fälschlicherweise an ihn zugestellten Pakete (engl. blackholing).
- Der Angreifer antwortet auf Anfragen und imitiert dabei den Prefixbesitzer (engl. imposture).
- Der Angreifer kann die Anfragen speichern, lesen oder verändern und leitet sie anschließend an den Prefixbesitzer weiter (engl. interception).

Alle Angriffe eignen sich dazu, sowohl dem anfragenden AS als auch dem Prefixbesitzer zu schaden. Die betroffenen Schutzziele unterscheiden sich dabei jedoch. Die Nutzung fremder Prefixe für den Versand von SPAM ist ein immer wieder auftretendes Phänomen [132]. Blackholing schränkt dabei die Verfügbarkeit, Imposture sowohl die Vertraulichkeit als auch die Zurechenbarkeit und Interception die Vertraulichkeit sowie die Integrität maßgeblich ein. Die Verschlüsselung und die Signatur der Datenpakete können zwar die Schutzziele Zurechenbarkeit, Vertraulichkeit und Integrität sicherstellen, allerdings werden die resultierenden Mechanismen dann zu einer Nicht-Verfügbarkeit führen, da der Verbindungsaufbau nicht zustande kommt. Ein Angreifer kann also zumindest die Verfügbarkeit eines Prefixes durch Prefix-Hijacking einschränken.

3.3.2 Erkennung von Prefix-Hijacking

Theoretisch ist die Erkennung von Prefix-Hijacking auf der Control-Plane einfach. Alle BGP-Nachrichten werden untersucht und die in den Announcements

angegebenen Origins ermittelt. Gibt es mehr als ein AS, das als Origin für ein Prefix vorkommt, wurde ein MOAS-Konflikt erkannt. Für die Erkennung von Prefix-Hijacking muss dieser MOAS-Konflikt anschließend als illegitim eingestuft werden. Für diese Einstufung sind weitere Informationen nötig. Eine fehlerfreie Einstufung ist nur durch die Bestätigung des Prefixbesitzers, also des legitimen Origins, möglich. Dieser erfährt aber über die Control-Plane selbst nichts von dem Prefix-Hijacking, da entsprechende Announcements zur Vermeidung von Anomalien (etwa von Kreisen in den AS-Pfaden) gar nicht bis zum Origin des Prefix weitergereicht werden. Um die Besitzer von Prefixen zu informieren haben etwa Lad et al. [82] das „Prefix Hijacking Alert System“ (PHAS) entwickelt. Dieses betreibt mehrere Beobachtungspunkte, an denen die Announcements analysiert werden und informiert ein betroffenes AS per E-Mail, falls ein weiteres AS den beobachteten Prefix annonciert.

Qiu et al. [111] analysieren AS-Pfade, die an unterschiedlichen Beobachtungspunkten ermittelt werden. Unter anderem konnten sie auch Prefix-Hijacking mit einer sehr geringen Falsch-Positiv-Rate erkennen, ein Abgleich der Daten fand gegen bereits bekannte Prefix-Hijacking-Vorfälle statt. Eine Information des Prefixbesitzers oder anderer betroffener AS ist in dem Ansatz nicht vorgesehen. In einer nachfolgenden Untersuchung zeigen Qiu et al. [112], dass sie mit entsprechenden Beobachtungspunkten über die ermittelten tatsächlichen Pfade den Verursacher eines Prefix-Hijacking lokalisieren können. Dabei liegt der Fokus jedoch nicht auf MOAS-Konflikten sondern auf AS-Pfaden, die durch den Angreifer manipuliert werden.

Zheng et al. [153] beobachten Veränderungen der mittels Traceroute auf der Data-Plane ermittelten Pfade. Sie zeigen, dass es möglich ist, Prefix-Hijacking über die Anzahl der Hops und der konkreten Pfade zu einem Ziel zu erkennen. Zusätzlich zum legitimen Origin eines Prefix speichert das System weitere AS als Referenzpunkte, deren Prefixe einen zu teilen gleichen Pfad haben. Änderungen im Routing, etwa durch eine defekte Route, müssten dann ebenfalls Auswirkungen auf die Pfade zu den Prefixen der Referenzpunkte haben.

Hu und Mao [61] haben eine Methode entwickelt, mit der sie auch ohne die Mithilfe des Prefixbesitzers eine Klassifikation vornehmen können. Dafür erkennen sie die innerhalb eines Prefix angebotenen Dienste und vergleichen ausge-

hend von unterschiedlichen Beobachtungspunkten die Antworten der Dienste über alle aktiven Origins. Aus den Antworten leiten sie einen Fingerabdruck ab, der sich dann über alle Origins gleichen müsste, wenn es sich um einen legitimen MOAS-Konflikt handelt. Bei dieser Methode gibt es jedoch Einschränkungen. Die Klassifikation eines MOAS-Konflikts ist nur solange möglich, wie der MOAS-Konflikt existiert, eine retrospektive Untersuchung ist damit nicht möglich. Darüber hinaus müssen ausreichend viele Beobachtungspunkte existieren, so dass in jedem Fall eine Kommunikation mit allen Origins möglich ist.

Die in einer späteren Arbeit von Zhang et al. [150] vorgeschlagene Methode zur Erkennung von Prefix-Hijacking verbindet das Monitoring der Control-Plane und der Data-Plane. Im Gegensatz zu anderen Ansätzen ist diese Methode fokussiert auf den Prefixbesitzer selbst. Durch das Monitoring der Erreichbarkeit von etwa 3.000 Transit-AS ist es einem AS möglich, zu ermitteln, ob es Opfer eines Prefix-Hijacking ist. Während die Anfragen des Prefixbesitzers die Transit-AS ohne Probleme erreichen, werden die Antworten im Falle eines Prefix-Hijacking von einem Teil der beobachteten AS an das illegitime Origin weitergeleitet. Dies resultiert darin, dass keine Verbindung zwischen Transit-AS und dem legitimen Origin aufgebaut werden kann.

3.3.3 Fallstudien

Um ein Verständnis über den Ablauf von Prefix-Hijacking-Vorfällen zu erhalten, sollen an dieser Stelle bedeutende Fallstudien vorgestellt werden. Aufgrund der Menge an Vorfällen sollen an dieser Stelle nur drei Vorfälle betrachtet werden, die exemplarisch unterschiedliche Aspekte von Prefix-Hijacking verdeutlichen: Hardware-Fehler, Fehlkonfiguration und gezielte Angriffe. Die genannten Vorfälle werden auf vielen Webseiten und Blogs erwähnt und diskutiert. Eine Auflistung all dieser Quellen ist an dieser Stelle nicht sinnvoll, so dass sich die angegebene Literatur aus Gründen der Übersichtlichkeit fast ausschließlich auf Literatur bezieht, die auch an anderen Stellen dieser Arbeit verwendet wird.

AS 7007; April 1997

Im April 1997 annoncierte der regionale ISP MAI Network Service von seinem AS 7007 einen Großteil der weltweiten Routingtabelle mit seiner eigenen AS-Nummer als Origin an seinen Upstream-Provider SPRINT [32]. Bereits kurz darauf wurden Administratoren anderer AS auf den Fehler aufmerksam und veröffentlichten Nachrichten über die Mailingliste der North American Network Operators Group (NANOG) mit Hinweisen auf den Verursacher [93]. In einer Nachricht an die Mailingliste der NANOG äußerte sich das Unternehmen einen Tag später mit einer Entschuldigung und einer Erklärung für den Vorfall [21]. Ursächlich für den Vorfall war laut der Erklärung des Unternehmens ein nicht intendiertes Verhalten des Routers, der offenbar fehlerhafte Routen eines Kunden ungefiltert weiter verbreitet hat. Obwohl die Reaktion der Betreiber kurz nach dem Auftreten erfolgte, dauerte es etwa 6 Stunden, bis der Vorfall beendet war. Obwohl dieser Vorfall bereits 1997 eingetreten ist, wird er über Jahre später noch immer in der Literatur erwähnt [7, 61, 69, 75, 85, 89, 111, 130, 140, 149, 151]. Die Möglichkeit zur Kommunikation über die Mailingliste deutet darauf hin, dass der zugehörige Prefix der Mailingliste selbst nicht betroffen war, allerdings wurde dies von keiner der genannten Quellen näher untersucht. Da E-Mails als Datum den Zeitstempel des Versands tragen, ist es jedoch auch möglich, dass E-Mails erst im Anschluss an den Vorfall zugestellt wurden.

YouTube Hijacking; Februar 2008

Der wohl am häufigsten genannte Vorfall von Prefix-Hijacking in der Literatur ging im Jahr 2008 von der Pakistan Telecommunication Company Limited (PTCL) aus. Da in diesem Fall gezielt das Prefix eines Unternehmens betroffen war, wird dieser Vorfall im Gegensatz zu dem AS-7007-Vorfall von 1997 nicht nach dem Verursacher, sondern nach dem Opfer benannt. Das RIPE Network-Coordination-Centre (RIPE NCC) hat den Vorfall in einer Fallstudie näher betrachtet [119].

Das AS 17557 der PTCL annoncierte das Prefix 208.65.153.0/24 an seinen Upstream-Provider PCCW Global. Da YouTube zu dem Zeitpunkt das übergeordnete Prefix 208.65.152.0/22 annoncierte, wurde das falsche Announcement

weltweit in allen AS umgesetzt. In diesem Fall handelt es sich also um ein Sub-Prefix-Hijacking. Die Reaktion von YouTube gut 90 Minuten später war das Announcement des betroffenen /24-Prefix, so wurde aus dem Sub-Prefix-Hijacking ein Prefix-Hijacking. Ab diesem Zeitpunkt waren noch die AS betroffen, die einen kürzeren AS-Pfad zu dem AS 17557 der PTCL hatten. Um das Prefix-Hijacking weiter einzudämmen, annoncierte YouTube anschließend noch die beiden zugehörigen /25-Prefixe. Obwohl diese normalerweise gefiltert werden (vgl. Abschnitt 2.2.4), versuchte YouTube alle AS ohne zuverlässige Filterung mit den korrekten Routen zu versorgen. Dieser Vorfall endete nach etwas mehr als 2 Stunden damit, dass der Upstream-Provider der PTCL die Routen seines Kunden gefiltert und aktiv zurückgezogen hat. [119]

Das YouTube-Hijacking wird, ähnlich wie der AS-7007-Vorfall häufig in der Literatur referenziert [17, 69, 75, 85, 96, 105, 112, 121, 125, 126, 127, 129, 148].

Link Telecom Hijacking; April - August 2011

Von April bis August 2011 annonciert ein Angreifer nach und nach Prefixe des insolventen russischen Unternehmens Link Telecom. Erst nach etwa 4 Monaten fällt dem Unternehmen auf, dass die eigenen Prefixe regelmäßig auf Blacklisten zur Vermeidung von E-Mail-SPAM landen und Upstream-Provider diese Prefixe daher filtern [133]. Die Nutzung fremder Prefixe für den Versand von SPAM ist ein immer wieder auftretendes Phänomen [132].

Der Angreifer hat seit April 2011 nach und nach die nicht genutzten Prefixe von Link Telecom annonciert, um neue IP-Adressen zu erhalten, die noch nicht auf entsprechenden Blacklisten eingetragen sind. Von diesen IP-Adressen wurden dann über den gesamten Zeitraum SPAM-E-Mails versendet, so dass die betroffenen IP-Adressbereiche nach kurzer Zeit weitgehend geblockt wurden. Erst im September waren die betroffenen Routen wieder voll unter der Kontrolle von Link Telecom. [124]

Im Gegensatz zu den beiden vorigen Prefix-Hijacking-Vorfällen handelt es sich bei dem Link Telecom Hijacking um einen tatsächlich nachgewiesenen Angriff auf die Prefixe eines Unternehmens. Ähnliche nachgewiesene Angriffe zielen etwa auf die Kommunikation von Bitcoin-Netzwerken, um innerhalb der Netzwerke gefundene Bitcoins zu stehlen [92]. Solche Vorfälle verdeutlichen, dass

hinter Prefix-Hijacking unterschiedliche Motive stecken und sich auch Kriminelle dieser Technik bedienen können. In der Literatur ist der Link Telecom Vorfall dennoch weniger relevant [17, 69, 124, 125].

4 Daten: Datenquellen und Realitätsabgleich[4]

Zusammenfassung des Kapitels Für die Analyse des Internetroutings und zur Erkennung von Anomalien werden Daten aus der Control-Plane des Internets benötigt. Nur so lässt sich feststellen, welche Erreichbarkeitsinformationen zwischen den AS ausgetauscht werden. Nur wenige AS veröffentlichen die von ihnen erhaltenen Erreichbarkeitsinformationen unmittelbar. Kaum mehr als 500 AS beteiligen sich jedoch an der maßgeblich von der Forschung getriebenen Sammlung dieser relevanten Daten. Routingarchive sammeln und archivieren die Erreichbarkeitsinformationen, die ihnen von den teilnehmenden AS zur Verfügung gestellt werden. In unterschiedlichen Datenformaten werden sowohl aktuelle als auch historische Routingdaten zum Download angeboten. Die bereitgestellten Daten werden in der Forschung zur Analyse der Geschäftsbeziehungen zwischen AS oder zur Erkennung von Anomalien im Internetrouting, wie etwa Prefix-Hijacking, herangezogen. Da jedes AS eine leicht unterschiedliche Sicht auf das Internetrouting besitzt und aufgrund der geringen Anzahl teilnehmender AS lässt sich mit den Daten der Routingarchive nur eine Annäherung an die Realität erreichen. In diesem Kapitel werden die Daten der vier bekannten Routingarchive Routeviews, RIPE RIS, PCH und Isolario miteinander verglichen und Schnittmengen sowie Unterschiede analysiert. Dies erlaubt abschließend die optimierte Auswahl der Beobachtungspunkte für die Forschung im Kontext von Anomali-

[4] Die Inhalte basieren auf bisher nicht veröffentlichten eigenen Arbeiten

en im Internetrouting, so dass trotz der großen Datenmenge aller Archive möglichst umfassend die Informationen der Control-Plane berücksichtigt werden können und Redundanz verringert wird.

Geringe technische Hürden zur Teilnahme am Internet und die einfache Umsetzung des Internetroutings haben maßgeblich zum Erfolg dieses globalen Netzwerks beigetragen. Internetrouting ist ein dynamisches Konstrukt, welches minütlich vielen Tausend Änderungen unterliegt. Die Forschung in diesem Bereich stützt sich daher auf unterschiedliche Annahmen und Regelmäßigkeiten dieses Systems. Dazu gehört etwa eine Topologie auf Basis von Geschäftsbeziehungen, die eine Einteilung der AS in unterschiedliche Ebenen erlaubt: Tier-1 für global bedeutende, miteinander verbundene AS als Kern des Internets, bis hin zu Tier-3 für lokale Internetdienstleister mit wenigen Verbindungen, die graphentheoretisch am Rand des Internets liegen. Eine weitere Annahme ist das Paradigma der Tal-Freiheit von AS-Pfaden (vgl. Abschnitt 2.2.3).

Simulationen haben sich zur Evaluation von Forschungsergebnissen etabliert, diese basieren zumeist auf historischen Routingdaten. Diese Daten werden an unterschiedlichen Orten des Internets aufgezeichnet, über Routingarchive gesammelt und der Öffentlichkeit zur Verfügung gestellt. Dieses Kapitel beschreibt zunächst die verwendeten Methoden zur Sammlung solcher Routingdaten. Die in öffentlichen Routingarchiven enthaltenen Informationen werden analysiert und so unterschiedliche Anbieter verglichen. Anschließend werden Schwierigkeiten beim Realitätsabgleich thematisiert und daraus resultierende Probleme aufgezeigt.

4.1 Route-Reflektoren

Der Austausch von Routingdaten zwischen Border-Routern Autonomer Systeme ist bereits in Kapitel 2.2.4 dargestellt. Je nach internem Aufbau eines AS lassen sich diese empfangenen Routingdaten vom Border-Router auch an interne Router weiterleiten. Solche Daten werden insbesondere dann genutzt, wenn es mehrere Border-Router mit unterschiedlichen Verbindungen zu anderen AS gibt. Interne Router können dann bereits Datenpakete innerhalb des AS zu dem Border-Router weiterleiten, der einen kürzeren oder kostengünstigeren

Weg bereitstellt. Dafür werden die Border-Router so konfiguriert, dass sie als *Route-Reflektoren* funktionieren. Durch Route-Reflektoren werden eingehende Routingdaten (Updates) an die konfigurierten *Route-Reflektor-Clients* (RRCs) weitergeleitet. Als RRC kann an dieser Stelle auch Routingsoftware verwendet werden, etwa Quagga [136], die in der Lage ist, erhaltene Routen in Logdaten abzuspeichern. Praktisch können diese RRCs auch in anderen Netzen liegen und somit Routen mehrerer verbundener AS an einem zentralen Punkt sammeln. Die Routingdaten werden von den meisten RRCs im MRT-Format (Multi-Threaded Routing Toolkit (MRT) Routing Information Export Format) [18] in Dateien geschrieben und von dort in regelmäßigen Update-Intervallen in Routingarchive geladen.

Zusätzlich zu den Updates erstellen die RRCs in regelmäßigen Abständen eine Übersicht der aktuellen Routingtabelle. Dabei werden nur Einträge berücksichtigt, die in der BGP-Datenbank (engl. Route Information Base, RIB) vorhanden sind. Da innerhalb eines AS auch andere Routingprotokolle verwendet werden können, wird die tatsächliche Routingtabelle eines Routers aus allen RIBs der verwendeten Routingprotokolle zusammengesetzt. Die Daten aus den RIBs der RRCs werden je nach Anbieter als „rib“, „bview“ oder „snapshot“ bezeichnet.

4.2 Verwandte Arbeiten

Eine wissenschaftliche qualitative Analyse aller Aspekte öffentlich verfügbarer Routingarchive wurde bisher nicht veröffentlicht. Es gibt jedoch Arbeiten, die einen Vergleich von Routingarchiven durchführen. Das Ziel der meisten Arbeiten in diesem Bereich ist die Erstellung einer AS-Topologie, also einer Art Landkarte für das Internet.

Khan et al. [74] nutzen BGP-Funktionen von Looking-Glass-Servern (vgl. Abschnitt 5.2), um Routingtabellen direkt abzufragen. Dabei vergleichen sie die verbundenen AS von Routeviews, RIPE RIS und PCH (vgl. Abschnitt 4.3) mit den von ihnen über Looking-Glass abgefragten Routern. Zusätzlich ermitteln sie über die IP-Adresse der Router, ob der Router als Route-Reflektor eingesetzt wird und zusätzlich über Looking-Glass abgefragt werden kann. Dabei vergleichen sie nicht nur die Router selbst sondern auch die Nachbar-AS der

abgefragten Router. Leider fehlt eine Übersicht, welche RRCs der Archive verwendet wurden, ebenso findet eine Analyse der ausgetauschten Erreichbarkeitsinformationen auf dieser Ebene nicht statt. Verbindungen zwischen AS werden ausschließlich mit Topologieprojekten vom IRL [66] oder CAIDA [25] verglichen, die zwar auch die Routingarchive von RIPE RIS, Routeviews und PCH verwenden, allerdings ist so ein unmittelbarer Vergleich der Routingarchive untereinander nicht möglich.

Chang et al. [27] vergleichen die Daten von Routeviews mit den Daten von Looking-Glass-Servern und Routingpolicy-Informationen aus den Datenbanken der RIRs. Während die Menge der gefundenen AS nur geringfügig abweicht, können Chang et al. bis zu 40% mehr Peerings erkennen als allein auf Basis der Daten von Routeviews möglich war. Sie zeigen auch, dass bis zu 80% der Peerings einzelner AS nicht über die gesammelten Daten der Control-Plane sichtbar sind.

Chen et al. [30] untersuchen Unterschiede in der Sicht einzelner Beobachtungspunkte. Ein Beobachtungspunkt entspricht dabei einem Route-Reflektor der Routingarchive. Verglichen werden die Anzahl beobachteter Prefixe, AS und AS-Verbindungen, wobei kein dedizierter Vergleich der Routingarchive insgesamt stattfindet. Allerdings zeigen sie etwa, dass 100 zufällig gewählte Beobachtungspunkte ausreichen, um 90% der AS-Topologie im Internet herzuleiten. Damit existiert bereits ein Hinweis auf eine deutliche Schnittmenge der beobachtbaren Erreichbarkeitsinformationen zwischen den RRCs. Aber auch darauf, dass einzelne RRCs nicht ausreichen, um einen möglichst vollständigen Blick zu erhalten.

Auch Gregori et al. [56] zeigen die Unvollständigkeit der Erreichbarkeitsinformationen in Routingarchiven, ebenfalls mit einem Fokus auf die Ableitung von AS-Topologieinformationen. Dafür werden ebenfalls Unterschiede zwischen RIPE RIS, Routeviews und PCH untersucht und die Beobachtungspunkte in drei Klassen unterteilt. Diese Klassen sind die Grundlage der Argumentation, dass über P2C-Verbindungen (vgl. Abschnitt 2.2.3) die meisten Erreichbarkeitsinformationen übertragen werden. Das ergibt sich aber im Grunde auch schon aus der Annahme der Weiterleitung selbst. Natürlich werden alle Erreichbarkeitsinformationen eines Upstream-Providers an die Kunden-AS weitergeleitet. Über

P2P-Verbindungen oder in Richtung eines Upstream-Providers werden hingegen nur die eigenen Prefixe und die Prefixe der Kunden weitergeleitet. Dass laut Gregori et al. insbesondere große Upstream-Provider als Route-Reflektor beitragen, führt zu einer großen Beobachtungslücke von P2P-Verbindungen. Daher entwickeln sie eine Methode zur optimierten Auswahl von AS als Beobachtungspunkt, um diese Unvollständigkeit zielgerichtet zu verringern. Dies gibt zwar Hinweise auf AS, die bevorzugt an Routingarchiven teilnehmen sollten, allerdings gibt es keine Möglichkeit diese Daten ohne die aktive Teilnahme der AS zu erhalten.

Es ist keine Arbeit bekannt, die auf Basis aller verfügbaren RRCs ermittelt, welche Auswahl an RRCs notwendig ist, um eine entsprechende Abdeckung der Erreichbarkeitsinformationen zu erhalten.

4.3 Routingarchive

Der für Europa zuständige regionale Internetregistrar RIPE bietet Routingarchive unter dem Dienst Routing-Information-Service (RIS) [118] an. Daneben gibt es weitere Anbieter, die auch regelmäßig in wissenschaftlichen Publikationen als Datenbasis verwendet werden: das Projekt Routeviews der Universität Oregon [122] und den kommerziellen Anbieter Packet Clearing House (PCH) [106]. Der Dienst „Isolario“ wurde im Rahmen eines Forschungsprojekts des nationalen italienischen Forschungsrats (ital. Consiglio Nazionale delle Ricerche, CNR) entwickelt [65]. Isolario verfolgt das Ziel, über zusätzliche manuelle Eingaben der Teilnehmer zusätzliche Informationen über das Internetrouting zu erhalten. Zusätzlich zu den Archivdaten mit festen Update-Intervallen bieten einige Anbieter auch sogenannte Live-Feeds an. Das RIPE betreibt seit Februar 2019 einen Live-Feed [117] als öffentlichen Prototypen zur Erweiterung des RIS [4]. Dieser Live-Feed sendet Updates aller RRCs des RIPE RIS im JSON-Format. Im Gegensatz zu Archivdaten mit festen Update-Intervallen ist mit solchen Live-Feeds eine Anomalieerkennung in Echtzeit möglich.

Obwohl Routingarchive also keinen vollständigen Blick auf das Internet ermöglichen, bieten sie grundlegende Informationen über das Internetrouting. Für eine Untersuchung von Prefixen und deren Origins im Rahmen einer Anomalieerkennung, lassen sich die Routingarchive verwenden, selbst wenn sich eine

AS-Topologie nicht umfänglich ableiten lässt. Tabelle 1 listet diese vier Routingarchive auf und gibt einen Überblick über die Eigenschaften, wie die Anzahl verbundener Autonomer Systeme, die geografische Positionierung der RRCs und entsprechende Update-Intervalle.

Tabelle 1: *Übersicht der Routingarchive*

Name	AS	RRCs	Standorte	Updates
RIPE RIS	123	23	Afrika: 1 Asien: 2 Australien: 0 Europa: 15 Nordamerika: 4 Südamerika: 1	RIB: Alle 8 Std. Updates: Alle 5 Min.
Routeviews	221	24	Afrika: 3 Asien: 2 Australien: 1 Europa: 3 Nordamerika: 12 Südamerika: 3	RIB: Alle 2 Std. Updates: Alle 15 Min.
PCH	/[a]	193	Afrika: 37 Asien: 27 Australien: 10 Europa: 49 Nordamerika: 49 Südamerika: 21	RIB: Alle 12 Std. Updates: Alle 1 Min.
Isolario	183	4	/[b]	RIB: Alle 2 Std. Updates: Alle 5 Min.

[a] PCH bietet keine Liste beteiligter AS an.
[b] Isolario macht keine Angaben über die Standorte der RRCs

4.4 Quellenauswahl

Auf den ersten Blick ist zu erkennen, dass selbst innerhalb eines RRCs mit mehreren AS, unabhängig von seinem Standort, Erreichbarkeitsinformationen redundant enthalten sind. Während die AS-Pfade sich dabei zumindest in den ersten Hops unterscheiden, sollten die Origin-Informationen, also welches AS als Ursprung eines Prefixes gilt, über alle RRCs und Archive konsistent sein. Um mehr als die von Chen et al. [30] erwähnten 90% der sichtbaren Informationen

zu erhalten, reicht es jedoch nicht aus, nur einzelne RRCs zu berücksichtigen. Um dies zu überprüfen und die Redundanz der enthaltenen Daten zu quantifizieren, wurden die Daten entsprechend untersucht. Das Ziel ist dabei nicht bloß die Gegenüberstellung der Routingarchive sondern die Auswahl von RRCs zu ermitteln, die notwendig ist, um eine möglichst umfassende Abdeckung zu erhalten. Die Ergebnisse der Untersuchung sind in den folgenden Abschnitten dargestellt.

4.4.1 Methodik

Im Rahmen der Untersuchung wurden RIB-Daten der vier genannten Routingarchive zu möglichst gleichen Zeitpunkten miteinander verglichen und ermittelt, welche RRCs berücksichtigt werden sollten. Da es sich um die Routingtabellen der Route-Reflektoren handelt, sind dort alle Updates vor dem Zeitpunkt ebenfalls berücksichtigt. Um temporäre und zyklische Effekte der enthaltenen Informationen auszuschließen werden alle Untersuchungen für drei unterschiedliche Tage innerhalb eines Kalendermonats durchgeführt: für den 1. März 2019, den 15. März 2019 und den 31. März 2019 mit den RIBs von 0:00 Uhr. Da PCH für die RRCs nur einmal täglich eine Routingtabelle der RRCs zur Verfügung stellt, und diese meist gegen 3:00 Uhr in der Nacht verfügbar ist, wurde als Uhrzeit für die anderen Routingarchive 0:00 Uhr festgelegt. Laut MRT-Datenformat sollen die Zeiten in den Archivdateien in der *Coordinated Universal Time* (UTC) abgespeichert werden [18].

Alle RRCs werden eingelesen, um eine Grundgesamtheit der enthaltenen Erreichbarkeitsinformationen zu erhalten. Auf Basis dieser Grundgesamtheit werden dann die einzelnen RRCs bewertet und ermittelt, wie viele RRCs notwendig sind, um eine gewisse Abdeckung zu erreichen. Dabei wird neben dem RRC mit dem größten Anteil auch die notwendige Anzahl an RRCs für die folgenden Mindestmengen betrachtet: $\geq 75\%$, $\geq 99\%$, $\geq 99,5\%$, $\geq 99,9\%$ und $\geq 99,99\%$.

Die optimale Auswahl der RRCs ist ein Mengenüberdeckungsproblem (engl. set covering) und damit eines der klassischen NP-vollständigen Probleme [71]. Das Problem lässt sich im Hinblick auf die Anzahl der RRCs oder auf eine möglichst kleine Schnittmenge (engl. exact cover) der RRCs betrachten. Die Redundanz der RRCs ist per se recht hoch, so dass nur eine Optimierung der

Anzahl an RRCs betrachtet wird. Eine Berechnung der optimalen Auswahl erscheint angesichts der betrachteten Mengen von mehr als 64.000 AS, mehr als 400.000 AS-Verbindungen und mehr als 1.200.000 Prefixen als nicht sinnvoll. Der Greedy-Algorithmus von Johnson [70] berechnet in polynomieller Zeit ($O(n \ln n)$) eine Auswahl, die maximal $\ln n + 1$ mal größer ist, als die optimale Auswahl. Feige [44] zeigt eine untere Schranke effizienter Approximierungs-Algorithmen für Mengenüberdeckungsprobleme von $(1 - O(1))\ln n$, was im Grunde dem Greedy-Algorithmus entspricht. Für die an dieser Stelle verfolgten Zwecke reicht eine Annäherung mit dem Greedy Algorithmus aus. [44, 70]

Die Implementierung des Auswahl-Algorithmus orientiert sich an dem Greedy-Algorithmus von Johnson [70]. Seien $R = \{r_1, \ldots, r_x\}$ die Menge aller RRCs und a das betrachtete Attribut (Origin, Prefix oder Peering) mit $G = A_a(R)$ als die Grundgesamtheit aller Werte für a aus R.

1 `Attribute = {"Origin", "Prefix", "Peering"}`
2 `Min = {0,75;0,99;0,995;0,999;0,9999}`
3 `FÜR` $v = (a, m)$ `IN Attribute×Min:`
4 $Auswahl_v = \{\}$
5 $Auswahl_v = Auswahl_v \cup \{r\}$ `FÜR` $r \in R$ `mit`
$|A_a(Auswahl_v \cup \{r\})| = \max_{r' \in R} |A_a(Auswahl_v \cup \{r'\}|.$
6 `WENN` $|A_a(Auswahl_v)| < (m \cdot |A_a(R)|)$ `GEHE ZU 5`

Für jedes Attribut und jede Mindestmenge wird im ersten Schritt der beste RRC ermittelt, das ist der RRC mit der größten Schnittmenge mit der Grundgesamtheit. Anschließend werden bis zum Erreichen der Mindestmenge sukzessive die RRCs zur Auswahl hinzugefügt, die die Schnittmenge mit der Grundgesamtheit am meisten erhöhen.

Die Schnittmengenberechnung wurde mit Daten der drei definierten Zeitstempel und mit der jeweils ersten über alle RRCs vollständig nutzbaren Routingtabelle durchgeführt. Tabelle 2 zeigt die zum jeweiligen Zeitpunkt geltenden Bedingungen dieser Untersuchung.

Tabelle 2: *In Routingarchiven enthaltene Informationen*

Datum	RRCs	Prefixe	Origins	Peerings
1. März 2019	196	1.237.318	64.825	405.423
15. März 2019	197	1.269.638	65.194	429.453
31. März 2019	197	1.261.573	100.351	568.211

4.4.2 Origin

Diese Untersuchung ermittelt die Schnittmengen und Abweichungen der Ursprungs-AS aller verfügbaren Prefixe über unterschiedliche RRCs der verschiedenen Anbieter. Es soll insbesondere untersucht werden, ob bzw. wie unterschiedliche Standorte eine unterschiedliche Sichtbarkeit auf Prefix-Origins haben. Für die Erkennung von Prefix-Hijacking ist es wichtig, eine uneingeschränkte Sicht auf alle Origin-AS für ein bestimmtes Prefix zu erhalten. Das ist nur dann möglich, wenn die Daten der verwendeten RRCs sich hinsichtlich der Prefix-Origins ergänzen.

Um die Schnittmengen der Origin-AS zu bestimmen, werden die Daten aller verfügbaren RRCs der Routingarchive verwendet. Um dabei zufällig auftretende Sichtbarkeit weitgehend auszuschließen werden die Schnittmengen von drei unterschiedlichen Zeitpunkten innerhalb eines Monats berechnet. Die verfügbaren RRCs werden dann anhand der übereinstimmenden Prefix-Origins gruppiert. Somit können RRCs anhand der Abweichungen aufgrund ihres Standorts unabhängig vom Zeitpunkt für die gewünschte Datenbasis berücksichtigt werden. Die Ergebnisse der Origin-Analyse sind in Tabelle 3 dargestellt.

Tabelle 3: *Enthaltene AS in den betrachteten RRCs*

	01.03.2019	15.03.2019	31.03.2019
Anteil bester RRC	99,546%	99,546%	99,999%
Anzahl RRCs für			
$\geq 99\%$	1	1	1
$\geq 99,5\%$	1	1	1
$\geq 99,9\%$	11	10	1
$\geq 99,99\%$	41	38	1
$= 100\%$	47	44	2

Für die Origin-AS zeigen die Ergebnisse eine deutliche Abweichung am 31. März 2019. Die ungewöhnlich hohe Anzahl kann auf den RRC mit dem Namen „Naboo“ von Isolario zurückgeführt werden. Dieser RRC listet zu diesem Zeitpunkt 90.975 zusätzliche Routen, die den anderen RRCs gänzlich unbekannt sind, zwischen dem AS 34549 der deutschen Firma meerfarbig.net und weiteren AS. Diese AS sind zum Teil solche mit reservierten AS-Nummern, die eigentlich nicht im Internetrouting verwendet werden. Werden diese Routen von der Betrachtung ausgenommen, ergibt sich für die Origin-AS ein insgesamt stabiles Bild. Abgesehen von dieser Anomalie bedeutet dies auch, dass über die Standorte hinweg ein konsistentes Bild der Prefix-Origins besteht und für die Wahl der verwendeten RRCs keine zu berücksichtigenden Einschränkungen bestehen.

Tatsächlich sind mit nur einem RRC (route-views4) von Routeviews bereits mehr als 99% aller AS sichtbar. Um alle sichtbaren AS zu erhalten, genügen weniger als 50 der verfügbaren RRCs.

4.4.3 Prefix

Die Anzahl der Prefixe nimmt ausgehend vom 1. März zunächst zu, dann wieder leicht ab, es ist jedoch eine steigende Tendenz wahrzunehmen. Da keine freien IPv4-Prefixe mehr existieren, kann die Anzahl der Prefixe nur durch das Aufteilen eines Prefixes in entsprechende Subnetze möglich sein. Die Ergebnisse der Untersuchung sind in Tabelle 4 dargestellt. Der RRC mit den meisten

Tabelle 4: *Enthaltene Prefixe in den betrachteten RRCs*

	01.03.2019	15.03.2019	31.03.2019
Anteil bester RRC	80,5012%	79,7281%	80,1608%
Anzahl RRCs für			
≥ 75%	1	1	1
≥ 95%	3	5	4
≥ 99%	16	15	15
≥ 99,5%	25	23	23
≥ 99,9%	51	49	48
≥ 99,99%	97	96	93
= 100%	141	139	136

Prefixen beinhaltet nur etwa 80% der Gesamtmenge an Prefixen. Grundsätzlich

sollten aber alle Präfixe auch an allen RRCs sichtbar sein, um die Erreichbarkeit zu gewährleisten. Diese Diskrepanz ist nur durch Aggregation von Prefixen zu erklären, also dem Zusammenfassen zweier benachbarter Prefixe zu einem. Solche Aggregationsmethoden werden unter anderem verwendet, um die Routingtabelle möglichst klein zu halten. Während bereits etwa 15 RRCs ausreichen, um 90% der annoncierten Prefixe zu betrachten, müssen für die Gesamtmenge der Prefixe bis zu 141 unterschiedliche RRCs berücksichtigt werden. Eine umfassende Analyse der Prefixe setzt also eine deutlich größere Datenbasis voraus, als für die Betrachtung der Origin-AS.

4.4.4 Peering

Maßgeblich für den Aufbau eines Überblicks über Beziehungen zwischen Autonomen Systemen sind die bekannten Verbindungen zwischen diesen. Aus den Routingdaten der RRCs sind auf Basis der AS-Pfade in den Announcements Rückschlüsse über physikalische Verbindungen der AS untereinander möglich. Es kann davon ausgegangen werden, dass im AS-Pfad aufeinander folgende AS eine BGP-Verbindung miteinander unterhalten. Empfangende BGP-Router fügen ihre eigene AS-Nummer dem AS-Pfad hinzu, bevor sie das Announcement selbst an verbundene Nachbarn weiterleiten.

Es wird also davon ausgegangen, dass im AS-Pfad benachbarte AS eine physikalische Verbindung und damit auch eine Geschäftsbeziehung unterhalten. Allein aus der Tatsache der physikalischen Verbindung lässt sich keine Information über die Art der Beziehung aussagen. Es handelt sich dabei aber im Kontext von Internetrouting mindestens um eine Nachbarschaftsbeziehung.

Diese Nachbarschaftsbeziehungen sind Grundlage existierender Arbeiten, etwa der Ableitung von Geschäftsbeziehungen aufgrund der Anzahl und der Nutzung dieser Nachbarschaftsbeziehungen [81]. Daher ist es wichtig, bei der Erstellung einer verwendbaren Datenbasis möglichst alle Hinweise auf Nachbarschaftsbeziehung mit einzubeziehen. Die Auswahl der dafür zu nutzenden RRCs soll auf Basis der im Folgenden beschriebenen Untersuchung getroffen werden.

Die Daten aller verfügbaren RRCs werden für die Betrachtung der Nachbarschaftsbeziehungen eingelesen. Für jede Nachbarschaftsbeziehung werden da-

bei die RRCs gesammelt, die Announcements erhalten haben, die eine Nachbarschaftsbeziehung implizieren. Die Auswahl zu berücksichtigender RRCs wird dann auf Basis dieser Daten getroffen, bis alle Nachbarschaftsbeziehungen berücksichtigt wurden. Die Ergebnisse der Untersuchung sind in Tabelle 5 dargestellt.

Tabelle 5: *Enthaltene Peerings in den betrachteten RRCs*

	01.03.2019	15.03.2019	31.03.2019
Anteil bester RRC	52,8749%	52,3345%	53,2786%
Anzahl RRCs für			
≥ 75%	6	6	4
≥ 95%	18	18	16
≥ 99%	31	31	29
≥ 99,5%	35	36	33
≥ 99,9%	54	54	49
≥ 99,99%	95	93	89
= 100%	121	123	124

Aus den Ergebnissen der Untersuchung ist ersichtlich, dass sich hinsichtlich der Nachbarschaftsbeziehungen ein differenziertes Bild ergibt, je nachdem, welche RRCs verwendet werden und welche nicht. Es müssen also ähnlich wie bei den Prefixen deutlich mehr RRCs als Quelle für eine gute Datenbasis verwendet werden.

4.5 Realitätsabgleich

Eine große Problematik bei Analysen des Internetroutings ist die fehlende Möglichkeit zum Realitätsabgleich. Die Datenbasis auf der ein Großteil der Routingforschung basiert sind Announcements, die in teilnehmenden Autonomen Systemen gesammelt werden. Aus diesen Ankündigungen werden die enthaltenen Pfade extrahiert und davon Verbindungen zwischen AS abgeleitet. Stehen zwei AS in einem Pfad nebeneinander wird eine physikalische Verbindung zwischen diesen angenommen. Während dieses Vorgehen nachvollziehbar ist und vermutlich auch einem Abgleich mit der Realität standhalten wird. Es ist aber davon auszugehen, dass viele physikalische Verbindungen nur eine sehr geringe

Reichweite haben oder für tatsächliche Routingentscheidungen nicht relevant sind und daher die Beobachtungsstellen nicht erreichen.

Es wäre daher zwar möglich, eine sogenannte „Ground Truth“ für Verbindungen zwischen Autonomen Systemen zu erhalten, wenn jeder AS-Betreiber entsprechende Informationen herausgäbe. In der Realität ließe sich ein solches Unterfangen nicht sinnvoll umsetzen und hätte auch Probleme durch Inkonsistenzen aufgrund unterschiedlicher Reaktionszeiten der AS-Betreiber. Daher nutzen Forscher als Annäherung an die Realität genau die Daten, die sich durch die Sammlung der Routingarchive ohne Schwierigkeiten ermitteln lassen. Während diese Daten für grundlegende Forschungen im Routingbereich zunächst keine Einschränkungen darstellen - die Ergebnisse lassen sich in den meisten Fällen entsprechend übertragen - können sie für die Untersuchung von Vorfällen und resultierende Einschränkungen nicht ohne entsprechende Fehlerwahrscheinlichkeit verwendet werden.

Im Rahmen der Untersuchung verwandter Arbeiten erfolgt auch ein Abgleich der für die jeweiligen Analysen genutzten Daten zum Realitätsabgleich. Daraus ergibt sich ein eindeutiges Bild, dass sich die akademische Betrachtung von Routinganomalien fast ausschließlich auf historischen Routingdaten der genannten Routingarchive stützt. Einige Arbeiten nutzen zusätzlich Daten aus Traceroutes oder Looking-Glass-Servern.

4.6 Fazit

Die Berechnungen der in RRC-Daten enthaltenen Informationen zeigen, dass je nach Fragestellung die Nutzung eines kleinen Teils der RRCs ausreichen kann, um eine ausreichende Informationsdichte zu erzielen. Allerdings müssen insbesondere bei der Betrachtung der Prefixe als auch bei der Betrachtung der Nachbarschaftsbeziehungen fast alle RRCs berücksichtigt werden. Es scheint akademischer Konsens zu sein, die Analyse von Internetrouting allein auf Basis der historischen Daten existierender Routingarchive zu stützen. Leider werden häufig nicht alle verfügbaren Quellen dafür berücksichtigt. Ein Realitätsabgleich darüber hinaus ist aufgrund fehlender Daten nicht vollständig möglich. Auch eine Untersuchung der Fehlerwahrscheinlichkeit ist auf Basis der vorliegenden Daten nicht möglich.

In diesem Kapitel wurde gezeigt, dass je nach Anforderung an die Vollständigkeit der Daten eine unterschiedlich große Anzahl an RRCs analysiert werden muss, um eine entsprechende Sichtbarkeit zu erreichen. Während bereits ein RRC ausreicht, um 99% der im Internet aktiven AS aufzulisten, müssen für eine vollständige Abdeckung mit bis zu 44 RRCs deutlich mehr Daten analysiert werden. Während für mehr als 75% der sichtbaren Prefixe bereits ein RRC ausreicht, zeigt sich der Effekt der unterschiedlichen Sichtweisen im Internet sehr deutlich, wenn 100% der sichtbaren Prefixe berücksichtigt werden sollen. Dafür sind dann nämlich zum Teil mehr als 140 RRCs mit ihren unterschiedlichen Sichten notwendig. Dieser Effekt zeigt sich auch bei den Verbindungen zwischen AS, allerdings werden dort für mehr als 75% bereits sechs RRCs benötigt. Für eine umfassende Sicht sind insgesamt jedoch noch etwa 125 RRCs notwendig.

Die Ergebnisse lassen sich für die optimierte Auswahl der in Routingarchiven enthaltenen Daten sowohl in der Forschung als auch beim alltäglichen Monitoring des Internetroutings verwenden.

5 Monitoring: Nutzung weiterer Datenquellen[5]

Zusammenfassung des Kapitels Bezogen auf die Zusammenschaltung von rund 45.000 AS zum Zeitpunkt der Untersuchung, ist das Internet und insbesondere sein Routingsystem sehr fragil. Ein besonderes Problem im Hinblick auf die Schutzziele der IT-Sicherheit ist das implizite gegenseitige Vertrauen der AS untereinander. Obwohl dies als Schwachstelle bereits seit mehr als einem Jahrzehnt sowohl in der Wissenschaft als auch unter AS-Betreibern diskutiert wird, gibt es bisher kein etabliertes Konzept zur Absicherung. Monitoring des globalen Internetroutings und die Analyse zur Erkennung von Routinganomalien ist daher zwingend notwendig. Für die Analyse von Routinganomalien ist es wichtig, eine stets aktuelle Sicht auf das Peering im Internet zu erhalten. Dieses Kapitel zeigt Möglichkeiten auf, die Datenbasis für dieses Monitoring zu erweitern und im Bezug auf Peeringbeziehungen auf einem aktuellen und möglichst validen Stand zu halten. Die eingesetzten Verfahren zur Erkennung von Routinganomalien liefern eine große Anzahl an Auffälligkeiten. Zur Erkennung von Anomalien werden diese Auffälligkeiten im Hinblick auf Stabilität und Validität weiter untersucht. Je mehr Daten dafür zur Verfügung stehen, umso zuverlässiger ist die Klassifikation und Validierung der Anomalien.

[5] Die Inhalte basieren auf M. Wübbeling, T. Elsner und M. Meier. „Inter-AS routing anomalies: Improved detection and classification". In: *2014 6th International Conference On Cyber Conflict (CyCon 2014)*. 2014, S. 223–238
Till Elsner hat an der Konzeption der Looking-Glass-Auswertung mitgearbeitet und zur Implementierung der Abfrage von Looking-Glass-Servern beigetragen.

Kapitel 4 diskutiert die Limitierungen öffentlich verfügbarer Daten. Die Daten erlauben zwar keine vollständige Erkenntnis über alle AS-Verbindungen, ermöglichen aber grundlegendes Monitoring des Internetroutings zur Anomalieerkennung. Die in diesem Kapitel zusätzlich gesammelten öffentlich verfügbaren Daten dienen als Grundlage für die Berechnung der Prefix-Hijacking-Resilienz in Kapitel 6 dieser Arbeit.

Es existieren unterschiedliche Ansätze zur Erkennung und Klassifikation von Routinganomalien auf Basis der Daten aus dem Routingsystem selbst, also aus Routingarchiven. Aufgrund der in den Routingarchiven vorliegenden Daten, klassifiziert keiner dieser Ansätze alle erkannten Situationen zuverlässig. Eine möglichst genaue Klassifikation der Situationen ist aber notwendig für die Einschätzung, ob ein Konflikt legitim oder illegitim ist. Nur so lässt sich eine möglichst aussagekräftige Kritikalität für jeden einzelnen Konflikt ableiten. Wichtig ist dabei die Einschätzung der Validität bisher unbekannter Peeringbeziehungen.

Die geringe Menge an Informationen über Peeringbeziehungen außerhalb des Routingsystems selbst ist dabei deshalb ein Problem, weil kein eindeutig definierter Zustand ohne Konflikte bekannt ist. Es ist also im Grunde kein direkter Vergleich der Datenlange in den Routingarchiven mit den realen Bedingungen möglich. Um Fakten über tatsächliche Routingbeziehungen und legitime Prefixbesitzer erhalten zu können, sollen weitere Quellen für die Begutachtung herangezogen werden. Mit diesen weiteren Quellen lassen sich dann zumindest teilweise weitere Belege für Entsprechungen in der Realität finden, so dass die Daten der Control-Plane überprüft werden können. Somit lässt sich ein besserer Realitätsdatenabgleich ermöglichen, auf dessen Basis dann eine Klassifikation der Routinganomalien durchgeführt werden kann.

In diesem Kapitel geht es um die Verwendung zusätzlicher, ebenfalls öffentlich verfügbarer Informationen über das Internetrouting zur Anreicherung der Datenbasis und zur Verifikation bekannter Peeringbeziehungen. Es wird gezeigt, dass über Looking-Glass-Dienste, die von einzelnen AS betrieben werden, sowie über Peeringdatenbanken und öffentlich verfügbare Informationen von IXPs weitere Daten gesammelt werden können.

Die maßgeblichen Beiträge sind (1) die Sammlung von weiteren Daten zum Beleg von Routingbeziehungen zwischen AS und dadurch höhere Genauigkeit bei der Suche und Klassifikation von illegitimen Routinganomalien, (2) einen Ansatz auf Basis o.g. Systeme und Daten, um zusätzliche Hinweise und Belege zu finden mit denen Routinganomalien besser erkannt und klassifiziert werden können, (3) eine Auswahl verwendbarer Quellen für diese Anreicherung und (4) ein System zur automatischen Sammlung und Normalisierung dieser Informationen von unterschiedlichen Standpunkten innerhalb der Ebene des Internetroutings, von Betreibern von Internetknotenpunkten und von AS-spezifischen Diensten wie Looking-Glass, das die Abfrage von Informationen direkt von innerhalb eines AS laufenden Routern erlaubt.

5.1 Verwandte Arbeiten

Die Unvollständigkeit der in Routingarchiven existierenden Informationen wurde bereits in Abschnitt 4.2 diskutiert. In der Literatur finden sich viele Ansätze, um die Daten der Control-Plane mit weiteren Daten anzureichern. Dabei steht hauptsächlich die Erstellung einer AS-Topologie im Fokus der Arbeiten. Einige Arbeiten versuchen die WHOIS-Datenbanken der RIRs in die Erstellung einzubeziehen [27, 59, 88, 131]. Die Daten der RIRs werden jedoch nur beim Anlegen eines AS einmalig abgefragt, die permanente Pflege der Daten obliegt den Betreibern des AS selbst. So gibt es etwa in der WHOIS-Datenbank des RIPE gut gepflegte Datensätze ebenso wie solche Einträge, aus denen keine weiteren Informationen zu gewinnen sind. Auch wurde bereits gezeigt, dass Betreiber gezielt falsche Informationen in den Datenbanken gespeichert haben [131].

Auch Traceroute wurde häufig als Mittel zur Anreicherung von Daten oder der Analyse von Verbindungen im Internet verwendet [8, 26, 42, 55, 86, 88, 128, 134]. Allen Ansätzen gemein ist das Problem der Zuverlässigkeit von Traceroutes [5, 6] und die Tatsache, dass Hops etwa in IXPs zu nachweislich falschen Ergebnissen führen [28, 63, 91].

Looking-Glass-Server wurden immer wieder genutzt, um die aus verschiedenen Quellen abgeleiteten Informationen mit Informationen der Data-Plane zu überprüfen [5, 27, 88, 101]. Zwar werden Internetknotenpunkte, insbesondere als Fehlerquelle in Traceroutes (s.o.), aber auch zur Ermittlung der AS-

Topologie [51, 85] in einigen Arbeiten erwähnt, eine Nutzung der Mitgliederdaten von Internetknotenpunkten zur Analyse neuer Peerings unter Berücksichtigung von Peeringpolicies ist nicht bekannt.

5.2 Looking-Glass

Um zuverlässige Informationen über aktuelle Peeringbeziehungen von Autonomen Systemen zu erhalten, sind vor allem BGP-spezifische Informationen wie Routingtabellen und nächste Hops für unterschiedliche Routen interessant. Um sicherzugehen, dass die aus Routingarchiven erhaltenen Informationen korrekt sind, sollen weitere Informationen direkt von Routern innerhalb von AS genutzt werden. Dafür bieten sich Looking-Glass-Dienste an, wobei der Begriff Looking-Glass nicht fest definiert und nicht auf Router beschränkt ist. Ein *Looking-Glass* (LG) ist im Routingkontext eine Webanwendung, die von Administratoren eines Autonomen Systems betrieben wird, um Einblick in die Konfiguration und den Status von Routern innerhalb ihres AS zu ermöglichen. Dabei läuft das LG üblicherweise auf einem Webserver und ist für den Zugang zu einem oder mehreren Routern innerhalb des AS konfiguriert. Je nach LG lassen sich unterschiedliche, durch den Administrator freigegebene Kommandos direkt an die Konsole eines Routers senden. Die Ausgabe der Konsole wird anschließend, zumeist unverändert, über die Webanwendung zurückgegeben. LGs erlauben also Einblicke in Teile der Routerkonfiguration, ohne einen direkten Zugang zum Routing. Damit ist ein Blick in den generellen Routingstatus eines AS möglich, was hier vor allem im Hinblick auf BGP relevant ist. Es gibt verschiedene LG-Implementierungen. Die meisten davon sind als Open-Source-Software kostenlos, einfach zu verwenden und anzupassen. Die Implementierungen unterscheiden sich in der Anzahl unterstützter Routerhersteller und in der Anzahl unterstützter Systeme. Tabelle 6 listet die Unterschiede der 6 meistgenutzten und frei verfügbaren Implementierungen auf.

	KLG	MRLG	Telephone-LG	IBGP-LG	Cougar-LG	Vyatta-LG
Implementierung	PHP	Perl	PHP	Java	Perl	Perl, Javascript
Router	-	Cisco, Quagga, Zebra, Marconi/Fore Systems (erweiterbar)	Router unabhängig	-	Cisco, Zebra, Juniper	Vyatta
Verbindung zum Router	Telnet	Telnet	Telnet	Telnet	SSH, Telnet	SSH
Kommandos	Traceroute, Ping, BGP-Lookup, Whois-Lookup, IPv4/v6	Traceroute, Ping, BGP-Lookup, IPv4/v6	Traceroute, Ping	BGP-Lookup	Traceroute, Ping, BGP-Lookup	Traceroute, Ping, BGP-Lookup
Besonderheiten	MySQL-Server für Name-Lookups, Ausgabe beliebig konfigurierbar	-	-	Visualisierung des Routingstatus und vergangener Ereignisse	-	-

Tabelle 6: *Looking-Glass Implementierungen*

5.3 Automatisierter Zugriff auf Looking-Glass

Automatisierte Anfragen an beliebige LGs sind eine Herausforderung. Während Router einen direkten Zugriff auf ihre Konfiguration über die Konsole bieten, meist über telnet oder ssh, haben LGs sehr unterschiedliche Interfaces, um Kommandos an die verfügbaren Router zu senden. Für menschliche Benutzer ist eine Verwendung zumeist intuitiv über die Weboberfläche möglich. Durch die hohe Flexibilität in der Anpassung von Optik und Funktion der meisten Implementierungen muss eine automatisierte Abfrage zumindest an die maßgeblichen Elemente der unterschiedlichen Implementierungen angepasst werden. Dies führt unter anderem dazu, dass auch die HTML-Eingabefelder zum Teil unterschiedlich benannt sind, was eine Automatisierung deutlich erschwert. Insbesondere die Ergebnis-Darstellung von LGs eignet sich nicht gut für eine automatisierte Auswertung. Die meisten LGs zeigen einfach die Konsolenausgabe der Router ohne weitere Überarbeitung an. Die relevanten Informationen können also nicht unmittelbar genutzt sondern müssen zunächst in der Ausgabe gefunden werden.

Der vom CAIDA betriebene Dienst „Periscope“ ermöglicht die einheitliche Abfrage unterschiedlicher LGs und unterstützt dabei auch verschiedene Implementierungen. Zum Zeitpunkt der letzten Untersuchung (Stand Juni 2016) unterstützt Periscope 297 AS. Aktuell (Stand März 2019) steht Periscope nicht mehr zur Verfügung. Der von der niederländischen „netherlands network operator group“ (NLNOG) betriebene RING-Dienst erlaubt über eine REST-API den Zugriff auf die Routingdaten von 430 Teilnehmer-AS [99] (Stand April 2019). Andere Webseiten pflegen LG-Datenbanken mit zum Teil mehr als 1.000 LG URLs [14, 15, 16] (Stand April 2019). Auch wenn das insgesamt nur ein kleiner Teil des Internets ist, können die Daten grundsätzlich wertvolle Informationen liefern. Um möglichst alle verfügbaren LGs nutzen zu können, wird auf Basis der Periscope-Forschung ein eigenes Werkzeug entwickelt, dass möglichst generisch die existierenden LG-Implementierungen unterstützt, das sich aber auch einfach anpassen lässt, falls die so erzeugte Abfrage nicht möglich ist. Dafür wird ein vorlagenbasierter Ansatz auf Basis regulärer Ausdrücke gewählt. Die Vorlagen enthalten reguläre Ausdrücke zur Erkennung der eingesetzten LG-Implementierung sowie der möglichen Abfragen und Antworten des Servers. Das erlaubt bei Bedarf eine einfache Anpassung des Systems an weitere LGs.

5.3.1 Auffinden von Looking-Glass

Bevor LGs automatisiert angefragt werden können, müssen die URLs für diese Anfragen bekannt sein. Für die Untersuchung sollen die existierenden Listen angefragt werden und die URLs der LGs herausgearbeitet werden. Da die Listen kein einheitliches Format haben, sollen Muster in den Inhalten der HTML-Seiten gefunden werden. So werden alle URLs gefunden, die als Text oder Links angezeigt werden. Aktuell erhält man aus den drei LG-Datenbanken [14, 15, 16], insgesamt 953 unterschiedliche URLs von LGs (Stand 14. März 2019).

Obwohl die Struktur der unterschiedlichen Implementierungen bekannt ist, können Betreiber beliebig wählbare Pfade des Webservers für das LG konfigurieren. Eine Analyse der bekannten Listen zeigt, dass bestimmte Muster in den URLs regelmäßig verwendet werden. Es finden sich 528 Einträge, die eigene Subdomains (etwa „lg.example.com“) für LGs verwenden. Lediglich 129 davon haben zusätzlich Pfade unterhalb des Wurzelpfads für den Zugriff auf das LG.

Es lassen sich typische verwendete Pfade in den URLs erkennen. Für die bekannten 953 Einträge gibt es 140 einzigartige Pfade zu den LGs. Die übrigen Pfade kommen mehrfach vor. Die häufigsten Pfade, die 10-mal oder häufiger vorkommen sind: / (497), /lg (136), /lg/lg.cgi (30), /cgi-bin/lg.cgi (26), /cgi-bin/bgplg (18).

Um weitere LGs zu finden, die nicht in den LG-Datenbanken enthalten sind, können diese Pfade etwa in Suchmaschinen genutzt werden. Die Google-Suchmaschine erlaubt die Angabe von URLs auch mit Wildcard-Symbolen. So lässt sich für alle Pfade eine Suche ausführen, die mit dem Suchstring „site:*/<PFAD>“ für alle Pfade weitere LGs liefern kann. Ausgehend von den 953 bekannten URLs sollen im Rahmen dieser Arbeit keine weiteren LGs über entsprechende Suchen hinzugefügt werden.

5.3.2 Nutzung von Looking-Glass

Um die bekannten LGs abzufragen wurde ein Werkzeug entwickelt, dass auf Basis von Konfigurationsdateien für unterschiedliche LG-Implementierungen verwendet werden kann. Diese müssen manuell erstellt werden und können

von dem Werkzeug zur Erkennung von LG-Implementierungen verwendet werden. Darüber hinaus enthält eine Konfiguration entsprechende Vorlagen, die zur Erstellung von Anfragen an ein LG genutzt werden. Damit die Ausgaben des LG verwendet werden können, gibt es weiterhin reguläre Ausdrücke, die das Parsen der Ergebnisse ermöglichen.

```
1  post
2  <<<
3  bgp
4  query=bgp&protocol=IPv4&addr=
5  >>>ip
6  \&router=
7  >>>get
8  .*?router=(*?).*
9  <<<
10 traceroute
11 ...
```

Listing 5.1: *Konfigurationsdatei einer LG-Implementierung*

Listing 5.1 zeigt eine entsprechende Konfigurationsdatei an. Die einzelnen Bestandteile sind dabei wie folgt:

```
1  post
```

Dokumentiert das HTTP-Verb, mit dem die Abfrage an das LG gesendet wird.

```
2  <<<
3  bgp
```

Leitet eine Anfrage ein, dabei ist der Wert in Zeile 3 der Name des Kommandos, das beim Aufruf des Werkzeugs ausgewählt wird. Das Programm erlaubt für jede Konfiguration unterschiedliche Anfragetypen, entsprechend der in einer LG-Instanz erlaubten Kommandos.

```
4  query=bgp&protocol=IPv4&addr=
5  >>>ip
6  \&router=
7  >>>get
8  .*?router=(*?).*
```

Ab Zeile 4 bis Zeile 8 wird die Anfrage zusammengebaut. Das Steuerzeichen „»>ip“ in Zeile 5 beschreibt die Übernahme der IP-Adresse, die dem Werkzeug

bei einem Aufruf mitgegeben wird, als Wert für den Parameter „addr=“. In Zeile 7 wird mit dem Steuerzeichen „»>get“ ein Wert aus der Webseite des LG ausgelesen. Das ist etwa für die Angabe von Routern notwendig, die durch das LG abgefragt werden können. Bei den meisten LGs werden Router über eine Auswahlliste in der Weboberfläche ausgewählt. Der erste mit dem Ausdruck in Zeile 8 gefundene Wert wird als Wert für den Parameter „router=“ hinzugefügt. Damit ist der Querystring der Abfrage vollständig.

```
9  <<<
10 traceroute
11 ...
```

Als nächstes folgt dann ab Zeile 9 die Definition zum Aufruf des Traceroute-Kommandos mit den gleichen Regeln zur Abfrage-Erstellung.

Theoretisch sollten mit diesem Werkzeug nahezu beliebige LGs abgefragt werden. Leider liefern trotz manueller Anpassung der Konfiguration bereits nach kurzer Zeit viele LGs keine Resultate mehr. Aufgrund der fehlenden Standardisierung und häufig wechselnden Konfigurationen ist eine Verwendung von LGs für die kontinuierliche Analyse von Routinganomalien nur mit viel manuellem Aufwand möglich.

5.4 Internetknotenpunkte

Bei internetknotenpunkten handelt es sich zumeist um spezialisierte Rechenzentren, in denen Router der Teilnehmer betrieben werden und vom Betreiber eine entsprechende Infrastruktur vorgehalten wird, die den Aufbau von Peeringbeziehungen erleichtert. So können Teilnehmer mit einem verbundenen Router mit allen anderen Teilnehmern Verbindungen aufbauen und Peering etablieren. [100]

In den folgenden Abschnitten werden zunächst die Organisation und der Aufbau von IXPs und anschließend mögliche Peering Policies der Teilnehmer beschrieben.

5.4.1 Organisation

Internetknotenpunkte bilden heute den tatsächlichen Kern des Internets im Hinblick auf die Netz-Infrastruktur. Die klassische AS-Topologie ist zwar noch erkennbar, IXPs verursachen jedoch eine Abflachung dieser Topologie [2]. Einige IXPs sind aus Verbänden oder Vereinen der Betreiber Autonomer Systeme hervorgegangen, die zunächst untereinander Peering etablieren wollen. Der nach eigenen Angaben im Bezug auf Datenverkehr größte IXP De-CIX ist eine hundertprozentige Tochter des eco Verband der Internetwirtschaft e.V. mit Sitz in Frankfurt (Main) [35]. Häufig sind IXPs also zunächst auf geografische Nähe von AS bezogen, so dass eine physikalische Netzanbindung zum IXP möglich ist. Ein IXP unterscheidet sich von einem klassischen Rechenzentrum dadurch, dass er seinen Kunden selbst keinen Internetzugang (Upstream) anbietet. Gäbe es an einem IXP keinen Upstream- bzw. Transit-Provider mit dem die Teilnehmer peeren können, so wäre an diesem IXP einzig die Kommunikation der Teilnehmer untereinander möglich. [2, 29, 115]

Ist ein AS Teilnehmer eines IXPs, so nennt man dies (wie bei Rechenzentren auch) einen Point-of-Presence (PoP). Insbesondere Inhalteanbieter in Form von Content-Delivery-Netzwerken (CDN) unterhalten PoPs in möglichst vielen IXPs, um dort über viele Verbindungen zu anderen AS die Kosten für Datenverkehr möglichst gering zu halten. Auch Upstream-Provider erreichen einen Großteil ihrer Kunden über unterschiedliche PoPs. [2, 29]

Um die Infrastruktur möglichst einfach zu halten und das Peering zusätzlich überwachen und regeln zu können, setzen größere IXPs sogenannte Route-Server ein. Diese sind eine Art Multiplexer für BGP-Verbindungen. Ein Route-Server erlaubt so durch die Konfiguration von nur einem Peering, nämlich mit dem Route-Server selbst, den Routenaustausch aller Teilnehmer untereinander. [115]

5.4.2 Peeringpolicies

Jedes AS folgt beim Peering und bei der Auswahl von Peers eigenen, meist betriebswirtschaftlichen Aspekten. AS versuchen die Kosten für ihren Upstream möglichst gering zu halten, indem sie direkt mit den AS peeren, mit denen sie

viele Daten austauschen. Daher ist es für AS-Betreiber wichtig, ihren Datenverkehr zu beobachten und solche AS zu identifizieren, mit denen viele Daten ausgetauscht werden. Sind die Kosten für ein direktes Peering dauerhaft günstiger als die Kosten für den Upstream-Provider in Richtung des anderen AS, wird ein Peering angestrebt. Dabei muss natürlich auch das andere AS eine solche Rechnung durchführen. Mit Hilfe von IXPs lassen sich dabei entsprechende Synergieeffekte erzielen, wenn möglichst viele potentielle Peers PoPs bei denselben IXPs unterhalten.

Ausgehend von diesen Gründen bei der Auswahl von Peers, lassen sich für AS unterschiedliche Richtlinien (engl. peering policies) beschreiben: offenes, geschlossenes oder selektives Peering. Peeringpolicies unterscheiden sich von Routingpolicies dadurch, dass sie die Einstellung eines Unternehmens zu Peering ausdrücken, während Routingpolicies eine Kontrolle der ausgetauschten Routen ermöglichen (vgl. Abschnitt 2.2.2). Diese Informationen werden den anderen Teilnehmern meist über den IXP mitgeteilt. Eine offene Peering Policy drückt aus, dass mit jedem anderen Teilnehmer Peering etabliert werden kann. Insbesondere dafür bietet sich die Verbindung zum IXP-Route-Server an, so wird die maximale Anzahl an Peerings umgesetzt. Eine geschlossene Peering Policy drückt aus, dass ein AS derzeit kein Interesse an weiteren Peeringbeziehungen hat. Ähnlich ist eine selektive Peering Policy, die in der Regel dann gewählt wird, wenn zwar grundsätzlich Peering gewünscht ist aber nicht wie beim offenen Peering mit allen anderen Teilnehmern.

Eine öffentlich bekannte Peering Policy kann Auskunft darüber geben, wie wahrscheinlich ein AS neue Peeringbeziehungen etabliert. So können neu auftretende Verbindungen zwischen AS in den Routingdaten entsprechend bewertet werden.

5.5 Datensammlung

Für die Nutzung weitere Daten werden im Oktober 2013 öffentlich verfügbare Daten von LGs und IXP-Mitgliederlisten gesammelt und ausgewertet. Aufgrund der großen Menge an Autonomen Systemen und IXPs werden zunächst nur die in der EU ansässigen AS und IXPs analysiert. Zum Zeitpunkt der Untersuchung im Oktober 2013 gibt es 28 Mitgliedstaaten in der EU. Über die RIPE

Whois-Datenbank lassen sich in diesen Mitgliedstaaten 11.500 Autonome Systeme identifizieren. Dies sind etwas 25% der zu diesem Zeitpunkt registrierten AS weltweit. Die berücksichtigten AS annoncieren zu diesem Zeitpunkt etwa 70.000 Prefixe. Eine vollständige Routingtabelle des RIPE RIS im Oktober 2013 listet weltweit etwa 510.000 Prefixe, so dass die betrachteten AS etwa 14% der erreichbaren Prefixe ausmachen.

Das Ziel der Untersuchung ist, weitere Informationen dieser in der EU befindlichen AS zu sammeln, um die Datenbasis für die Anomalieerkennung anzureichern. Ein erster Ansatzpunkt ist die Nutzung der WHOIS-Abfrage vom RIPE. RIPE-WHOIS-Einträge enthalten weitere Informationen über die registrierten AS. Dort findet man neben der AS-Nummer den Namen des AS, den Betreiber, eine allgemeine Beschreibung sowie Kontaktinformationen und zum Teil auch Informationen über Peering-AS. Die Anzahl der Abfragen an der RIPE WHOIS-Datenbank hat zum Zeitpunkt der Untersuchung eine Beschränkung auf 1.000 Abfragen pro anfragende IP-Adresse in 24 Stunden, wenn auch Kontaktinformationen mit abgefragt werden.

Dieses Limit ist bei der Anomalieerkennung schnell erreicht, so dass weitere Quellen mit ähnlichen oder gleichartigen Informationen gesucht werden mussten. Die Webseite peeringdb.com [107] enthält spezifische Informationen über Peeringbeziehungen und bietet auch eine Liste bekannter IXPs in Europa. Dabei handelt es sich im Oktober 2013 um 119 IXPs in der EU sowie die URL der Webseite und die bei peeringdb.com als Teilnehmer registrierten AS.

Einträge in der peeringdb.com-Datenbank enthalten zum Teil auch Links zu LGs innerhalb eines AS. Um in der peeringdb.com-Datenbank geführt zu werden, ist die Aktivität des AS-Betreibers notwendig. Dieser muss sich dort anmelden und notwendige Informationen für den Eintrag hinterlegen. Entsprechend finden sich dort nicht alle registrierten AS sondern nur solche, die darin einen Mehrwert für ihren Betrieb sehen. Es gibt auch AS die als Teil ihrer Peeringpolicy die Existenz eines Eintrags voraussetzen oder IXPs die für ihre Teilnehmer einen Datenbankeintrag in der peeringdb.com-Datenbank zur Bedingung machen. Da die Einträge in der peeringdb.com-Datenbank manuell erstellt und auch manuell gepflegt werden müssen, kann nicht davon ausgegangen werden,

dass die Datenbank aktuell ist. Vielmehr muss davon ausgegangen werden, dass die dort hinterlegten Informationen veraltet und unvollständig sind.

Auf Basis der Liste von EU IXPs werden Informationen über Mitglieder direkt von den Webseiten der IXPs gesammelt. Die meisten IXPs bieten auf ihrer Webseite selbst eine Liste mit den Teilnehmern an und listen zusätzlich noch weitere Informationen, etwa die Peering Policy. Vereinzelt bieten IXPs sogar eine Peering Matrix an aus der die Verbindungen der AS eindeutig hervorgehen. Die Informationen auf den Mitgliederseiten der IXPs sind als deutlich aktueller und wertvoller zu betrachten. Beim Einrichten von Peerings handelt es sich nämlich um das Hauptgeschäftsfeld eines IXPs und die Pflege der Mitgliederlisten ist dafür nicht nur aus marketingtechnischer Sicht ein relevanter Teil des Workflows bei der Einbindung neuer Kunden. Falls keine Peering Matrix angegeben ist, listen viele IXPs zumindest Informationen über die Peering Policies der Mitglieder auf.

Insgesamt 66 der 119 untersuchten IXPs veröffentlichen Informationen über die Peeringpolicies ihrer Kunden. Diese Peeringpolicies werden genutzt, um während der Analyse von Erreichbarkeitsinformationen neue Peeringverbindungen einschätzen zu können. Solche topologischen Informationen sind notwendig, um zu entscheiden, ob ein neuer AS-Pfad nachvollziehbar ist, oder nicht. Es ist wahrscheinlicher, dass zwei AS miteinander eine Peeringverbindung aufbauen, wenn diese Kunden desselben IXPs sind. Die Daten der peeringdb.com-Datenbank zeigen, dass viele AS nicht nur Kunde bei einem IXP sind, sondern in den meisten Fällen bei mehreren IXPs einen PoP unterhalten. Dies erhöht die Anzahl von Peeringmöglichkeiten für die AS, falls diese eine offene Peeringpolicy haben. Im Falle einer selektiven oder geschlossenen Peeringpolicy ist die Wahrscheinlichkeit für neue Peerings geringer, was auf ein insgesamt stabiles Verhalten eines AS hindeutet. Eine offene Peeringpolicy könnte ein Hinweis auf ein kleineres AS sein, da große Tier-1 oder Tier-2 Upstream-Provider aufgrund ihrer monetär ausgerichteten Peeringstrategie meist selektive oder geschlossene Peeringpolicies haben. Die Topologieinformationen eines AS lassen sich mit den AS-Beziehungen von IRL [66] und CAIDA [25] abgleichen.

5.6 Auswertung

Die gesammelte Liste mit 119 IXPs innerhalb der Europäischen Union ist die Grundlage für die Sammlung zusätzlicher Informationen zur Anomalieerkennung. Zum Zeitpunkt der Untersuchung im Oktober 2013 listet peeringdb.com für diese 119 IXPs insgesamt 3.065 verbundene AS. Von den 119 bekannten IXPs konnten 66 Mitgliederlisten heruntergeladen werden. Mit dem hier vorgestellten Ansatz konnten so 5.185 AS als Mitglieder der IXPs identifiziert werden. Die Unterschiede der gesammelten Mitgliederlisten und der peeringdb.com-Datenbank für die sieben größten europäischen IXPs (im Hinblick auf die Mitgliederzahlen) sind in Tabelle 7 dargestellt. Im Vergleich zu den Mitgliedern

Tabelle 7: *Vergleich der Anzahl gefundener AS mit peeringdb.com*

IXP	peeringdb.com	eigene Sammlung
AMS-IX	564	627
DE-CIX	453	515
France-IX	191	449
NL-IX	173	390
V-IX	87	120
Netnod	14	88
DIS-DK	41	42

aus der peeringdb.com-Datenbank wurden mit dem hier vorgestellten Verfahren 74% mehr Mitglieder der sieben größten europäischen IXPs identifiziert. Zusätzlich dazu kann davon ausgegangen werden, dass die direkt von den IXPs gesammelten Daten deutlich aktueller und damit zuverlässiger sind, als die Daten von peeringdb.com.

17 der gesammelten Mitgliederlisten enthielten Informationen zu den Peeringpolicies von insgesamt 2024 unterschiedlichen AS. Trotz der geringen Anzahl können diese zusätzlichen Informationen den Anteil der als legitim klassifizierten Konflikte erhöhen, etwa im Falle von Multihomed-AS. Abbildung 7 zeigt den Anteil der unterschiedlichen Peeringpolicies in der gesammelten Datenbank. Insgesamt wurden 1452 AS mit einer offenen, 454 mit einer selektiven und 92 mit einer geschlossenen Peeringpolicy identifiziert. Von 175 AS konnte die Angabe der Peeringpolicy in den Mitgliederlisten nicht ausgewertet werden. Die Anzahl der IXPs an denen ein einzelnes AS als Mitglied geführt wird, kann

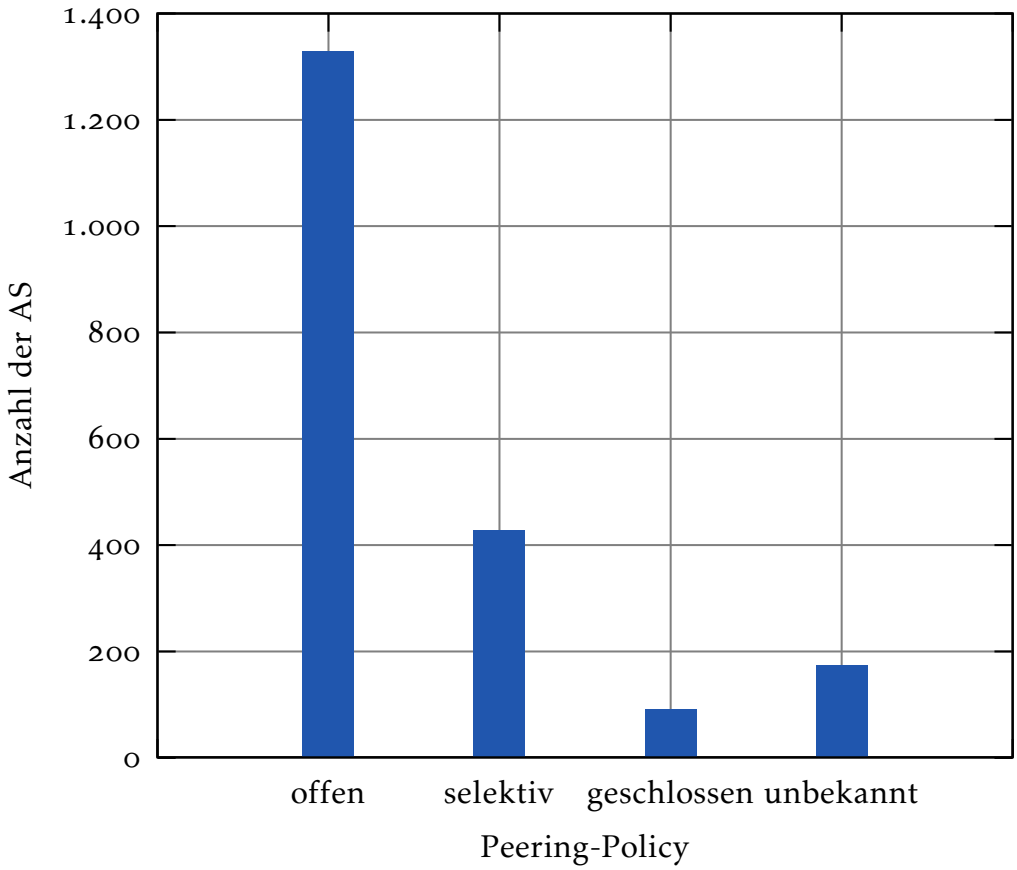

Abbildung 7: *Verteilung der Peeringpolicies*

einen Anhaltspunkt auf die Größe und die Rolle innerhalb der AS-Topologie geben. Daher wurde auch die Anzahl der IXPs an denen ein AS als Mitglied geführt wird untersucht. Abbildung 8 zeigt, dass die meisten der gefundenen AS eher wenige PoPs bei IXPs unterhalten.

Die gefundenen LGs können weitere Hinweise auf die Existenz von Peeringverbindungen liefern. Wenn eine bisher unbekannte Peeringverbindung in einem AS-Pfad erkannt wird, dann sollen die in diesen AS existierenden LGs abgefragt werden. Die Abfrage der LGs nach Nachbarschaftsbeziehungen ist mit unterschiedlichen Kommandos möglich. Eine komplette Routingtabelle gibt die meisten Hinweise auf bestehende Peeringverbindungen. Nicht alle LGs erlauben aber den Zugriff darauf, so dass an dieser Stelle auch mit Traceroutes zuverlässige Ergebnisse möglich sind. Im Gegensatz zu den Arbeiten, in denen Traceroutes ganze AS-Pfade verifizieren, soll in diesem Szenario nur der

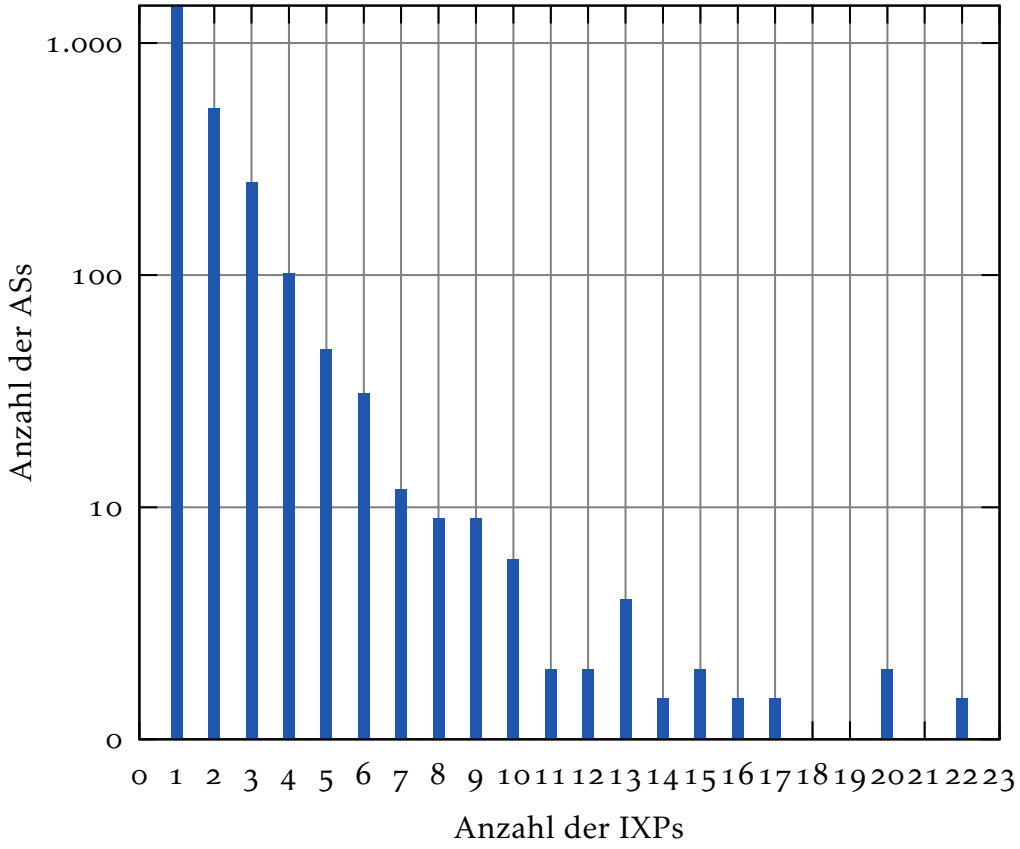

Abbildung 8: *Anzahl der IXPs pro AS*

erste Hop, also das direkte Nachbar-AS abgefragt werden. Bei diesem ersten Hop hat das angefragte AS noch selbst die Entscheidungsmöglichkeit darüber, an welches der benachbarten AS das Datenpaket gesendet wird. Somit ist eine Überprüfung der direkten Verbindung auch mit Traceroutes möglich. Bereits ab dem zweiten Hop in einem AS-Pfad ist diese Überprüfung jedoch nicht mehr zuverlässig.

Von den 116 innerhalb der Europäischen Union gefundenen LGs waren im Rahmen der Untersuchung 97 verwendbar. Abbildung 9 zeigt die Verteilung der LGs auf die Mitgliedsstaaten der EU. Obwohl die Zuordnung der AS in einzelne Länder der EU erfolgt, betreiben die AS ihre LGs an unterschiedlichen Standorten auf dem gesamten Erdball und haben entsprechende Peeringverbindungen. Somit eignen sich diese LGs nicht nur für die Verifikation innereuropäi-

scher Peeringverbindungen sondern erlauben die Betrachtung von Konflikten im gesamten Internet.

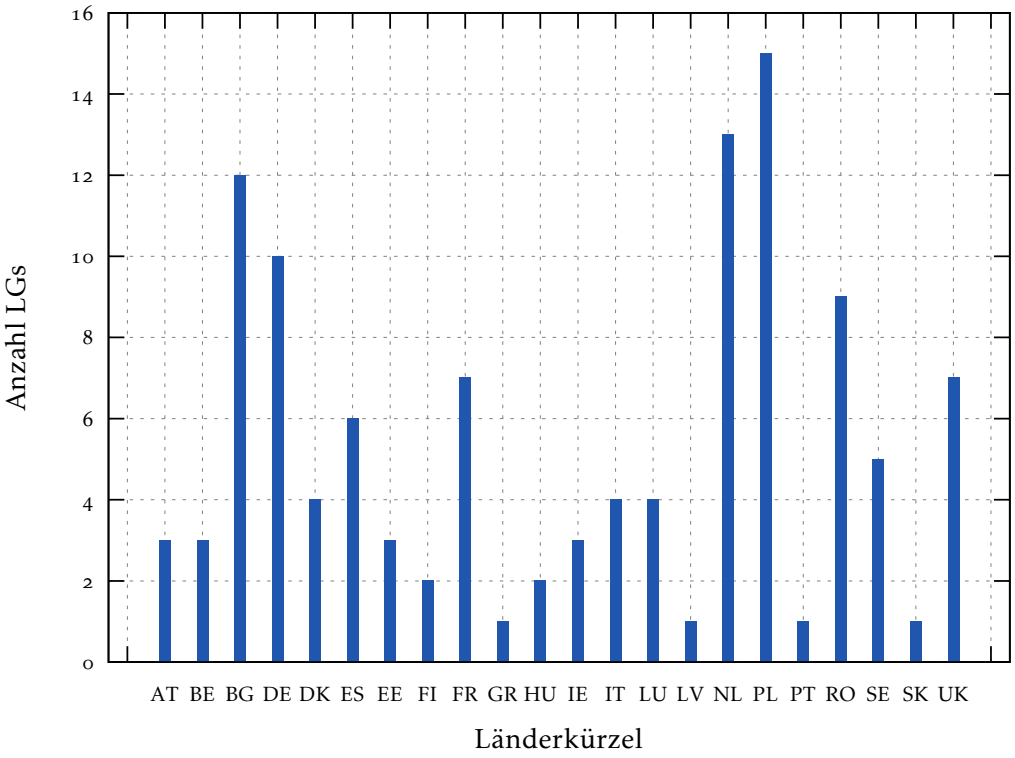

Abbildung 9: *Zuordnung der LGs auf die Länder der Europäischen Union*

5.7 Fazit

In diesem Kapitel wurden öffentliche Informationen über bestehende und mögliche Peeringbeziehungen verwendet, um die Datenbasis von Forschung im Routingbereich zu erweitern und zu verifizieren.

LGs erweitern die Sicht auf Inter-AS-Peeringbeziehungen im Internet, die grundlegend durch Routingarchive wie RIPE RIS, Routeviews und PCH gegeben ist. Die Klassifikation bisher unbekannter Verbindung allein auf Basis der historischen Archivdaten ist nur sehr schwer möglich. Die Abfrage von Looking-Glass-Servern zeigte sich mit viel manuellem Aufwand für die Anpassung an unterschiedliche Softwareversionen als sehr mühsam, wobei die erhaltenen Informationen als sehr zuverlässig zu betrachten sind.

Es wurde gezeigt, dass öffentliche Mitgliederdatenbanken weitere Hinweise auf die Existenz von Verbindungen zwischen AS geben. Für die Arbeiten wurden alle europäischen IXPs mit öffentlich verfügbaren Mitgliederlisten untersucht. Die 66 nutzbaren Mitgliederlisten von Internetknotenpunkten bieten mit mehr als 70% zusätzlichen Mitgliedern für die sieben größten europäischen Internetknotenpunkte deutlich mehr Informationen als etwa die auf peeringdb.com freiwillig hinterlegten Daten. Die zusätzlich gesammelten Peeringpolicies der Mitglieder lassen sich für die noch präzisere Analyse neuer Verbindungen zwischen AS verwenden.

Die aus den öffentlich verfügbaren Mitgliederlisten der Internetknotenpunkte zusätzlich gesammelten Daten werden in dem folgenden Kapitel 6 verwendet, um mögliche weitere Verbindungen zwischen AS und die Auswirkungen auf die Prefix-Hijacking-Resilienz zu überprüfen.

6 Analyse: Prefix-Hijacking-Resilienz[6]

Zusammenfassung des Kapitels Prefix-Hijacking ist nach wie vor eine große Bedrohung im Internetrouting. Bestätigte Vorfälle in der Vergangenheit zeigen, dass auch kleine Autonome Systeme in der Lage sind, Erreichbarkeitsinformationen zu manipulieren und damit eine große Wirkung zu erzielen. Obwohl Ansätze zum Schutz von Prefixen existieren, sind diese nicht ausreichend genug verbreitet, um eine kritische Masse zu erreichen. Derzeit ist die bevorzugte Möglichkeit für AS das kontinuierliche Monitoring eigener Prefixe, um zeitnah Prefix-Hijacking-Vorfälle zu erkennen. Auf Basis vorhandener Topologieinformationen kann die Widerstandsfähigkeit von AS gegen Prefix-Hijacking ermittelt werden. In diesem Kapitel wird die Ungenauigkeit der Formel zur Berechnung von Prefix-Hijacking evaluiert und durch eine verbesserte Formel ausgeglichen. Zusätzlich wird die Rolle von Internetknotenpunkten für die Nutzung von Peeringmöglichkeiten untersucht. Dabei werden die Ergebnisse des vorigen Kapitels, die zusätzlichen Informationen über Mitglieder von IXPs, verwendet. Darüber hinaus wird der Effekt zusätzlicher Verbindungen eines AS durch tatsächlich existierende Möglichkeiten zum Peering überprüft.

[6] Die Inhalte basieren auf M. Wübbeling und M. Meier. „Improved Calculation of AS Resilience against IP Prefix Hijacking“. In: *2016 IEEE 41st Conference on Local Computer Networks Workshops (LCN Workshops)*. 2016, S. 121–128

Annonciert ein AS den IP-Adressraum eines anderen AS spricht man von Prefix-Hijacking (dt. Prefixentführung). Betrachtet man den Ursprung eines Prefixes als Origin, existieren als Folge von Prefix-Hijacking mehrere, zunächst gleichwertige Origins für ein Prefix. Da einer der Origins der tatsächliche Besitzer eines Prefixes ist und der andere Origin fälschlicherweise das Prefix des Besitzers annonciert, ist es sinnvoll, die Origins diesbezüglich zu unterscheiden: Der legitime Besitzer ist der wahre Ursprung (engl. true origin) und das illegitim annoncierende AS ist der falsche Ursprung (engl. false origin). Pakete, die an betroffene IP-Adressen des True Origin adressiert sind, werden dann dem False Origin zugestellt. Das betrifft jedoch nicht alle Pakete, sondern nur die Pakete von Kommunikationspartnern jener AS, die den Pfad zu dem False Origin des Prefix auswählen, sich also im Hinblick auf Routing näher an dem illegitimen Besitzer befinden. In jedem Fall führt Prefix-Hijacking zu einer Beeinträchtigung der Verbindungen des True Origin mit einigen seiner Kommunikationspartner.

Beispiel: Zustellung von Briefpost

Vergleichbar ist ein solcher Vorgang mit der Zustellung von Briefpost. Befestigt ein Hausbewohner die Hausnummer des Nachbarhauses gut sichtbar an der eigenen Außenwand, ist es möglich, dass einige Briefe in den falschen Briefkasten eingeworfen werden. Allerdings werden auch in diesem Fall nicht alle Briefe falsch eingeworfen. Der Briefträger wird die Briefe in das Haus einwerfen, an dem er zuerst vorbei kommt, er also den kürzesten Weg zurücklegen muss. Je nach Fahrtrichtung ist das also entweder der Briefkasten des wahren oder des falschen Empfängers.

Ein Angreifer kann durch Prefix-Hijacking bewusst IP-Adressen eines AS übernehmen und so Datenpakete, die nicht an ihn adressiert sind, umleiten und darauf zugreifen. Prefix-Hijacking ist eine permanente Bedrohung des Internetroutings. Edward Snowden veröffentlichte Dokumente der National Security Agency (NSA), aus denen hervorgeht, dass die NSA in der Lage ist, das Internetrouting maßgeblich zu beeinflussen und Datenverkehr gezielt über AS zu leiten, in denen die NSA diesen Datenverkehr analysieren kann [97]. Veröffentlichungen zeigen, dass nicht nur staatliche Akteure wie die NSA oder das chinesische Unternehmen China Telecom [36], in der Lage sind, Prefix-Hijacking gezielt

einzusetzen. Auch kleine Unternehmen mit verhältnismäßig kleinen AS, die topologisch gesehen keine relevante Rolle für das Internetrouting besitzen, können erfolgreich die Prefixe anderer AS übernehmen [75, 138]. Das gegenseitige Vertrauen von AS untereinander, wie es implizit durch BGP bedingt wird, ist eine massive Einschränkung und ermöglicht so maßgeblich Prefix-Hijacking. Historisch setzen auch andere Internetprotokolle gegenseitiges Vertrauen beteiligter Akteure voraus. Im Gegensatz zu BGP wurden aber Protokolle wie HTTP [45], SMTP [76] und TELNET [110] schrittweise aktualisiert und an die Bedürfnisse angepasst oder großflächig ausgetauscht. BGP ist zwar in der Versionsgeschichte aktualisiert worden, allerdings nicht maßgeblich in den Bereichen Authentifikation oder Validierung von Erreichbarkeitsinformationen.

Es gibt neben Vorschlägen zur Erweiterung von BGP noch protokollunabhängige Ansätze, um die Sicherheit des Internetroutings zu erhöhen. Allerdings konnte sich noch kein Mittel erfolgreich durchsetzen. „Resource Public Key Infrastructure“ (RPKI) ist der wohl bekannteste Ansatz, die Nutzungsstatistik der einzelnen RIR für RPKI lag 2016 zwischen 0,6% und 12%. Das bedeutet, dass AS nur wenige Möglichkeiten haben, ihre Prefixe proaktiv vor Prefix-Hijacking zu schützen. Gerade deshalb ist es wichtig zu verstehen, wie Prefix-Hijacking funktioniert und welche Effekte und reaktiven Maßnahmen es gibt.

Es gibt zwei unterschiedliche Ursachen für Prefix-Hijacking: auf der einen Seite stehen dabei Fehlkonfigurationen von Border-Routern, auf der anderen Seite gezielte Angriffe gegen einzelne Netzbereiche. Im Gegensatz dazu sind die tatsächlichen Folgen und mögliche Gegenmaßnahmen bisher weitgehend unerforscht. Betrachtet man die aus Prefix-Hijacking resultierende Partitionierung des Internets, als eine Folge von Prefix-Hijacking, so kann die individuelle Widerstandsfähigkeit (engl. resilience) ein wichtiger Indikator sein. Prefix-Hijacking-Resilienz (kurz: Resilienz), wie von Lad et al. [81] vorgeschlagen, lässt sich nutzen, um den potentiellen Erfolg eines Angreifers zu bestimmen. Dabei sind die *Resilienz* und der *Impact* die Kenngrößen der resultierenden Partitionen bei einem Prefix-Hijacking-Vorfall. Leider ist die von Lad et al. vorgeschlagene Formel zur Berechnung ungenau, da sie nicht die Eigenschaften von BGP berücksichtigt. Grundsätzlich scheint zwar die Anzahl an Peeringverbindungen eines AS Auswirkungen auf die Resilienz zu haben, allerdings ist auch die Auswahl der Peers von entscheidender Bedeutung. Um zusätzliche Verbindun-

gen zu etablieren und so die eigene Resilienz zu steigern, soll auf möglichst kostengünstige Möglichkeiten zurückgegriffen werden. Dafür eigenen sich Verbindungen zwischen solchen AS, die bereits Mitglied desselben IXPs sind. Meist reicht dann die Konfiguration des Peerings in den Border-Routern.

Die in diesem Kapitel beschriebenen Arbeiten machen dabei drei wichtige Beiträge zur Bewertung von Prefix-Hijacking-Resilienz und der Nutzung von Peeringmöglichkeiten:

1. Die existierende Formel zur Berechnung von Prefix-Hijacking-Resilienz wird analysiert und die Ungenauigkeit in der Formel an einem kleinen Testnetzwerk entsprechend veranschaulicht.
2. Eine verbesserte Formel zur Berechnung wird vorgestellt und genutzt, um die Prefix-Hijacking-Resilienz von im Internet aktiven AS zu berechnen. Zur Berechnung der Abweichungen der von Lad et al. vorgestellten Formel werden beide Formeln für die Berechnung der Resilienz derselben AS verwendet.
3. Die verbesserte Formel wird genutzt, um die Möglichkeiten von IXPs für die Vernetzung und damit unmittelbar für die Prefix-Hijacking-Resilienz zu bewerten.

6.1 Verwandte Arbeiten

Prefix-Hijacking als Folge fehlender Sicherheitsmechanismen ist in der Literatur bereits bekannt. Regelmäßige Anomalien im globalen Internetrouting bestätigen die Schwachstelle und zeigen auch, dass es keine ausreichenden Gegenmaßnahmen gibt. Es wurden Erweiterungen für BGP und neue Protokolle entwickelt, um die Schwächen von BGP auszugleichen und eine Authentifikation der Erreichbarkeitsinformationen zu ermöglichen. Keiner dieser Ansätze wurde bisher in großem Maße umgesetzt. Lediglich RPKI zeigt weiterhin wachsende Anwendungszahlen, wenngleich für eine erfolgreiche Umsetzung noch deutlich mehr AS die Absicherung der Prefixe berücksichtigen müssen.

6.1.1 Proaktiver Schutz

Wendlandt et al. fokussieren in ihrer Arbeit das Ziel der sicheren Kommunikation und argumentieren, dass Internetrouting nur sehr schwer abzusichern ist und deshalb Ansätze zur sicheren Kommunikation auf Basis eines unsicheren Internetroutings entwickelt werden müssen. Um unsichere Kommunikation zur unterbinden, sollen möglichst ausschließlich abgesicherte Kommunikationsinhalte übermittelt werden. DNSSec erlaubt die Authentifikation von DNS-Informationen auch über unsichere Kanäle. Andere gängige Protokolle im Internet, etwa HTTP, SMTP, SIP oder SSH besitzen bereits als kryptografisch sicher geltende Verfahren zur Verschlüsselung und gegenseitigen Authentifikation. Dabei kann es natürlich zu einer Nicht-Erreichbarkeit des legitimen Kommunikationspartner kommen (vgl. Abschnitt 3.3.1).

Diese Nicht-Erreichbarkeit wird durch einen weiteren proaktiven Ansatz von Grey et al. [57] adressiert, wenngleich der Fokus auf der Zuverlässigkeit von VPN-Netzwerken basiert. Die Schwächen auf der Protokoll-Ebene von BGP können genutzt werden, um VPN-Netzwerke von Organisationen anzugreifen und den Aufbau von geschützten Verbindungen zu verhindern. Prefix-Hijacking ist dabei einer von mehreren Angriffen gegen VPN-Netzwerke auf Routingebene, die von Grey et al. untersucht werden. Das vorgeschlagene Overlay-Netzwerk basiert auf Peer2Peer-Kommunikation (auf Anwendungsebene) und erlaubt trotz fehlerhafter Erreichbarkeitsinformationen die zuverlässige Verwendung des VPN-Netzwerks. [57]

6.1.2 Monitoring

Da proaktive Maßnahmen auf Protokollebene nicht ausreichend sind, wurden Ansätze zum Monitoring von Prefixen zur Erkennung von Prefix-Hijacking entwickelt. Diese basieren ebenfalls auf unterschiedlichen öffentlich verfügbaren Informationen über das Internetrouting, hauptsächlich Routeviews [61, 82, 129] aber auch RIPE RIS [118].

Lad et al. [82] schlagen ein Benachrichtigungs-System vor, dass nach einer Registrierung die entsprechenden Prefixe überwacht und die Besitzer im Falle eines auftauchenden False Origins informiert. Die Analyse der Erreichbarkeitsinformationen im Rahmen der Evaluation finden auf Basis der Routeviews Archi-

ve statt, lassen sich aber ohne Aufwand um Daten aus anderen Archiven wie RIPE RIS erweitern. PHAS erkennt dabei Änderungen in der Origin-Struktur für Prefixe und setzt diese in einen zeitlichen Zusammenhang. Wurde ein Prefix-Hijacking-Fall entdeckt, erfolgt die Benachrichtigung an die Besitzer per E-Mail. Da eine E-Mail-Zustellung im Falle eines Prefix-Hijacking möglicherweise nicht möglich ist, empfehlen Lad et al. die Registrierung unterschiedlicher E-Mail-Adressen, insbesondere von gut angebundenen Dienstleistern wie Googlemail oder Yahoo. Für die weitere Klassifikation eines erkannten Falls, werden die AS-Pfade der Announcements im Hinblick auf die letzten Hops vor dem Origin sowie möglicherweise betroffene Sub-Prefixe untersucht.

Hu und Mao [61] verwenden zusätzlich dazu für die Echtzeit-Alarmierung noch Daten aus sieben zusätzlichen AS, die ohne Verzögerung nutzbar sind. Die Erkennung von Prefix-Hijacking erfolgt über eine Kombination aus erkannten MOAS-Konflikten und Fingerprinting von erreichbaren Hosts ausgehend von Servern des Forschungsverbunds „Planetlab“ [109]. So können von unterschiedlichen AS ausgehend Informationen über Computer innerhalb betroffener Prefixe gesammelt und analysiert werden.

Shi et al. [129] nutzen zusätzlich zu den Daten der Routeviews Archive weitere Live-Updates von BGPmon [102]. Für die Verifikation von Prefix-Hijacking werden Routingdaten aus öffentlichen Route-Servern verwendet und Looking-Glass für den Versand von Pings (ähnlich dem Ansatz von Hu und Mao) genutzt, um die Erreichbarkeit eines Endpunkts zu testen. Dabei argumentieren Shi et al., dass eine Nutzung von Planetlab-Servern zur weiteren Analyse schon deshalb nicht optimal sei, weil es keinen direkten Bezug von Planetlab zu BGP gäbe. Grundsätzlich lässt sich eine Erreichbarkeit von Endpunkten in den betroffenen Prefixen also auch über Ping-Kommandos testen, solange ICMP-Nachrichten nicht gefiltert werden.

6.1.3 Risikoanalyse Prefix-Hijacking

Um auf Basis der bereits genannten Arbeiten Aussagen über mögliche Folgen von Prefix-Hijacking treffen zu können, schlagen Lad et al. eine Formel zur Berechnung der Widerstandsfähigkeit gegen Prefix-Hijacking vor. Die Formel ist bis dato die wissenschaftlich akzeptierte Berechnungsgrundlage der Resilienz

von AS. Leider ist bei der Entwicklung der Formel der Dynamik von BGP nicht ausreichend Rechnung getragen worden. Bei der Berechnung wird nicht berücksichtigt, dass BGP ein Pfadvektorprotokoll ist und die Routenauswahl des Vorgängers auf einem AS-Pfad die Möglichkeiten nachfolgender AS maßgeblich beeinflusst. Bevor in einem späteren Abschnitt die Berechnungsformel genauer analysiert wird, soll sie an dieser Stelle noch einmal dargestellt werden.

Lad et al. definieren eine β-Funktion entsprechend Formel 6.1, um die Auswirkungen (engl. impact) eines Angreifers a (in diesem Fall also False Origin) in einem Prefix-Hijacking-Fall für ein beliebiges Prefix eines Opfers t (also True Origin) zu berechnen. Für die Funktion benötigen sie darüber hinaus einen weiteren Kommunikationspartner v, der von a falsche Erreichbarkeitsinformationen für ein Prefix von t erhält und diese übernimmt.

$$\beta(a,t,v) = \begin{cases} 1, & \text{falls } v \text{ falsche Informationen von } a \text{ erhält} \\ & \text{und für das Prefix von True Origin } t \text{ nutzt} \\ 0, & \text{sonst} \end{cases} \tag{6.1}$$

Zusätzlich argumentieren Lad et al., dass der Impact gleich der Resilienz eines AS ist. Das lässt sich einfach nachvollziehen, da es bei Impact und Resilienz gleichermaßen darum geht, eigene Prefixe im Internet zu verbreiten, lediglich die Rolle ist jeweils eine andere[7].

Die β-Funktion in dieser Form lässt sich nur dann anwenden, wenn die Routenauswahl von v bekannt ist. Dies ist leider auf Basis der in Routingarchiven enthaltenen Informationen nicht immer der Fall, vor allem dann nicht, wenn kein tatsächliches Prefix-Hijacking vorliegt. Dann konkurrieren a und t nämlich nicht und die jeweiligen Routen zu den Prefixen von a und t werden von v entsprechend für beide AS gewählt. Wird beim Auswahlprozess also die Länge der Pfade relevant, dann kann mit der β-Funktion kein Wert mehr ermittelt werden. Lad et al. schlagen für diesen Fall vor die Wahrscheinlichkeit der Routenauswahl auf Basis einer Gleichverteilung der kürzesten Pfade von a und t zu v zu betrachten und als Auswahlprozess abzubilden. Dafür nutzen sie in einem

[7] Mit dem defensiven Fokus auf IT-Sicherheit wird im weiteren Verlauf dieser Arbeit daher vordergründig die Resilienz betrachtet.

weiteren Schritt die Funktion $\overline{\beta}$, die die resultierende Wahrscheinlichkeit für die Auswahl des Pfads von v zu a berechnet. Bei der Routenauswahl wird für einen Prefix nur der jeweils kürzeste AS-Pfad zu den Origins a und t berücksichtigt. Die $\overline{\beta}$-Funktion wird also nur genutzt, wenn die kürzesten Pfade zu a und die kürzesten Pfade zu t gleich lang sind. Dabei kann es mehrere kürzeste Pfade von v zu a und von v zu t geben. Diese Anzahl der kürzesten Pfade von v zu einem beliebigen n wird von der Hilfsfunktion $p(v,n)$ zurückgegeben[8]. Daher betrachtet $\overline{\beta}$ die Verteilung über alle kürzesten Pfade zu den jeweiligen Origins entsprechend Formel 6.2.

$$\overline{\beta}(a,t,v) = \frac{p(v,a)}{p(v,a)+p(v,t)} \tag{6.2}$$

Der Wert der Resilienz des True Origin t gegen Prefix-Hijacking lässt sich auf Basis dieser Funktion mit einer einfachen Gleichung ermitteln. Die Anzahl aller Pfade zu dem True Origin wird geteilt durch die Anzahl aller kürzesten Pfade für ein Prefix. Nun muss für beliebige Angreifer a und beliebige Kommunikationspartner v der entsprechende Wert für $\overline{\beta}(t,a,v)$ berechnet und summiert werden. Abschließend wird entsprechend der Durchschnitt gebildet und das Ergebnis ist die Resilienz des True Origin entsprechend der Formel 6.3 (die Notation dieser Formel ist mehrdeutig, dennoch wurde sie ohne Änderungen aus [81] übernommen).

$$R(t) = \sum_{a \in N} \sum_{v \in N} \frac{\overline{\beta}(t,a,v)}{(N-1)(N-2)} \tag{6.3}$$

6.2 Bewertung der Resilienz Autonomer Systeme

Um die Berechnung der Resilienz eines AS gegen Prefix-Hijacking zu bewerten sollen unterschiedliche Routingsituationen simuliert werden. Zunächst werden die Vorbedingungen und der Versuchsaufbau des Experiments dargestellt und anschließend die Mängel der Formel von Lad et al. näher erläutert.

[8] An dieser Stelle sei bereits angemerkt, dass eine saubere Definition der Variablen und entsprechender Mengen durch Lad et al. zu keinem Zeitpunkt stattfindet.

6.2.1 Aufbau

Die Simulation basiert auf drei unterschiedlichen öffentlich verfügbaren Datentypen für die Analyse von Routinganomalien. Um Erreichbarkeitsinformationen zu berücksichtigen werden Archive des RIPE RIS verwendet. Diese beinhalten Informationen aus der Control-Plane, die von Route Reflector Clients (RRC) gesammelt werden. Um einfache Routingpolicies umsetzen zu können, werden die Topologieinformationen von CAIDA verwendet. Routingmöglichkeiten werden mit IXP-Mitgliederinformationen abgeglichen, die als Ergebnisse aus den Arbeiten zu Kapitel 5 zur Verfügung stehen.

Um die Daten miteinander verwenden zu können, ist es wichtig, dass diese etwa zum selben Zeitpunkt erhoben werden. Für die Untersuchung wurde der 1. Februar 2015, 08:00 Uhr MEZ als Zeitpunkt festgelegt. Für die Daten der Control-Plane werden die Daten der zu dem Zeitpunkt aktiven $RRC_x.x \in \{00, 01, 03, 04, 05, 06, 07, 10, 11, 12, 13, 14, 15\}$ verwendet. Diese Erreichbarkeitsinformationen werden angereichert mit den Topologieinformationen des CAIDA mit dem Label „20150201“, die laut CAIDA-Webseite alle Announcements aus dem gesamten Januar 2015 berücksichtigen. Enthalten die Topologieinformationen AS-Verbindungen, die keine Entsprechung in den Daten des RIPE RIS haben, werden diese als gültig angenommen und der Liste der AS-Verbindungen hinzugefügt.

Wie in Kapitel 2.2.3 beschrieben, ist das Internet umgangssprachlich aufgeteilt in Tier-1, Tier-2 und Tier-3 AS. Um diese Topologieinformationen formaler zu betrachten, soll diese Hierarchie näher an die tatsächliche Topologie angepasst werden. Dafür sollen im Folgenden AS in Ebenen organisiert werden. Diese Ebenen repräsentieren die Tiefe eines AS in Relation zu einem Tier-1 AS, das der Ebene 0 zugeordnet ist. Die Ebene 0 dieser Betrachtung entspricht dabei fast der Menge an Tier-1 AS aus der umgangssprachlichen Betrachtung: es ist die Menge aller AS, die alle Teilnehmer des Internets ohne Upstream-Provider erreichen können. Graphentheoretisch handelt es sich um eine Clique, also untereinander verbundene AS, die über ihre Peeringbeziehungen unterschiedliche Teile des Internets miteinander verbinden. Einige Betreiber dieser AS unterhalten verschiedene AS mit jeweils eigenen Nummern. Diese werden zwar nicht so häufig verwendet, lassen sich aber in den AS-Pfaden der Erreichbarkeitsin-

formationen erkennen. Bei differenzierter Betrachtung würden diese AS-Pfade gelegentlich zu eigenartigen Ergebnissen, wie Kreisen in den Pfaden, führen.

Beispiel: Kreise in AS-Pfaden
Der AS-Betreiber Verizon verwendet unter anderem die AS-Nummern 701, 702 und 703. Diese AS stehen vermutlich in einer Sibling-to-Sibling-Beziehung (vgl. Abschnitt 2.2.3) In AS-Pfaden finden sich Abschnitte wie „[...] 702 701 702 [...]“. Solche Pfade werden eigentlich durch die Implementierungen von BGP verhindert. Befindet sich das eigene AS bereits im Pfad eines Announcements, wird es nämlich nicht weiter verarbeitet. Die Router des AS 702 würden die BGP-Nachrichten von Routern des AS 701 nicht weiter verarbeiten, da AS 702 im Pfad bereits existiert.

Um solche AS-Nummern zu identifizieren, werden alle Pfade ermittelt, die derartige Kreise enthalten und die Betreiber der AS-Nummern mit den RIR-Whois-Datenbanken abgeglichen. Anschließend werden die zusätzlichen AS-Nummern der Liste der Ebene-0-AS hinzugefügt, um diese Ebene möglichst vollständig zu erfassen. Darüber hinaus werden jene AS zur Ebene 0 hinzugefügt, die die Clique erweitern, also zu allen bisherigen Clique-Mitgliedern entsprechende Peeringbeziehungen unterhalten, unter der Maßgabe einer möglichst großen Clique.

Die für die Simulation berechnete Topologie enthält 6 Ebenen. Die anteilige Verteilung der AS auf diese Ebenen ist in Tabelle 8 dargestellt.

Tabelle 8: *Ebenen der Internet-Hierarchie*

Ebene	0	1	2	3	4	5
# AS	22	15.882	29.488	5.842	335	61
% der AS	0,04	30,80	57,18	11,33	0,65	0,12

Die Topologieinformationen von CAIDA erlauben die Berücksichtigung von AS-Beziehungen bei der Simulation der Verbreitung von Erreichbarkeitsinformationen. So kann insbesondere das in Kapitel 2.2.3 vorgestellte Valley-Free-Paradigma eingehalten werden.

Um über alle Simulationsdurchläufe vergleichbare Ergebnisse zu erhalten, wurde im Vorfeld eine Menge von 100 Angreifern bestimmt. Diese werden zufällig

aus der Menge aller AS herausgesucht. Dabei ist diese Auswahl näherungsweise gleichverteilt über den Hierarchie-Ebenen. Tabelle 9 zeigt die Anzahl der Angreifer aus jedem AS-Level.

Tabelle 9: *Verteilung der Angreifer auf AS Ebenen*

Ebene	0	1	2	3	4	5	Summe
# Angreifer	0	31	56	11	2	0	100

6.2.2 Mängel der Formel von Lad et al.

Wie bereits beschrieben schlagen Lad et al. eine Formel zur Berechnung der Prefix-Hijacking-Resilienz vor. Die aus dieser Formel resultierende Wahrscheinlichkeit berücksichtigt dabei nur annähernd die Eigenschaften von Peering und ist daher nicht so exakt, wie möglich. Die Formel berücksichtigt dabei nicht die Eigenschaften von BGP als Pfadvektorprotokoll. Das führt dazu, dass Routingentscheidungen von Vorgänger-AS auf dem Verbreitungspfad von Erreichbarkeitsinformationen nicht entsprechend berücksichtigt werden. In der Evaluation von Lad et al. wird jeder mögliche kürzeste Pfad für die Betrachtung herangezogen. Eine realistische Betrachtung müsste diese Routingentscheidung aber mit einbeziehen, denn auf Basis dieser Entscheidung werden Erreichbarkeitsinformationen überhaupt nur an die Nachbar-AS weitergegeben. Da die zur Verfügung stehenden Routingdaten nicht vollständig die Realität widerspiegeln eignen sich diese nicht zum entsprechenden Gegenbeweis. Daher diskutieren die nächsten Abschnitte die Mängel der von Lad et al. vorgeschlagenen Formel. Abbildung 10 dient dabei der einfachen Demonstration zur Unterstützung der Argumentation.

Führt man die Formel von Lad et al. auf dem Graphen des Testnetzwerks durch, erhält man die Werte, die in Tabelle 10 dargestellt sind. Betrachtet man die Verteilung der Erreichbarkeitsinformationen, weicht der Wert für AS 2 von den Erwartungen ab. Um das Problem deutlicher zu zeigen, sollen einige Zwischen-

Tabelle 10: *Resilienz berechnet mit der Formel von Lad et al.*

$a \in AS$	1	2	3	4	5	6
$R(a)$	0,65	0,4875	0,425	0,1375	0,65	0,3

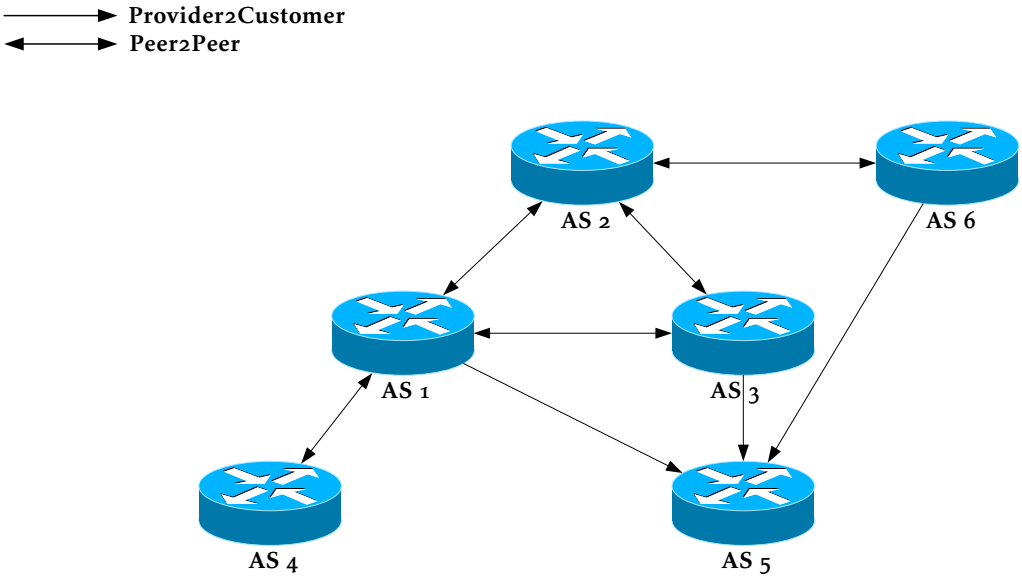

Abbildung 10: *AS-Peering-Graph des Testnetzwerks*

ergebnisse der Berechnung für den Wert von AS 2 im Detail nachgerechnet werden. Betrachtet man insbesondere den Teil der Rechnung, in dem (für ein beliebiges Prefix) AS 2 True Origin, AS 4 False Origin und AS 5 das betrachtete, möglicherweise betrogene AS in der Formel ist. Es gibt drei kürzeste Pfade von AS 5 zum True Origin AS 2. Nur ein kürzester Pfad führt von AS 5 zu False Origin AS 4. Berechnet man nun mit der $\overline{\beta}$-Formel von Lad et al. die Wahrscheinlichkeit, mit der AS 5 einen der Pfade zu AS 2 auswählt, erhält man folgerichtig als Ergebnis $\frac{3}{4}$. Die Gegenwahrscheinlichkeit, also die Wahrscheinlichkeit der Auswahl eines Pfads zu AS 4 beträgt damit $\frac{1}{4}$.

Mit Berücksichtigung der erwähnten Routingdynamik erscheint dieses Zwischenergebnis eigenartig. Bevor die Erreichbarkeitsinformationen von AS 1 an AS 5 weitergeleitet werden, wählt AS 1 bereits einen der kürzesten Pfade, entweder zu AS 2 oder zu AS 4 aus. Nur die dieser Auswahl entsprechenden Erreichbarkeitsinformationen werden dann an AS 5 weitergeleitet. Das bedeutet, dass AS 1 entscheidet, welcher Pfad AS 5 für die Routenauswahl zur Verfügung steht. Betrachtet man im Gegenzug die anderen beiden Pfade von AS 2 zu AS 5, so werden diese von AS 3 bzw. AS 6 ohne weitere Entscheidungsmöglichkeit weitergegeben, da es sich dort um die einzigen kürzesten Pfade handelt. Das bedeutet, um die korrekte Wahrscheinlichkeit der Pfadauswahl bei AS 5 zu

bestimmen, muss zunächst die Wahrscheinlichkeit der Pfadauswahl von AS 1 bekannt sein und entsprechend berücksichtigt werden.

Da AS 1 mit beiden Origins direkt verbunden ist, beträgt die Wahrscheinlichkeit der Auswahl jeweils $\frac{1}{2}$. Im nächsten Schritt bedeutet dies, dass die Wahrscheinlichkeit für AS 5 drei Erreichbarkeitsinformationen zu erhalten, die zu AS 2 als True Origin führen $\frac{1}{2} \times \frac{1}{3} + \frac{2}{3} = \frac{5}{6}$ ist. Damit ist die Wahrscheinlichkeit von AS 4 betrogen zu werden im Gegenzug nur noch $\frac{1}{6}$. Verglichen mit den Werten der $\overline{\beta}$-Funktion von Lad et al. berechnet die verbesserte Formel höhere Werte, mit einer Differenz zwischen beiden Werten in Höhe von $0,0833$, was einer Abweichung von mehr als 8% entspricht. Im Bezug auf die gesamte Topologie beträgt die Abweichung insgesamt noch $0,8\%$.

6.2.3 Verbesserung der Resilienz-Formel

Wie beschrieben, berücksichtigt die existierende Formel nicht in vollem Umfang alle möglichen AS-Topologien. Um exaktere Ergebnisse zu erhalten, müssen die Routingentscheidungen der Nachbar-AS ebenfalls berücksichtigt werden. Zu diesem Zweck wird im Folgenden eine verbesserte Formel zur Berechnung der Resilienz vorgestellt.

Die $\beta(t,a,n)$- und $\overline{\beta}(t,a,n)$-Funktionen von Lad et al. berechnen die Wahrscheinlichkeit eines AS n, eine Route zum True Origin t anstelle einer Route zu False Origin a auszuwählen. Um die Ungenauigkeit in dieser Funktion auszugleichen, wird anstelle der beiden Funktionen eine neue Funktion $\beta(t,a,n)$ (6.4) definiert, die rekursiv die Routenauswahl aller AS auf dem Pfad mit einbezieht.

$$\beta(t,a,n) = \begin{cases} 0 & \text{, wenn } \textit{Fall 1} \\ \frac{1}{|P_{(t,a,n)}|} & \text{, wenn } \textit{Fall 2} \\ \sum\limits_{p \in P_{(t,a,n)}} \frac{1}{|P_{(t,a,n)}|} \times \beta(t,a,p) & \text{, wenn } \textit{Fall 3} \end{cases} \tag{6.4}$$

Fall 1: t ist nicht, aber a ist direkter Nachbar von n.
Fall 2: t ist und a kann direkter Nachbar von n sein.
Fall 3: t und a sind beide nicht direkte Nachbarn von n.

Tabelle 11: *Resilienz-Werte berechnet mit der verbesserten Formel*

$a \in AS$	1	2	3	4	5	6
$R(a)$	0,65	0,4917	0,425	0,1333	0,65	0,3

Um Mehrdeutigkeit auszuschließen, sollen die Mengen zunächst definiert werden.

V - die Menge aller AS (engl. vertices).

$A = V \backslash \{t\}$ - die Menge aller mögliche Angreifer AS für einen gegebenes True Origin $t \in V$.

$N = V \backslash \{t, a\}$ - die verbleibenden AS in V. Also die AS, die nicht Angreifer ($a \in A$) und nicht True Origin ($t \in V$) sind.

$P_{(t,a,n)}$ - die Menge der Nachbar-AS, die einen kürzesten Weg zu den Origins $t \in V$ und $a \in A$ an $n \in N$ weiterleiten.

Daraus ergibt sich eine neue Formel für die Resilienz (6.5) auf Basis der Verbreitung von Erreichbarkeitsinformationen mit BGP.

$$R(t) = \sum_{a \in A} \sum_{n \in N} \frac{\beta(t, a, n)}{|A| \times |N|} \tag{6.5}$$

Basierend auf dem Graphen in Abbildung 10 sind die mit dieser Formel berechnet Resilienz-Werte der AS in Tabelle 11 dargestellt.

6.3 Simulation zur Resilienz-Berechnung

In diesem Abschnitt soll die Frage beantwortet werden, ob die Möglichkeiten einer besseren Vernetzung an Internetknotenpunkten die Resilienz Autonomer Systeme beeinflusst. Bevor diese Frage beantwortet wird, soll zunächst die Situation von MOAS-Konflikten näher betrachtet werden. Die Simulation dient dabei ebenfalls dem Vergleich der ursprünglichen Formel zur Berechnung der Resilienz gegen Prefix-Hijacking und der in diesem Kapitel vorgeschlagenen, verbesserten Formel. Abschließend werden die Möglichkeiten zum Peering bei

IXPs berücksichtigt und resultierende Resilienz-Werte ausschließlich mit der verbesserten Formel berechnet.

6.3.1 Multiple Origin AS

Wie in Abschnitt 3.2 erklärt, sind MOAS-Konflikte ein gewöhnliches Phänomen im Internetrouting. Die verwendeten Routingdaten des RIPE RIS enthalten auch Informationen zu MOAS-Konflikten zwischen zwei oder mehreren AS. Zum Zeitpunkt der Untersuchung sind 7.149 Prefixe betroffen. Insgesamt sind dabei 1.983 AS in diese Konflikte involviert. Die Anzahl der in MOAS-Konflikten involvierten AS nach der Zugehörigkeit zu den unterschiedlichen AS-Ebenen ist in Abbildung 11 dargestellt.

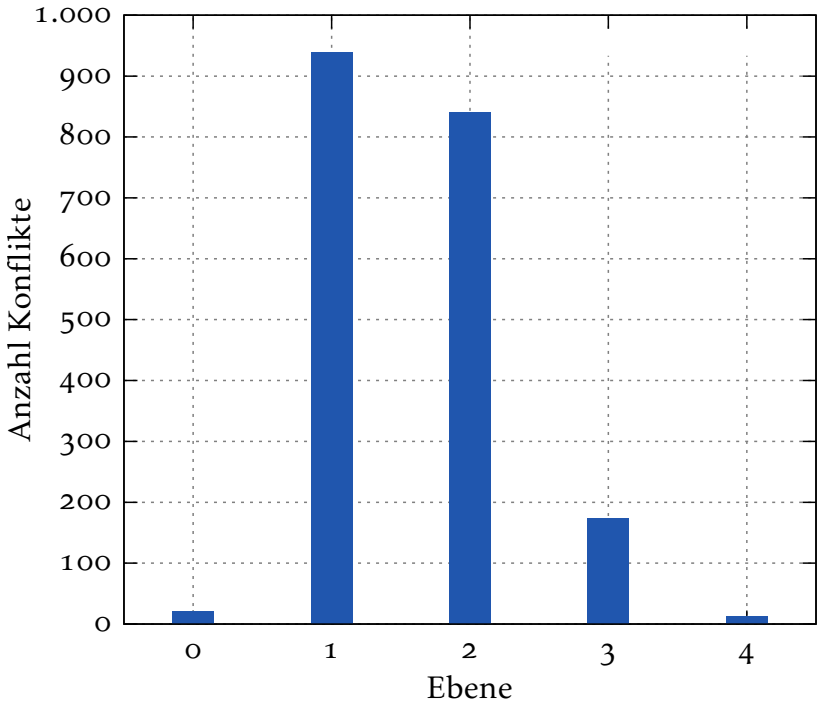

Abbildung 11: *Topologische Position der in MOAS-Konflikte involvierten AS*

Abbildung 12 zeigt die Ausprägung der Ebenen-Unterschiede bei MOAS-Konflikten. Es wird deutlich, dass viele Konflikte zwischen AS auf derselben Ebene stattfinden. Die meisten Konflikte gibt es zwischen AS der Ebene 1 und der Ebene 2, gefolgt von Konflikten bei denen die involvierten AS gemeinsam in

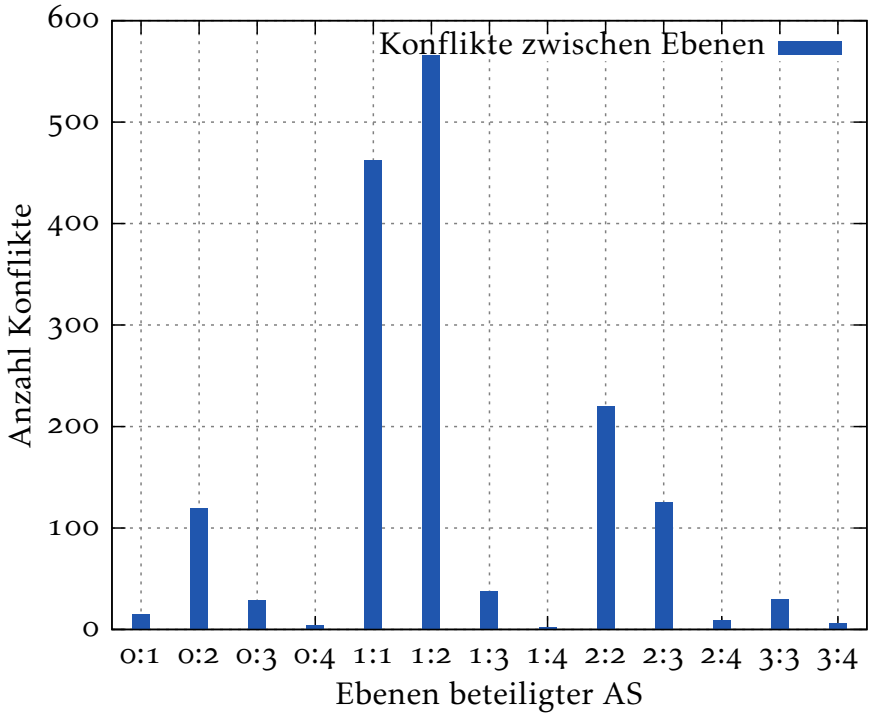

Abbildung 12: *MOAS-Konflikte zwischen unterschiedlichen Ebenen*

Ebene 1 liegen. Von diesen Konflikten innerhalb der Ebene 1 zeigt Abbildung 13 die Unterschiede der berechneten Resilienz-Werte für die beteiligten AS.

Abbildung 13 verdeutlicht, dass die meisten MOAS-Konflikte zwischen AS mit ähnlichen Resilienz-Werten existieren, nämlich innerhalb eines Abstands von 0,2. In diesem Punkt könnte auch einer der Gründe für die MOAS-Konflikte liegen. MOAS-Szenarien lassen sich für Load-Balancing verwenden. Ein Inhalteanbieter (engl. Content Delivery Network, CDN) etwa kann so aus unterschiedlichen AS heraus operieren und MOAS-Szenarien verwenden, um allein auf Basis dynamischer Routingentscheidungen möglichst kurze Pfade zum Konsumenten anzubieten. Wird MOAS etwa für solches Load-Balancing verwendet, sollten AS mit ähnlichen Eigenschaften bevorzugt kooperieren. Das Ziel dabei ist eine gute Aufteilung der übrigen AS in entsprechende Partitionen, so dass alle am Load-Balancing beteiligten AS in etwa dieselbe Anzahl an AS bedienen können. Nur wenige Konflikte haben eine deutliche höhere Differenz der Resilienz-Werte, von 0,2 bis 0,72. Zwar mag es Gründe für entsprechende Kooperationen zwischen solchen AS geben, allerdings kann das auch ein Indi-

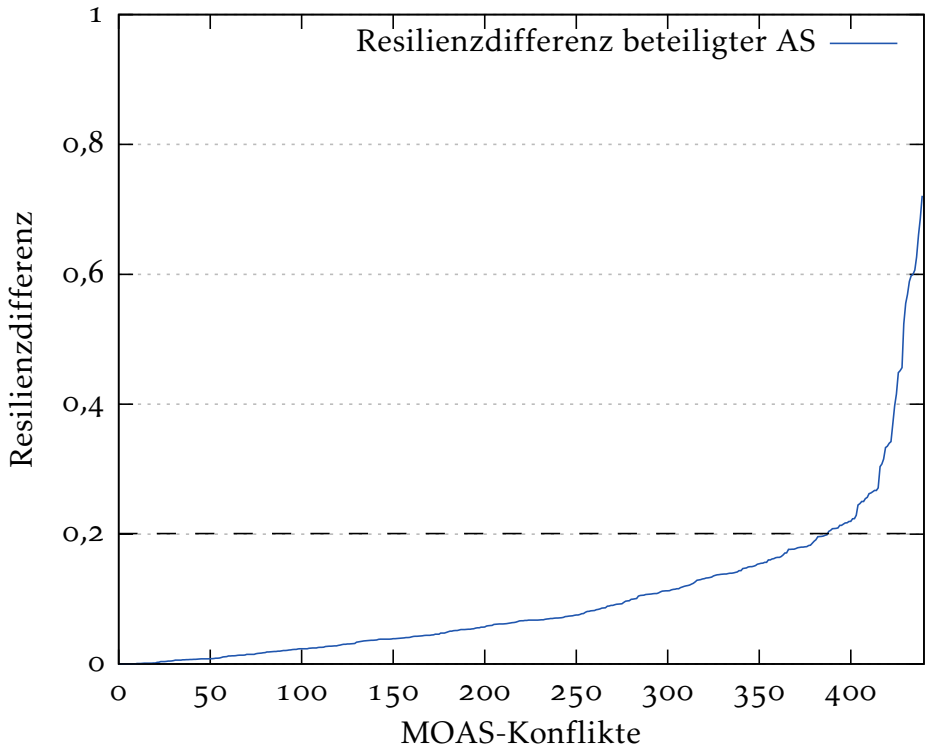

Abbildung 13: *Resilienzunterschiede in MOAS-Konflikten konkurrierender AS*

kator für Prefix-Hijacking-Vorfälle sein. Die resultierenden Partitionen wären in der Größe recht unterschiedlich, so dass keine gleichmäßige Verteilung von Anfragen möglich wäre.

Die meisten MOAS-Konflikte finden nur zwischen zwei AS statt. Lediglich 264 (entspr. 3,67%) der in den Daten enthaltenen MOAS-Konflikte haben mehr als 3 beteiligte AS. Auch wenn das keine große Anzahl ist, sei an dieser Stelle erwähnt, dass sich durch die angepasste β-Funktion der verbesserten Formel diese, im Gegensatz zu der von Lad et al. vorgeschlagenen Formel, auch zur Berechnung von MOAS-Konflikten mit mehr als 2 AS verwenden lässt. Diese Möglichkeit wird durch die angepasste β-Funktion realisiert. Insgesamt erhöht dies jedoch die Komplexität der Resilienz-Berechnung deutlich, da alle Paare bzw. Tupel möglicher Angreifer berücksichtigt werden müssen.

6.3.2 AS Resilienz

Die durchschnittliche Resilienz der unterschiedlichen Ebenen, berechnet mit der verbesserten Formel, wird in Abbildung 14 gezeigt. Daraus geht hervor, dass die Resilienz im Durchschnitt höher ist, je weiter man in der Topologie aufsteigt. Ein Grund dafür ist die Länge der Pfade an den unteren AS, je weiter ein AS vom Kern des Internets entfernt ist, umso längere Pfade entstehen zwischen diesem AS und den meisten übrigen AS. Die maximale Länge eines Pfads von einem AS zum anderen ist also auch abhängig von der eigenen Position. Bei einer maximalen Anzahl von 5 Ebenen im Internet, erreichen AS der Ebene 0 alle anderen AS mit max. sechs Hops (einem Hop auf der Ebene 0 zuzüglich der Hops bis zu Ebene 5). Von Ebene 5 zu einem anderen Ebene 5 AS in einem anderen Teilbaum müssen elf Hops besucht werden (5 Hops bis zur Ebene 0, ein Hop zum nächsten Ebene-0-AS und dann wieder 5 Hops bis zum Ziel-AS). Somit werden auch die kürzesten Pfade von und zu den weiter unten gelegenen AS immer länger, was einen schlechteren Wahrscheinlichkeitswert der β-Funktion zur Folge hat. Je weiter ein AS also vom Kern des Internets entfernt ist, umso schlechter kann es sich gegen Prefix-Hijacking-Angriffe höherer Ebenen behaupten.

Um nun die Formel von Lad et al. und die verbesserte Formel zu vergleichen, wurde die Resilienz aller AS im Internet auf Basis der zuvor gewählten 100

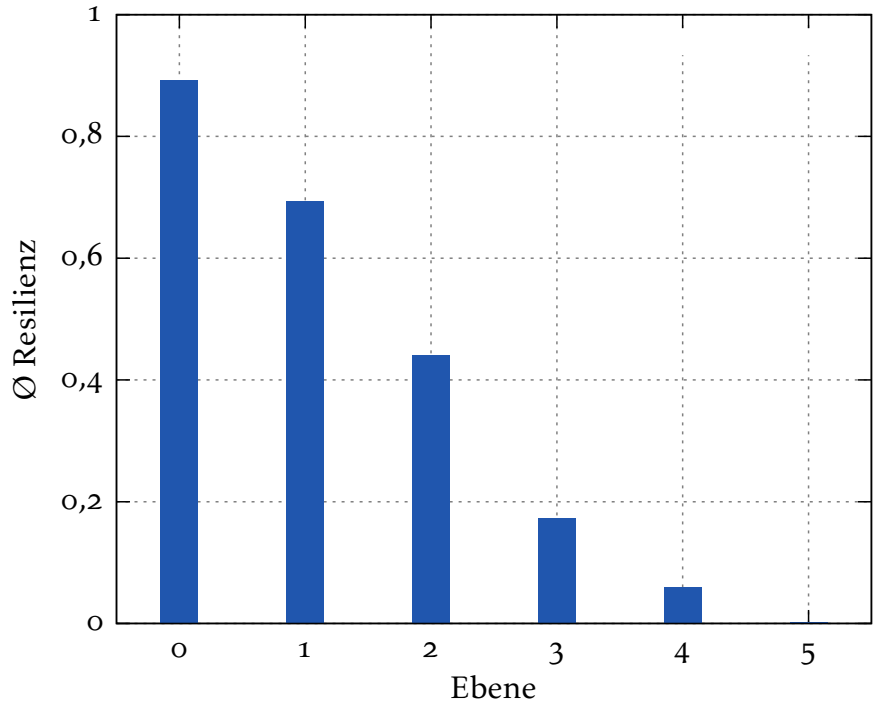

Abbildung 14: *Durchschnittliche Resilienz der Topologieebenen*

Angreifer untersucht. Abbildung 15 zeigt, dass die Werte der Formel von Lad et al. zum Teil deutlich von den Ergebnissen der verbesserten Formel abweichen, wenngleich sie in den meisten Fällen recht nah an die Werte der verbesserten Formel herankommt.

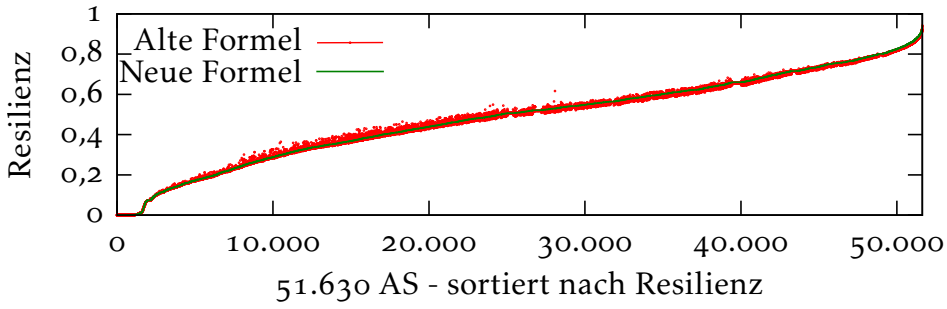

Abbildung 15: *Resilienzwerte der ursprünglichen und der verbesserten Formel*

Dabei fällt auf, dass die Abweichungen im unteren Bereich der Resilienz eher nach oben abweichen und im oberen Bereich der Resilienz eher nach unten. Eine mögliche Erklärung dafür könnte darin liegen, dass AS mit eher geringer

Resilienz in den unteren Ebenen der Topologie zu finden sind. Die Formel von Lad et al. liefert im Hinblick auf die Analyse in Abschnitt 6.2.2 dann niedrigere Ergebnisse, wenn die Pfade kurz sind und wenige gemeinsame Teilpfade existieren. Da die Pfade in den unteren Ebenen wie bereits dargelegt länger sind, steigt auch die Wahrscheinlichkeit der gemeinsamen Teilpfade und damit einer entsprechenden Abweichung nach oben. In den oberen Ebenen gilt entsprechend das Gegenteil, die Formel von Lad et al. berechnet dann entsprechend geringere Resilienz-Werte.

Die Feststellung von Lad et al., dass die größten Resilienz-Werte bei AS in Ebene 1 existieren deckt sich mit den in der Simulation gemachten Ergebnissen. Die Varianz der Resilienz-Werte in Ebene 1 ist aber deutlich größer als in Ebene 0, so dass sich dieser Effekt nicht auch im Vergleich der Ebenen-Durchschnitte aus Abbildung 14 erkennen lässt. Daher lässt sich argumentieren, dass Ebene 0 die Ebene mit der größten (durchschnittlichen) Resilienz ist.

6.3.3 Internetknotenpunkte

Die weitere Vernetzung von AS kann als eine Möglichkeit gesehen werden, kürzere Pfade zu erzeugen und damit die Resilienz gegen Prefix-Hijacking zu verbessern. Daher sollen in diesem Abschnitt diese Peeringmöglichkeiten betrachtet werden und die Resilienz-Werte verglichen werden. IXPs hätten damit ein weiteres Verkaufsargument, wenn sie die Resilienz indirekt beeinflussen können. IXPs erlauben die kostengünstige Verbindung zwischen AS, die bereits einen Anschluss an denselben IXP besitzen. Da die meisten in MOAS-Konflikten involvierten AS in der Ebene 1 liegen und der Durchschnitt trotz größter Absolutwerte für die Resilienz kleiner ist als von der Ebene 0, soll diese Ebene in diesem Abschnitt fokussiert untersucht werden.

Bei Verbindungen von AS unterschiedlicher Ebenen ist zumeist das AS der höheren Ebene ein kostenpflichtiger Upstream-Provider für das AS der niedrigeren Ebene. Um den Effekt von kostengünstigem Peering nicht durch mögliche Kosten für Upstream-Peering abzuschwächen, sollen nur Peerings auf derselben Ebene untersucht werden. Da trotz günstiger finanzieller Kosten der Aufbau einer Peeringbeziehung mit einem gewissen Aufwand verbunden ist, sollen vier unterschiedliche Szenarien verglichen werden. Je nach Szenario unterscheidet

sich die Anzahl der neu etablierten Peerings im Verhältnis zu allen existierenden Möglichkeiten. In den vier Szenarien werden also 1%, 10%, 50% und 100% der existierenden Peeringmöglichkeiten neu etabliert.

Als Peeringmöglichkeit zählen solche AS, die bisher nicht nachvollziehbar miteinander Peering betreiben, aber in denselben IXPs als Mitglieder geführt werden. Die Datenbasis dieser Untersuchung sind die in Kapitel 5 erhaltenen IXP-Mitgliederdatenbanken. Dort gibt es für die 1.960 an europäischen IXPs teilnehmenden AS auf der Ebene 1 insgesamt 978.256 Peeringmöglichkeiten. Alle simulierten neuen Verbindungen sollen als Peer-to-Peer-Verbindung klassifiziert werden. Das bedeutet im Gegenzug für diese Simulation, dass nur die Pfade in tiefere Ebenen verbessert werden, nämlich für die Kunden der entsprechenden neuen Peers. Eine andere Klassifizierung, insbesondere eine als Transit- oder Upstream-Verbindung wird nicht erwogen, da sie in den meisten Fällen weitere Kosten verursachen.

Im Internet entsteht eine gegenseitige Beeinträchtigung der AS, wenn sich Resilienz-Werte verändern. Denn eine höhere Resilienz eines AS hat zwangsweise eine Absenkung der Resilienz anderer AS zur Folge. Dies lässt sich an der Anzahl der AS verdeutlichen, die im Falle eines MOAS-Konflikts Daten für ein Prefix zum True Origin versenden. Je größer die Resilienz des True Origin ist, umso mehr AS senden ihre Daten zum richtigen Ziel. Umso kleiner wird also der Impact eines False Origin als Angreifer. Da Resilienz und Impact gleichgroß sind, ändert sich also auch die Resilienz eines Angreifers mit.

Um die Veränderungen zu beobachten soll also für jedes AS auch direkt ein Prefix-Hijacking-Szenario mit simuliert werden. Die Simulation basiert also auf den 1.960 gefundenen AS, die in europäischen IXPs als Mitglieder gelistet werden und in Ebene 1 der Topologie liegen. Da manche AS bereits untereinander Verbindungen unterhalten weichen die Zahlen in den folgenden Simulationen immer ein wenig von dieser Gesamtmenge ab. Die Anzahl der tatsächlich veränderten AS lässt sich aber jeweils ermitteln. Zufällig werden nun für jedes dieser AS 1%, 10%, 50% und 100% der tatsächlichen Peeringmöglichkeiten in IXPs herausgesucht und die neuen Verbindungen simuliert. Anschließend wird die Resilienz erneut berechnet und mit der vorherigen Resilienz verglichen.

Bei 1% zufällig gewählten zusätzlichen Peerings werden insgesamt 9.591 zusätzliche Verbindungen erstellt. Insgesamt haben 30 AS anschließend eine höhere Resilienz (im Durchschnitt 0,1786%) und 1.373 AS hatten anschließend eine geringere Resilienz (im Durchschnitt ebenfalls 0,1786%), wie in Abbildung 16 dargestellt. Dabei hatte AS 41883 mit 0,354% den höchsten Zugewinn an

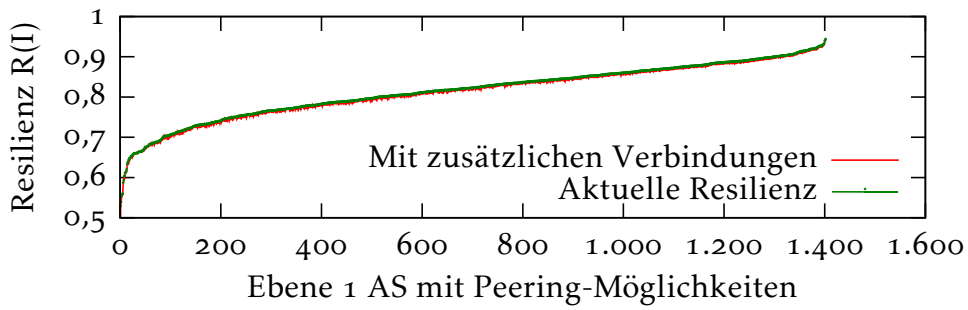

Abbildung 16: *Resilienz-Werte von AS auf Ebene 1 nach dem Hinzufügen von zusätzlich 1% der möglichen Verbindungen*

Resilienz. Zum Zeitpunkt der Simulation hatte AS 41883 lediglich zwei Verbindungen zu anderen AS, von denen keins ebenfalls auf Ebene 1 liegt. Vielmehr gibt es eine Verbindung zu einem AS auf Ebene 0, vermutlich dem Upstream-Provider und eine Verbindung zu einem AS auf Ebene 2. Den größten Verlust an Resilienz mit 1% zusätzlicher Peeringverbindungen hat AS 20672 erfahren. Der Wert sank um 1,5195% von 0,7040 auf 0,6933.

Bei der Simulation mit zusätzlich 10% der möglichen Verbindungen, werden insgesamt 97.883 zusätzliche Verbindungen zwischen 1.508 AS simuliert. Die Veränderung der Resilienz diese AS zeigt Abbildung 17. Insgesamt verzeichne-

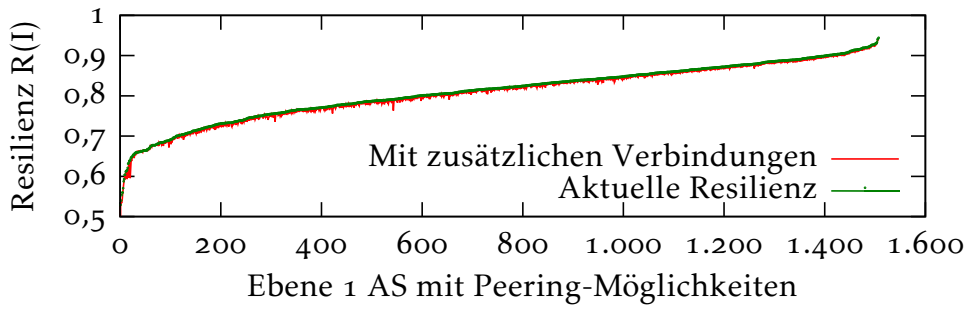

Abbildung 17: *Resilienz-Werte von AS auf Ebene 1 nach dem Hinzufügen von zusätzlich 10% der möglichen Verbindungen*

ten 44 AS eine Vergrößerung der Resilienz um durchschnittlich 0,21%. 1.464

AS hatten im Gegensatz dazu eine um durchschnittlich 0,4825% geringere Resilienz. Dabei hatte wieder AS 41883 den größten Zugewinn, der mit 0,46% bei 19 zusätzlichen Peeringverbindungen höher war als im ersten Versuch. Den größten Verlust an Resilienz hatte AS 59865. Der Wert sank bei 109 zusätzlichen Verbindungen um 6,8797% von 0,6395 auf 0,5954.

Im dritten Versuch werden 50% der Peeringmöglichkeiten gewählt. Es werden für 1.510 AS insgesamt 489.005 zusätzliche Verbindungen simuliert. Abbildung 18 zeigt die Veränderung der Resilienz-Werte für die beteiligten AS. 55 der

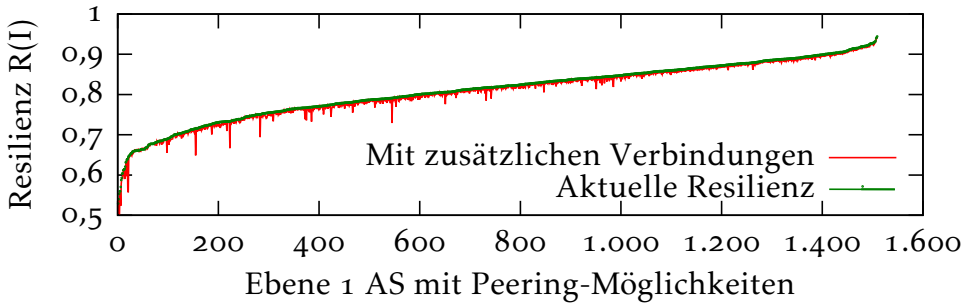

Abbildung 18: *Resilienz-Werte von AS auf Ebene 1 nach dem Hinzufügen von 50% der möglichen Verbindungen*

AS erzielten einen höheren Resilienz-Wert (durchschnittlich 0,23%), während 1.455 AS eine um durchschnittlich 0,61% geringere Resilienz hatten. Wieder ist AS 41883 mit diesmal 0,56% das AS mit dem größten Zugewinn bei insgesamt 53 zusätzlichen Verbindungen zu anderen AS. Den größten Verlust an Resilienz hat in diesem Versuch AS 1200. Die Resilienz sank um 14,07% von 0,5533 auf 0,4751.

Im vierten Versuch werden in der Simulation alle möglichen Verbindungen zwischen den AS etabliert. Abbildung 19 zeigt den Unterschied der Resilienz-Werte für die betrachteten AS. Wieder ist AS 41883 das AS mit dem höchsten Zugewinn (0,58% bei 71 zusätzlichen Verbindungen) von insgesamt 56 AS. Wie im dritten Versuch lag der Zugewinn bei durchschnittlich 0,23%. 1.454 AS hatten eine im Durchschnitt um 0,6715% geringere Resilienz als vorher. Den größten Verlust an Resilienz hatte wieder AS 1200. Diesmal sank der Wert bei 875 zusätzlichen Verbindungen um 31,5% von 0,5533 auf 0,3783.

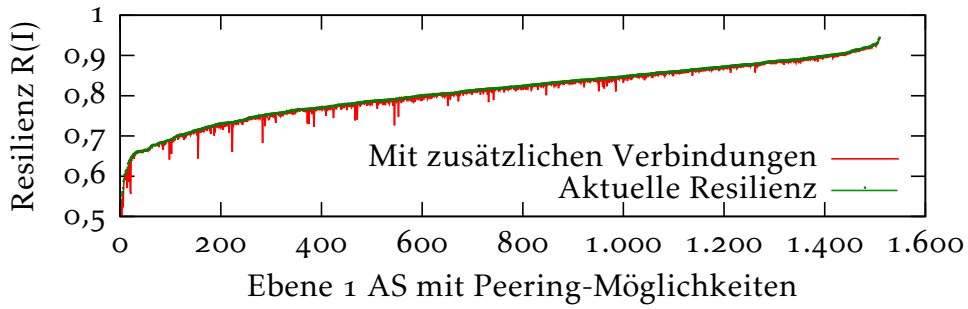

Abbildung 19: *Resilienz-Werte von AS auf Ebene 1 nach dem Hinzufügen aller möglichen Verbindungen*

6.4 Fazit

In diesem Kapitel wurde die Ungenauigkeit in der bisher verwendeten Formel zur Berechnung der Prefix-Hijacking-Resilienz von AS demonstriert und in einer neuen Formel optimiert. Anschließend wurde die verbesserte Formel verwendet, um den Effekt zusätzlicher Peerings auf die Prefix-Hijacking-Resilienz zu untersuchen. Ein positiver Effekt zusätzlicher Verbindungen wäre vor allem für IXPs ein Verkaufsargument. Allein durch das Peering mit AS auf derselben Ebene konnte nur in manchen Fällen eine tatsächliche Erhöhung der Resilienz gezeigt werden. In den anderen Fällen hatten zusätzliche Peerings einen gegenteiligen Effekt. Im Gegensatz zu reinen Verbindungen auf derselben Ebene, wäre eine Betrachtung von Transit-AS oder Upstream-AS Peeringmöglichkeiten sinnvoll, zumindest dann, wenn ein Prefix-Hijacking akut im Gange ist. Allerdings sind dabei, trotz der Präsenz beim gleichen IXP, finanzielle Aspekte für die Weiterleitung des Datenverkehrs im Vordergrund. Das Ziel des Betreibers eines AS ist ja in den meisten Fällen vordergründig, möglichst viele Daten in kurzer Zeit zu routen und diesen Dienst entsprechend den Kunden anzubieten. Allein um präventiv die Resilienz gegen ein zukünftiges Prefix-Hijacking zu erhöhen, wird kein Unternehmen die höheren Kosten eines zusätzlichen Upstreams auf sich nehmen. Als reaktive Maßnahme könnte ein solches Peering mit einem gezielt ausgesuchten Partner jedoch einen Vorteil für die Erreichbarkeit des betroffenen Prefix bringen. Diese Tatsache wird in dem folgenden Kapitel 7 ausführlich dargestellt.

7 Mitigation: Partitionen erweitern[9]

Zusammenfassung des Kapitels Das Border-Gateway-Protokoll als de-facto Standard beim Austausch von Erreichbarkeitsinformationen sieht keine Authentifikation von Autonomen Systemen vor. Daher ist Prefix-Hijacking eine große Bedrohung beim Internetrouting. Gegenmaßnahmen, wie etwa die RPKI Protokollerweiterung, sind bisher nicht in dem Maße im Einsatz, dass ein effektiver Schutz des gesamten Internetroutings damit möglich ist. Es ist auch nicht absehbar, dass diese Gegenmaßnahmen flächendeckend zum Einsatz kommen. Opfer eines Prefix-Hijacking zu sein ist für die Betreiber eines AS eine problematische Situation mit nur wenigen Handlungsoptionen. Dabei sind nicht nur die legitimen Besitzer eines Prefix als Opfer zu betrachten. Auch alle AS, die den Erreichbarkeitsinformationen des Angreifers glauben und ihre Pakete entsprechend weiterleiten, müssen als Opfer berücksichtigt werden. Letztere haben nämlich keine Möglichkeit mehr, mit dem legitimen Besitzer zu kommunizieren und gegebenenfalls vertrauliche Datenpakete erreichen den falschen Empfänger. Aktuelle Erreichbarkeitsinformationen der Internet Control-Plane, wie diese vom RIPE RIS gesammelt und zur Verfügung gestellt werden, eignen sich grundsätzlich für die Erkennung von Prefix-Hijacking. Durch Prefix-Hijacking entstehen unterschiedliche Partitionen von AS, solche, die Daten-

[9] Die Inhalte basieren auf M. Wübbeling und M. Meier. „Reclaim Your Prefix: Mitigation of Prefix Hijacking Using IPsec Tunnels“. In: *2017 IEEE 42nd Conference on Local Computer Networks (LCN)*. 2017, S. 330–338

pakete zum True Origin weiterleiten und solche, die Datenpakete zum False Origin weiterleiten. Diese Partitionen können näherungsweise ermittelt und analysiert werden. Eine exakte Ermittlung ist aufgrund der verfügbaren Daten nicht möglich (vgl. Kapitel 4). In diesem Kapitel werden Verfahren vorgeschlagen, um die resultierenden Partitionen mit den Bordmitteln eingesetzter Internetrouter zugunsten der Opfer zu verändern. Aus diesen Verfahren abgeleitete Maßnahmen ermöglichen legitimen Besitzern mit Hilfe eines Partners die Ihnen zugeordnete Partition, und damit ihren Einfluss, zu vergrößern. Dabei werden unterschiedliche Auswahlstrategien für Partner miteinander verglichen. Die drei am besten geeigneten Verfahren werden dann in einer emulierten Umgebung evaluiert. Diese Evaluation wird auf einem kleinen Netzwerk durchgeführt, das sich dem Internet im Hinblick auf Prefix-Hijacking ähnlich verhält. Der vorgeschlagene Ansatz eignet sich als Grundlage für ein (teil-)automatisiertes Werkzeug, um zukünftig Prefix-Hijacking zu begegnen.

Fehlende Authentifikation des im Internet eingesetzten Routingprotokolls BGP impliziert ein gegenseitiges Vertrauen aller AS untereinander hinsichtlich der ausgetauschten Erreichbarkeitsinformationen. Während dieses Vertrauen in den frühen Tagen des Internets nur eine Handvoll AS betraf, sind zum Zeitpunkt der Untersuchung laut den Daten der Routingarchive etwa 57.000 AS im Internet verbunden (Stand 2017). Dieses gegenseitige Vertrauen ist Ursache für die Anfälligkeit für Prefix-Hijacking, also die illegitime Verwendung des Prefix eines anderen AS, aller AS im Internet.

Prefix-Hijacking hat auch außerhalb der akademischen Welt in den letzten Jahren immer wieder große Aufmerksamkeit erfahren. Im Fokus stehen dabei Gerüchte über Geheimdienste oder andere staatliche Akteure, die Prefix-Hijacking für gezielte Spionage oder Zensur einsetzen [97]. Auch gewöhnliche Unternehmen nutzten in der Vergangenheit Prefix-Hijacking für (kriminelle) Aktivitäten. Dabei zeigen Veröffentlichungen interner Daten des italienischen Unternehmens „Hacking Team“, dass auch kleine periphere AS im Auftrag kleiner Unternehmen die Möglichkeiten haben, dass Internetrouting gezielt zu manipulieren und für ihre Zwecke zu missbrauchen [138].

Aufgrund der bekannten Bedrohung durch Prefix-Hijacking gibt es unterschiedliche Ansätze zur Erkennung und Klassifikation von Routinganomalien, die auch Prefix-Hijacking berücksichtigen. Viele Ansätze gehen dabei aber über eine Erkennung von Prefix-Hijacking nicht hinaus. Daher gibt es nur wenige Ansätze, die als Gegenmaßnahmen untersucht wurden, von denen jedoch keine flächendeckend eingesetzt wird (vgl. Kapitel 3).

Ein Grund dafür kann sein, dass die Maßnahmen immer nur in Simulationen unter Laborbedingungen evaluiert wurden. Die in diesem Kapitel vorgestellten Arbeiten versuchen diese Lücke zwischen Simulation und Realität zu verringern. Die drei maßgeblichen Beiträge dieses Kapitels sind:

1. Ein Ansatz als Gegenmaßnahme zu Prefix-Hijacking durch dynamischen Aufbau zusätzlicher Routingpfade mit Hilfe von IPSec-Tunneln zwischen dem legitimen AS und einem kooperierenden Partner-AS. Die zusätzlichen Pfade werden genutzt, um valide Erreichbarkeitsinformationen gezielt in Richtung solcher AS zu bringen, die für die Weiterleitung gefälschte Informationen eines Angreifers verwenden. So soll der Effekt des Angriffs abgeschwächt werden.
2. Durch Simulation werden die Auswirkungen von Prefix-Hijacking ermittelt und unterschiedliche Auswahlstrategien für Partner-AS evaluiert.
3. Die zusätzliche Verwendung einer Emulationsumgebung erlaubt einen Einblick in den tatsächlichen Prozess zur Routenauswahl von Internetroutern und zeigt Unterschiede zu simulierten Umgebungen auf. So wird die Lücke zwischen Simulation und Realität verringert.

7.1 Verwandte Arbeiten

Prefix-Hijacking als Folge fehlender Sicherheitsmechanismen in BGP ist ein in der Literatur bekanntes Problem. Die meisten Arbeiten betrachten dabei die Erkennung und Klassifikation von Prefix-Hijacking auf Basis der gesammelten und öffentlich verfügbaren Erreichbarkeitsinformationen von Routingarchiven. Solche Arbeiten sind bereits in den vorigen Kapiteln vorgestellt worden. Daher sollen an dieser Stelle nur gezielte reaktive Gegenmaßnahmen gegen Prefix-Hijacking vorgestellt werden.

7.1.1 Prefix-Hijacking-Mitigation

Prefix-Hijacking lässt sich als Spezialfall von MOAS betrachten [151] (vgl. Abschnitt 3.2). Dabei haben Zhao et al. neben der detaillierten Analyse von MOAS eine Möglichkeit zur Filterung illegitimer Erreichbarkeitsinformationen als Gegenmaßnahme zu Prefix-Hijacking vorgeschlagen [152]. Dieser Vorschlag sieht vor, dass ein legitimer Prefixbesitzer in seinen Announcements alle weiteren AS mit angibt, die als mögliche weitere Origins dieses Prefixes vorgesehen sind. Zhao et al. nennen dies eine MOAS-Liste, die sie über das BGP-*Community*-Attribut realisieren. So wäre es allen Routern möglich, die erhaltenen Erreichbarkeitsinformationen aller Origins auf Konformität prüfen. Diese Informationen sind dann aber, ähnlich wie die Erreichbarkeitsinformationen selbst, für den Empfänger nicht validierbar. Ebenso ist es möglich, dass diese Informationen durch nicht kompatible Router einfach entfernt werden. Ein Angreifer könnte selbst durch einfaches Hinzufügen seiner eigenen AS-Nummer diese Liste erweitern. Zhao et al. betrachten diesen Fall explizit in ihrer Arbeit und argumentieren damit, dass ein empfangendes AS mit dieser MOAS-Liste zwar nicht herausfinden kann, wer legitimer Besitzer des Prefix ist, aber es zumindest offensichtlich ist, dass es ein Problem mit diesem Prefix gibt. Daher handelt es sich bei diesem Ansatz im Grunde auch nicht um eine effektive Mitigation sondern eher um ein weiteres Mittel zur Erkennung von Prefix-Hijacking innerhalb eines Routers.

Die von Zhang et al. vorgeschlagene Gegenmaßnahme [149] ist dabei dem hier vorgestellten Ansatz am nächsten. Zhang et al. fokussieren dabei ihre Gegenmaßnahme auf den Einsatz von Routingpolicies und gezielter AS-Pfadmanipulation. Diese Maßnahmen müssen dabei von sogenannten „Lifesaver"- bzw. „Promoter"-AS durchgeführt werden, die selbst nicht von diesem Prefix-Hijacking betroffen sind. Somit ist die Auswahl der Kooperationspartner etwas eingeschränkt. Die Ergebnisse von Zhao et al. sind dabei vergleichbar mit der in dieser Arbeit untersuchten Auswahlstrategie „Nähe zum Grenzbereich" (vgl. Abschnitt 7.3.1), mit leicht besseren Ergebnissen durch die Berücksichtigung von Routingpolicies.

7.2 Veränderung resultierender Partitionen

Das Hauptziel der Arbeiten in diesem Kapitel ist die Veränderung der Partitionen, die durch Prefix-Hijacking entstehen. In der hier durchgeführten Betrachtung soll dabei die Veränderung durch den legitimen Prefixbesitzer angestoßen werden, nachdem dieser ein Prefix-Hijacking eines seiner Prefixe erkannt hat. Der legitime AS-Besitzer kann als einziger eindeutig zwischen legitimem MOAS, wie für Load-Balancing verwendet, und Prefix-Hijacking unterscheiden. Grundsätzlich können aber beliebige AS diese Veränderung stellvertretend für den Prefixbesitzer durchführen und dabei vergleichbare Resultate erzielen. Das bedeutet also, dass auch ein AS, das als Kommunikationspartner des True Origin in der Partition des False Origin liegt von sich aus diese Veränderung anstoßen kann, um für sich selbst wieder eine Kommunikation zu ermöglichen. Die zugrundeliegende Idee dieser Gegenmaßnahme ist die Verbreitung kürzerer Pfade zum True Origin. Diese kürzeren Pfade sollen dann innerhalb der Partition des False Origin die Auswahlprozesse der anderen AS entsprechend beeinflussen.

Obwohl Routingpolicies ein wichtiges Instrument beim Internetrouting sind, sollen sie im Rahmen dieser Arbeiten nicht berücksichtigt werden. Zwar können AS ihre Policies freiwillig in sogenannte Internet-Routing-Registrierungsstellen (IRR) eintragen [67], da die Policies zumeist als Geschäftsgeheimnis eines AS angesehen werden, verzichten viele AS jedoch darauf. Weitere öffentlich verfügbare Quellen für Routingpolicies sind die Topologieinformationen des Internet Research Labs (IRL) [66] und des Center for Applied Internet Data Analysis (CAIDA) [25]. Aus den Provider-Customer- und Peer-to-Peer-Beziehungen lassen sich grundlegende Routingpolicies für die Weitergabe von Erreichbarkeitsinformationen ableiten (vgl. Abschnitt 2.2.4) [89]. Es gibt zwar Versuche, darüber hinausgehend verwendete Routingpolicies, etwa über die Erreichbarkeitsinformationen von Routingarchiven, zu ermitteln, diese führen aber nicht zu zuverlässigen Routingpolicies [141].

7.2.1 Hypothese

Die Kern-Hypothese zu dieser Untersuchung ist, dass Partitionen, die durch Prefix-Hijacking verursacht werden, in der Form manipuliert werden können, dass die Partition des True Origin erweitert wird.

Um diese Erweiterung der Partition zu bewirken, müssen AS in der Partition des False Origin davon überzeugt werden, für den betroffenen Prefix eine andere Route zu verwenden. Da wir Routingpolicies dabei nicht berücksichtigen, ist für den Prozess der Routenauswahl die Länge des AS-Pfads maßgeblich. Um eine Erweiterung der Partition des True Origin zu bewirken, müssen also die Pfade in Richtung des True Origin kürzer werden als die Pfade in Richtung des False Origin. Der Erfolg dieses Ansatzes folgt unmittelbar aus der Dynamik des BGP-Protokolls.

Das vorgeschlagene Verfahren kann dabei durch beliebige AS umgesetzt werden, vorzugsweise dem True Origin und einem speziell gewählten kooperierenden AS. Die Wahl der kooperierenden AS ist für den Erfolg, also dass eine möglichst große Veränderung der Partitionen erreicht wird, maßgeblich. Dabei hängt das Ausmaß der Veränderung maßgeblich von der topologischen Position des kooperierenden AS ab. Ein AS mit größerem Impact (vgl. Kapitel 6), einer niedrigeren topologischen Ebene des AS oder einem höheren Knotengrad wäre damit besser als ein peripheres AS am topologischen Randbereich ohne viele Verbindungsmöglichkeiten als Kooperationspartner geeignet. Durch die resultierenden kürzeren Pfade innerhalb der Partition des False Origin werden die Pakete umliegender AS wieder umgeleitet in Richtung des True Origin.

Während dieser Ansatz so ohne Anpassungen in Simulationsumgebungen berechnet werden kann, lässt er sich nicht ohne weiteres in Emulationen oder realistischen Szenarios umsetzen. Das liegt an unterschiedlichen Parametern bei der Implementierung von Routerhardware, etwa speziellen Routingdynamiken wie der Implementierung der „route flapping protection“ von CISCO-Routern. Eine detaillierte Darstellung dieses Problems folgt in den nächsten Abschnitten.

7.2.2 Veränderung der Partitionen

Zwischen dem True Origin und dem Kooperationspartner gibt es zwei unterschiedliche Ansätze zur Kooperation:

BGP über IPSec-Tunnel

True Origin und der Kooperationspartner errichten einen IPSec-Tunnel zwischen zwei Border-Routern der jeweiligen AS. Diese virtuelle direkte Verbindung wird dann genutzt, um darüber eine BGP-Verbindung zwischen den beiden AS zu etablieren. Im Vergleich zu den bisherigen Routen sind die resultierenden Routen höchstens genau so lang, wie zuvor, bestenfalls kürzer.

Satz 7.2.1. *AS-Pfade von Announcements, die über eine getunnelte BGP-Verbindung zweier Autonomer Systeme weitergeleitet werden sind maximal so lang wie die AS-Pfade der Announcements, die auf dem üblichen Pfad ohne Tunnel weitergeleitet werden.*

Beweis von Satz 7.2.1. Hier sei

x das AS welches True Origin für ein Prefix ist und

y das AS welches Kooperationspartner von x ist.

Nach Konstruktion sind x und y direkte Nachbarn. Die Entfernung $e(x,y)$ in Hops zwischen den AS beträgt damit 1, die Länge des AS-Pfads $p = (x,y)$ der Erreichbarkeitsinformationen von x weitergeleitet durch y beträgt damit $|p| = e(x,y) + 1 = 2$ (nur die beiden AS in der Reihenfolge: y, x)

Ein Tunnel zwischen x und y ermöglicht eine virtuelle direkte Verbindung zwischen x und y, so dass die Erreichbarkeitsinformationen AS-Pfade enthalten, die einer direkten Verbindung entsprechen $|p_{\text{virtuell}}| = |p|$ für $e(x,y) = 1$. Nachbarn von y, die diese Pfade erhalten, erhalten so Pfade, die maximal so lang sind, wie der direkte AS-Pfad zu x über y.

Induktionsanfang über die Entfernung $e(x,y) = n$ für $n = 1$:

Zwischen x und y liegen keine weiteren AS, die kürzere Wege haben können. Alle Nachbarn von y erhalten die Erreichbarkeitsinformationen von x mit einem Pfad p mit $|p| = e(x,y) + 1 \geq |p_{\text{virtuell}}| = 2$.

Induktionsbehauptung: $e(x,y) = n \geq 2 \implies e(x,y) = n + 1 \geq 2$.

Induktionsschritt: Aus $|p| = e(x,y) + 1 \geq 2$, folgt unmittelbar, dass $|p| = n + 2 \geq 2$ für alle $n \in \mathbb{N}$.

□

Daraus ergibt sich auch, dass ein AS z, welches auf dem Pfad zwischen x und y liegt genau dann den Pfad über y zu x wählt, wenn die Entfernung $e(x,z) > e(y,z)$ ist.

Die AS im direkten Umfeld des Kooperationspartners erhalten also Erreichbarkeitsinformationen mit einem kürzeren Pfad als vorher und können so den Pfad über die virtuelle Verbindung zum True Origin nutzen. Um den Datenverkehr auf die notwendige Größe zu begrenzen, können die weitergeleiteten Prefixe des True Origin auf den von Prefix-Hijacking betroffenen Prefix eingeschränkt werden. Da die Nutzdaten des IPSec-Tunnels den üblichen Pfad vom Kooperationspartner zum True Origin weitergeleitet werden, beschränkt sich der Overhead für den Kooperationspartner auf die AS im direkten Umfeld, deren Datenpakete sonst über andere Pfade zum True Origin weitergeleitet werden.

Dieser Ansatz hat folgende Einschränkungen. Um BGP über einen solchen Tunnel zu leiten, müssen einige statische Routingeinstellungen vorgenommen werden. Mindestens die IPSec-Verbindung inkl. Nutzdaten muss auf dem üblichen Weg vom Kooperationspartner zum True Origin geleitet werden, ansonsten ist ein Tunnel-Aufbau nicht möglich. Wenn die Tunnel-Endpunkte des True Origin selbst nicht vom Prefix-Hijacking betroffen sind und die Routen über den IPSec-Tunnel gefiltert werden, ist das jedoch kein Problem. Getestet wurde diese Setup mit Routern der Firma CISCO. Der Test war jedoch nicht erfolgreich, da dort die Firmware die notwendigen Änderungen verhindert, um den Administrator vor einem zerbrechlichen Routingaufbau zu bewahren. Eine mögliche Alternative dazu sind OpenSource-Software-Router, wenngleich diese bei viel

Datenverkehr schnell zu einem Flaschenhals werden können. Da es sich bei den Einschränkungen um praktische Einschränkungen der verwendeten Hardware handelt, für die es entsprechende Workarounds gibt, soll dieser Ansatz im Rahmen der Simulation trotzdem betrachtet werden. Dort spielen diese Einschränkungen keine Rolle.

Erweitertes Prefix-Hijacking

Um den Pfad noch weiter zu verkürzen, und so die Partition des True Origin noch weiter zu vergrößern, ist es für das kooperierende AS möglich, den betroffenen Prefix selbst als Origin anzubieten. Dies erweitert das Prefix-Hijacking und erzeugt eine weitere Partition mit AS, die ihre Datenpakete zum Kooperationspartner routen. Dieser muss die Datenpakete, die dann zu ihm gelangen, dann nur auf dem richtigen Weg weiter zum True Origin senden. Für die Nachbarn des Kooperationspartners ist es dabei nicht möglich ist, diese Pakete an den True Origin weiterzuleiten, da diese ja alle die kürzere Route direkt zum Kooperationspartner erhalten haben. Es bietet sich also auch in diesem Fall ein IPSec-Tunnel zwischen True Origin und kooperierendem AS an, über den die Pakete dann weitergeleitet werden. Auch in diesem Fall müssen wieder statische Anpassungen am Routing vorgenommen werden, um den Tunnel aufbauen zu können.

Zusätzlich muss in diesem Fall eine IP-Adresse des betroffenen Prefix für die Konfiguration des Routers verwendet werden. Hier bietet sich an, einem Loopback-Adapter diese IP-Adresse zuzuweisen und so das Prefix zu beanspruchen. Um nun die Pakete durch den Tunnel zum True Origin weiterzuleiten genügt es nicht, einfach für den betroffenen Prefix entsprechende Routen zu setzen. Das liegt daran dass statische Routen eine administrative Distanz von 1 haben, während diese bei Netzwerk-Adaptern, wie dem Loopback-Adapter eine administrative Distanz von 0 haben. Um den Router trotzdem dazu zu bringen, die Pakete zielgerichtet weiterzuleiten, muss das Routing ausgetrickst werden. Um dies zu erreichen, konfiguriert der Administrator zwei statische Routen für die nächstkleineren Subnetze des betroffenen Prefix. Diese statischen Routen werden mit zwei weiteren statischen Routen ergänzt, einer statischen Route für die Broadcast-Adresse des ersten Subnetzes und die Netzadresse des zweiten Subnetzes, so können diese weiterhin erhalten bleiben.

Analog zum ersten Ansatz werden Antwortpakete nicht über den Tunnel gesendet, sondern können über das normale Routing zugestellt werden. Im Vergleich zum ersten Ansatz läuft dieser auf den gängiger Routerhardware und hat noch einen weiteren Vorteil darin, dass der AS-Pfad noch ein Hop kürzer ist. Rechnet man die Partition des Kooperationspartners dazu, führt dies zu einer größeren Partition des True Origin als im ersten Ansatz. Die einzige kleine Einschränkung dieses Ansatzes ist die eine verlorene IP-Adresse des betroffenen Prefix für den Loopback-Adapter.

Vergleich

Beide Ansätze eignen sich generell dazu, die Partition des True Origin mit Hilfe eines kooperierenden AS zu vergrößern. Während der erste Ansatz weniger Auswirkungen auf die Control-Plane des Internetroutings bewirkt, hat der zweite Ansatz weniger Einschränkungen in der praktischen Umsetzung, was insbesondere den Einsatz auf gängiger Routerhardware ermöglicht. Die zusätzliche Partition durch das kooperierende AS wird bei den folgenden Durchläufen der Simulation immer der Partition des True Origin zugerechnet. Im ersten Szenario gibt es darüber hinaus die Einschränkung, dass der Kooperationspartner kein direkter Nachbar des True Origin ist, da dann keine Auswirkungen auf den AS-Pfad möglich sind. Die Nähe des Kooperationspartners zum False Origin kann sich im Gegensatz dazu aber positiv auf die resultierende Partition des True Origin auswirken. Grundsätzlich eignen sich alle übrigen AS, außer dem False Origin, als Kooperationspartner des True Origin. Die Auswahlstrategie des Partners wird in einem nachfolgenden Abschnitt diskutiert.

7.2.3 Die Schnittmenge / Grenzpartition

Im Gegensatz zur Realität ist es in der Simulation möglich, dass es neben der Partition des True Origin und der Partition des False Origin noch einen dritten Partitions-Typen gibt. Während AS im Internet immer definitiv eine Route zum Origin eines Prefix auswählen, wie dies im Prozess zur Routenauswahl definiert ist, kann dieses Auswahl-Verhalten nicht zuverlässig simuliert werden. Der Prozess zur Routenauswahl berücksichtigt neben Routingpolicies, der Länge des AS-Pfads auch die IP-Adresse des verbundenen Routers, sogenannte „Multi Exit Discriminator“ (MED), und andere Parameter. Bei MED handelt es sich

um Zahlwerte, die bei mehreren Verbindungen zwischen zwei AS ausgetauscht werden um dem Nachbar-AS zu signalisieren, auf welchem Weg man bevorzugt Datenverkehr entgegennimmt. [139]

In einer Simulationsumgebung können diese Werte zur Routenauswahl nicht sinnvoll ermittelt werden. Daher bilden die AS mit derselben Distanz zu True Origin und zu False Origin die Schnittmenge beider Partitionen. Diese Schnittmenge wird auch als Grenzpartition (engl. border partition) des Prefix-Hijacking bezeichnet. Die Routenauswahl von AS in dieser Grenzpartition wird als Wahrscheinlichkeit betrachtet, basierend auf der Anzahl kürzester Pfade zum jeweiligen Origin. [81, 146]

Im Rahmen der hier durchgeführten Arbeiten soll die Grenzpartition entsprechend betrachtet werden, als eine Menge AS mit undefiniertem Routingverhalten. Es sollen nur solche Informationen verwendet werden, die sich zuverlässig aus der Control-Plane ableiten lassen. Daher werden nur die AS der Partition des True Origin als solche gezählt. Während der Simulation werden nur solche AS als kooperierende AS ausgewählt, die auf der Basis öffentlich nachvollziehbarer Informationen, also etwa der Routingarchive, ausgewählt werden können. Die Größe der Grenzpartition ist dabei jedoch nicht nebensächlich und soll entsprechend dokumentiert werden. Da die Möglichkeit besteht, dass entsprechende AS tatsächlich Pfade in Richtung True Origin wählen, wäre die Veränderung eines AS von der Partition des False Origin in Richtung Grenzpartition bereits eine Verbesserung.

7.2.4 Planung der Simulation

Die Simulation basiert auf Daten aus dem RIPE RIS Routingarchiv (vgl. Abschnitt 7.3.2). Es werden vollständige Routingtabellen aller aktiven Kollektoren verwendet, um ein möglichst vollständiges Bild der Routingsituation zu erhalten (vgl. Kapitel 4). Die für die Simulation entwickelte Software verwendet die Bibliothek *libbgpdump* [120] zum Einlesen der Daten aus den Routingarchiven. Die Routenauswahl und die Weiterleitung von Erreichbarkeitsinformationen basieren dabei auf den Beziehungen zwischen den AS, (vgl. Abschnitt 2.2.4). Die Daten der einzelnen RRCs werden eingelesen und aggregiert. Darauf aufbauend werden die Pfade der Announcements analysiert und auf Basis der

Nachbarschaftsbeziehungen ein Graph erzeugt. Obwohl der erzeugte Graph nicht alle existierenden Verbindungen im Internet darstellt, wird er als repräsentativ für das Internet angenommen.

In den Daten sind ebenfalls alle annoncierten Prefixe enthalten, ebenso wie die jeweiligen Origins der Prefixe. Beim Einlesen der Daten lassen sich so über die Zuordnung von Prefixen zu Origins bereits solche AS finden, die Teil eines MOAS-Konflikts sind. Die Liste der betroffenen Prefixe wird anschließend auf Paare der beteiligten AS reduziert und doppelte Paare werden aussortiert. So werden doppelte Berechnungen von Partitionen vermieden, diese sind nämlich unabhängig von den betroffenen Prefixen, allein die beteiligten AS sind entscheidend.

Die Arbeiten in diesem Kapitel beziehen sich auf die resultierenden Partitionen und Möglichkeiten, diese zu verändern. Da diese Fragestellung auch etwa für Load-Balancing interessant ist, spielt es keine Rolle, ob ein MOAS-Konflikt legitim oder illegitim ist. Daher wird jeder MOAS-Konflikt als Prefix-Hijacking interpretiert. Auch lässt sich auf Basis der Informationen in den Routingarchiven nicht ableiten, welches der beteiligten AS True Origin und welches False Origin ist.

Der nächste Schritt in der Simulation basiert auf der Auswahl eines geeigneten Kooperationspartners. Kriterien zur Auswahl werden in Abschnitt 7.3.1 im Detail vorgestellt. Die resultierenden Partitionen werden zunächst gespeichert und im Anschluss an die Simulation ausgewertet. Um möglichst realistische Aussagen zu treffen, werden die Ergebnisse auf emulierter Routerhardware verifiziert.

7.2.5 Planung der Emulation

Wie dargestellt, können die Ergebnisse von Simulationen zum Teil deutlich von realen Szenarios abweichen. So gibt es etwa in der Realität keine Grenzpartition, da sich Router immer für eine der verfügbaren Routen entscheiden. Um die Auswirkungen der vorgeschlagenen Maßnahmen zur Veränderung von Partitionen zu überprüfen, werden diese in einer Emulationsumgebung etwas näher an der Realität beobachtet.

Als Grundlage für die Emulation dient das Werkzeug „Graphical Network Simulator“ (GNS3) [49]. GNS3 erlaubt die einfache Konfiguration und Verwendung des MIPS-Emulators *Dynamips* [52] sowie die Vernetzung emulierter Geräte. Mit Dynamips können existierende Routerimages, etwa solche von CISCO-Routern mit IOS-Betriebssystem [31], ausgeführt werden. So können unterschiedliche Routingkonfigurationen und Ergebnisse von Entscheidungen auf echten Routern besser nachvollzogen werden. Insgesamt ergibt sich so ein besseres Bild zum Verständnis von Routingsituationen und der Routenauswahl von AS.

Obwohl es möglich ist, GNS3 über mehrere Computer in einem Cluster zu betreiben, konnten aufgrund mangelnder Ressourcen im Rahmen dieser Arbeit nicht alle der zum Zeitpunkt der Durchführung existierenden etwa 57.000 AS emuliert werden. Daher muss für die Emulation ein kleineres Internet erzeugt werden, welches geeignet ist, Prefix-Hijacking zu untersuchen und die Auswahl von Kooperationspartnern unterstützt. Die tatsächlich genutzte Konfiguration wird in Abschnitt 7.3.3 erläutert. Um eine Vergleichbarkeit zwischen den Ergebnissen der Simulation und der Emulation zu ermöglichen, wird die Simulation ebenfalls auf Basis dieses erzeugten Internets durchgeführt. Nach der Simulation wird das Prefix-Hijacking-Szenario mit GNS3 nachgestellt und die vorgeschlagenen Verfahren zur Veränderung resultierender Partitionen werden angewendet. Die resultierenden Partitionen werden dann mit den Partitionen der Simulation verglichen.

7.3 Versuchsdurchführung

Für die Versuchsdurchführung ist es notwendig, zunächst die Strategien zur Auswahl des Kooperationspartners zu definieren. Im Hinblick auf den Auswahlprozess werden drei weitere Hypothesen formuliert:

1. Der Erfolg der Partitionsveränderung hängt ab von den zur Verfügung stehenden Kooperationspartnern und der Auswahl eines Partners mit den folgenden Auswahlstrategien.
2. Ein topologischer Vorteil von Kooperationspartnern macht diese zu besseren Peers im Hinblick auf resultierende Partitionen.

3. Eine topologische Nähe des Kooperationspartners zum Angreifer ist ein Vorteil.

7.3.1 Auswahl des Kooperationspartners

Abhängig von dem individuellen Prefix-Hijacking-Szenario gibt es zwei Gründe für die Motivation, die resultierenden Partitionen zu verändern.

1. Als grundsätzliche Maßnahme zur Mitigation von Prefix-Hijacking und zur Rückgewinnung des eigenen Prefix und zur Verbesserung der eigenen Erreichbarkeit.
2. Zur gezielten Herstellung der Kommunikationsmöglichkeiten mit einzelnen AS in der Partition des False Origin ohne Berücksichtigung weiterer AS.

Während im ersten Fall die Partition des True Origin im Hinblick auf ihre Größe möglichst maximiert werden sollen, ist die Veränderung im zweiten Fall deutlich zielgerichteter und spezifischer.

Die Auswahl des Kooperationspartners ist maßgeblich für die resultierenden Partitionen. Für diese Arbeit wird davon ausgegangen, dass grundsätzlich jedes AS als möglicher Kooperationspartner in Frage kommt. Die Änderungen im Router des AS sind eher simpel und beide AS können die notwendigen Konfigurationsoptionen ohne großen Aufwand umsetzen.

Die Auswahl eines möglichst guten Kooperationspartners basiert auf der Motivation und dem Ausmaß des Prefix-Hijacking. Dabei wird zwischen den folgenden zwei Fällen unterschieden:

- Alle Prefixe des True Origin sind von dem Prefix-Hijacking betroffen.
- Es gibt mindestens ein Prefix des True Origin, das nicht vom Prefix-Hijacking betroffen ist.

Der Unterschied beider Fälle ist, dass im ersten Fall kein Tunnel vom True Origin zu einem AS innerhalb der Partition des False-Origin aufgebaut werden

kann. Daher muss der Kooperationspartner in diesem Fall innerhalb der Partition des True Origin liegen. Im zweiten Fall lässt sich direkt ein Tunnel zwischen dem True Origin und dem Kooperationspartner aufbauen, dafür kann dann ein nicht vom Prefix-Hijacking betroffener Prefix verwendet werden. Wenn wie im zweiten Fall ein beliebiges AS als Kooperationspartner ausgewählt werden kann, lassen sich weitere Auswahlstrategien berücksichtigen. Die folgenden Auswahlstrategien kommen für die Auswahl des Partners in Frage:

Zufällige Auswahl : Der Kooperationspartner wird zufällig aus der Liste der AS in der Partition des False Origin ausgewählt. Diese Auswahlstrategie erscheint zunächst ungewöhnlich, ist aber recht nah an realen Bedingungen, denn eine Kooperation ist hauptsächlich abhängig von bereits existierenden Geschäftsbeziehungen oder Bekanntschaften, die zumindest zum Teil ebenfalls willkürlich sind. Strategische Kooperationen zwischen AS sind in den übrigen Auswahlstrategien berücksichtigt.

Nähe zum Angreifer : Der ausgewählte Kooperationspartner soll sich in unmittelbarer Nähe zum False Origin befinden. Dies scheint auf den ersten Blick eine vielversprechende Position zu sein, um auch frühzeitig die Verbreitung der falschen Erreichbarkeitsinformationen zu unterbinden.

Niedrige topologische Position : Ein Kooperationspartner auf niedriger topologischer Ebene ist näher am Internet-Core. Je niedriger die Ebene eines AS ist, umso größer ist der Teilgraph unter diesem AS. Für Kooperationspartner auf der Topologieebene 0 sind mutmaßlich große Teile der Partition des False Origin unter dem Kooperationspartner aufgehängt. Eine Kooperation soll so zu einer noch größeren Partition des True Origin führen.

Hohe topologische Position : Der Kooperationspartner liegt weiter unten in der Topologie der Partition des False Origin. Auf den ersten Blick scheint dies eine schlechte Entscheidung zu sein, da AS in tieferen Ebenen oft schlechter angebunden sind. Betrachtet man aber die Bevorzugung der Routen von Kunden bei der Routenauswahl könnte diese Auswahl einen guten Kompromiss darstellen.

Optimale Position : AS in Ebene 1 haben zum Teil einen höheren Impact als andere AS (vgl. Kapitel 6). Es kann also vorteilhaft sein, einen Koope-

rationspartner aus der Ebene 1 auszuwählen. Obwohl der Impact von AS auch innerhalb einer Ebene variiert, soll in dieser Untersuchung das erste gefundene AS als Kooperationspartner gewählt werden.

Die meisten Peers : Ein Kooperationspartner mit einem hohen Rang, also einer hohen Anzahl an Peers, scheint nachvollziehbar eine gute Möglichkeit zu sein, möglichst vielen AS kurze Pfade für ein Prefix zu verteilen.

Die wenigsten Peers : Der Kooperationspartner liegt in der Partition des False Origin und wird aus der Menge der AS gewählt, die die wenigsten Peers haben. Diese Strategie verspricht keine großen Erfolge, wird aber als Gegensatz zur vorigen Strategie mit berücksichtigt.

Nähe zum Grenzbereich : Sollten alle Prefixe des True Origin von dem Prefix-Hijacking betroffen sein, muss ein AS gefunden werden, das für einen Tunnel in Frage kommt. Es muss also ein AS sein, dass selbst in der Partition des True Origin ist, aber nah an der Grenze zur Partition des False Origin.

7.3.2 Simulation

Die Simulation wird auf Daten der RIPE RIS Routingarchive durchgeführt. Es werden vollständige Abbilder der Routingtabellen aller RRCs vom 5. März 2017 um 00:00 Uhr verwendet. Dabei können nur die RRCs berücksichtigt werden, die zum Zeitpunkt der Untersuchung aktiv waren, also auch Daten zu diesem Zeitpunkt enthalten. Somit wurden die Daten der RRCs mit den laufenden Nummern $[0-1]$,$[3-7]$,$[10-16]$ für die Simulation verwendet. Da keine Annahme über die Legitimität eines MOAS-Konflikts getroffen werden kann, werden entsprechend alle berücksichtigt. So entsteht eine Übersicht aktueller Prefix-Hijacking-Szenarien im globalen Internetrouting. Diese Werte sind aufgrund der Größe des Internets nicht mit der Emulation prüfbar, sollte sich aber eine generelle Ähnlichkeit von Simulation und Emulation ergeben, sind sie praktisch ebenso relevant.

Um die Auswahlstrategien auch im Hinblick auf die ursprüngliche Größe der Partition zu bewerten, wird die Berechnung zweimal durchgeführt. So können beide AS einmal als True Origin und einmal als False Origin betrachtet werden. Für die Simulation wird mit jeder Auswahlstrategie eines der möglichen AS als

Kooperationspartner ausgewählt. Es wird angenommen, dass es mindestens ein weiteres Prefix des True Origin gibt, welches nicht von Prefix-Hijacking betroffen ist. Nur so ist es möglich, einen Tunnel vom True Origin zu einem beliebigen Kooperationspartner aufzubauen. Dies ist ebenfalls notwendig, um alle Strategien sinnvoll zu testen. Lediglich bei der Strategie „Nähe zum Grenzbereich“ kommt diese Annahme nicht zum Tragen.

Wie zu Beginn des Kapitels beschrieben, können zwei unterschiedliche Methoden zur Erweiterung der Partition des True Origin simuliert werden. Die erste Strategie sieht einen Tunnel zwischen True Origin und ausgewähltem Kooperationspartner vor, der auch eine BGP-Verbindung zwischen beiden AS ermöglicht. So können Erreichbarkeitsinformationen und Daten über den Tunnel ausgetauscht werden. Der Simulationsalgorithmus fügt dafür einfach eine (bisher nicht existierende) Verbindung zwischen den beiden betroffenen AS in den Graphen ein. Dies ist möglich, weil der Tunnel in diesem Fall als direkte Verbindung der beiden AS gesehen werden kann. Die Beziehung dieser neuen Verbindung wird als Customer2Provider angesehen, damit werden zukünftige Announcements auch über diese Verbindung an alle Nachbarn des Kooperationspartners weitergereicht. So erhalten die AS in der Umgebung des Kooperationspartners in der Partition des False Origin kürzere Pfade für den betroffenen Prefix des True Origin.

Im zweiten Ansatz soll das Prefix-Hijacking erweitert werden. Der Kooperationspartner wird dann zum dritten Origin des Szenarios. Auch in diesem Szenario gibt es einen Tunnel zwischen den kooperierenden AS, der beliebigen Datenverkehr transportiert. Da dieser keine Relevanz für BGP oder resultierende Partitionen hat, muss er in der Simulation nicht weiter berücksichtigt werden. Für das Ergebnis werden dann die Partitionen der kooperierenden AS zusammengefasst und mit der Partition des False Origin verglichen. Wichtig für die Evaluation ist dabei vordergründig die Anzahl der AS in der Partition des True Origin.

7.3.3 Emulation

Die Motivation, neben der Simulation noch die praktischere Emulation durchzuführen liegt darin, die Ergebnisse der Simulation zur verifizieren und die An-

wendbarkeit der Maßnahmen zu überprüfen. Wie bereits dargestellt, lassen sich in der Simulation auch solche Sachverhalte annehmen und berechnen, die so in der Realität nicht umsetzbar sind. Basierend auf GNS3 werden Prefix-Hijacking-Szenarios konfiguriert und die Gegenmaßnahmen an diesen Konfigurationen getestet. GNS3 simuliert dabei die Verbindungen zwischen verschiedenen Instanzen von Dynamips. Mit diesem Emulator lässt sich die in CISCO-Routern eingebaute Hardware emulieren und so IOS als Betriebssystem ausführen. Aufgrund der Eigenschaften einer Emulation, diese ist immer mit einem recht hohen Verbrauch an Ressourcen verbunden, ist die Anzahl der in diesem Versuch emulierbaren Router begrenzt. Mit einer einfachen BGP-Konfiguration benötigt jeder Router etwa 200 MByte Arbeitsspeicher. Die Auslastung des Prozessors ist praktisch immer eine volle Auslastung durch jeden Emulationsprozess. Dynamips erlaubt daher die Konfiguration sogenannter „Idle-Parameter“, dabei handelt es sich um Code-Stellen des Images, die regelmäßig durchlaufen werden. Dynamips stoppt dann die Ausführung und legt den Prozess für einen kurzen Moment schlafen. So kann die Auslastung deutlich reduziert werden. Ausgehend von optimalen Idle-Parametern lassen sich auf einer CPU mit vier Kernen etwa 100 bis 150 Router emulieren. Bei größeren Konfigurationen mit aktiven Filtern und vielen Prefixen sinkt die Anzahl der möglichen Router entsprechend. Um auch mit wenigen Ressourcen Prefix-Hijacking emulieren zu können, wird das verwendete Netzwerk deutlich verkleinert, allerdings immer nur soweit, wie die Eigenschaften des Netzwerks und des Internets im Hinblick auf Prefix-Hijacking und Partitionen vergleichbar bleiben. Das muss für die Konstruktion des Netzwerks immer berücksichtigt werden.

Um möglichst nah an dem Aufbau des Internets zu bleiben, bilden 4 AS die Clique auf der Ebene 0, also den Internet-Core. Für jedes dieser 4 AS wird auf Basis der Informationen aus den RIPE RIS Routingarchiven ein entsprechender Untergraph. Wie bereits erwähnt, werden Routingpolicies dabei nicht weiter berücksichtigt.

Es werden mehrere Prefix-Hijacking-Szenarios konfiguriert, die alle unterschiedliche topologische Ebenen betreffen. Die resultierenden Partitionen werden von der Simulationssoftware berechnet und dann validiert, indem die Router entsprechend abgefragt werden. Im Gegensatz zur Simulation gibt es bei der Emulation keinen Grenzbereich, da Router sich immer für eine Route zur Wei-

terleitung der Datenpakete entscheiden. Da der implementierte Prozess zur Routenauswahl auch auf der IP-Adresse des benachbarten Routers als Entscheidungshilfe zurückgreift, wäre es an dieser Stelle möglich, durch die Konfiguration des Versuchsaufbaus bestimmte Entscheidungen zu beeinflussen. Um diesen Einfluss auszuschließen sollen betroffene AS einheitlich den Pfad zum False Origin bevorzugen, was für das True Origin der Worst-Case wäre. Zusätzlich wird ein weiteres Prefix vom True Origin annonciert, welches jedoch nicht vom Prefix-Hijacking betroffen ist. Dieses Prefix wird dann für den Aufbau von Tunnel hinein in die Partition des False Origin verwendet. Obwohl das nicht nötig wäre, wird dieses Prefix auch für den Tunnel bei der Auswahlstrategie „Nähe zum Grenzbereich“ verwendet, so lässt sich die Konfiguration der Tunnel-Endpunkte ohne Anpassung übernehmen. Die Ergebnisse werden durch die Verwendung dieses zusätzlichen Prefixes nicht beeinträchtigt.

Der Tunnel wird limitiert auf den betroffenen Prefix und er soll so konfiguriert werden, dass es den entsprechenden Datenverkehr in Richtung des True Origin weiterleitet. Die Antworten des True Origin werden nicht über den Tunnel gesendet, dafür können die normalen Routen verwendet werden, solange der Prefix des Kommunikationspartners nicht auch betroffen ist. Für die praktische Anwendbarkeit soll der Tunnel möglichst automatisch erzeugt werden können, ausgehend von einem Werkzeug, das für aktive Prefix-Hijacking-Szenarien entsprechende Partitionen berechnet und optimale Kooperationspartner identifiziert. Da Verbindungen zu Routern über SSH möglich sind, sollten vorab die öffentlichen Schlüssel möglicher Kooperationspartner untereinander ausgetauscht werden. Wurde der Tunnel erfolgreich aufgebaut, müssen noch die statischen Route für das Prefix konfiguriert werden (vgl. Abschnitt 7.2.2). Die statischen Routen können erst nach dem Aufbau des Tunnels, sollten aber vor der Annoncierung des Prefixes erstellt werden. Aufgrund der bereits erwähnten administrativen Distanz lokaler Netzwerk-Adapter, werden statische Routen für die beiden nächstkleineren Subnetze eingerichtet. Zusätzlich werden diese für die Broadcast-Adresse des unteren und die Netz-Adresse des oberen Bereichs zwei statische Routen hinzugefügt. Es ist notwendig, eine IP-Adresse des betroffenen Prefixes einem Netzwerkinterface des annoncierenden Routers zuzuweisen. Diese IP-Adresse ist für die Weiterleitung verloren, da eine einzelne IP-Adresse als /32-Prefix interpretiert wird. Damit ist dieser Prefix immer

der spezifischere Prefix und eine statische Route zur Weiterleitung wäre ohne Effekt.

7.4 Auswertung

Die verwendeten Daten des RIPE RIS Routingarchivs enthalten 56.991 unterschiedliche AS. Insgesamt wurden 10.458 Prefixe erkannt, für die ein MOAS-Konflikt existiert. Da MOAS-Konflikte pro Prefix erkannt werden, wurden die Daten im Hinblick auf die beteiligten AS gefiltert und doppelte Paare entfernt. Dies führt zu 1.302 unterschiedlichen AS-Paaren mit MOAS-Konflikten. Insgesamt 1.942 AS sind in diese Konflikte eingebunden, das sind 3,3% der Gesamtmenge.

7.4.1 Die Auswahlstrategien

Die Simulation wurde durchgeführt, um die Effektivität unterschiedlicher Auswahlstrategien für Kooperationspartner zu ermitteln. Dabei wurde davon ausgegangen, dass beliebige AS als mögliche Kooperationspartner in Frage kommen und die Größe der Partition des True Origin relevant für die Evaluation ist. AS im Grenzbereich wurden dem False Origin zugeordnet. Abbildung 20 zeigt das absolute Wachstum der Partition des True Origin in AS für die unterschiedlichen Auswahlstrategien. Um die Verteilung der Partitionsveränderung, die Varianz und den Median als Indikatoren für die Effektivität der Auswahlstrategien darzustellen, sind diese Werte in Box-Plot-Diagrammen dargestellt. Die oberen Whisker verdeutlichen dabei, dass auch wenn die Partition des True Origin zunächst sehr klein ist, die Auswahl eines geeigneten Kooperationspartners massives Wachstum der Partition ermöglicht. Darüber hinaus ist ersichtlich, dass die Auswahl der AS mit den „meisten Peers“ die erfolgreichste Auswahlstrategie ist. Die Auswahlstrategien „Nähe zum Angreifer“ und „Niedrige topologische Position“ haben ähnlichen Erfolg, und auch die Auswahl eines AS mit der „optimalen Position“ führt zu einer deutlichen Veränderung der Partition. Die übrigen Auswahlstrategien scheinen für eine Vergrößerung der Partition nicht geeignet zu sein.

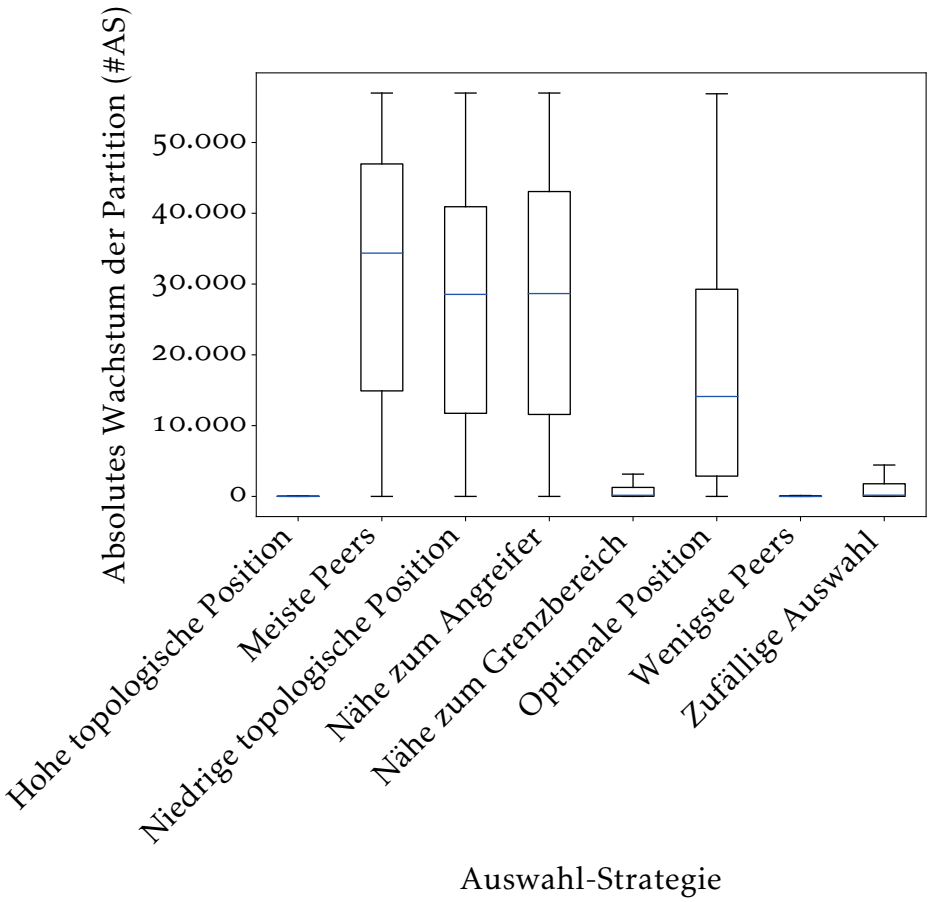

Abbildung 20: *Wachstum der Partition des True Origin (reale Daten)*

Bei der Betrachtung der relativen Veränderung in Abbildung 21 wird deutlich, dass die Strategie der „meisten Peers“ noch immer die größte Veränderung erreicht. Im Vergleich zu den Absolutwerten zeigt sich aber, dass die Strategie der „niedrigen topologische Position“ etwas besser als die der „Nähe zum Angreifer“ ist. Auch die Auswahlstrategie der „optimalen Position“ ist nach wie vor gut, allerdings mit deutlichem Abstand zu den anderen drei Strategien.

Abschließend kann für die Auswahlstrategien festgehalten werden, dass die drei besten Strategien grundsätzlich eine gute Entscheidung sind. Die übrigen Strategien erreichen mittlere bis gar keine Veränderungen der Partition des True Origin. Obwohl der prozentuale Gewinn explizit dargestellt ist, zeigen die Zahlen keine signifikante Korrelation, weder zwischen der vorherigen

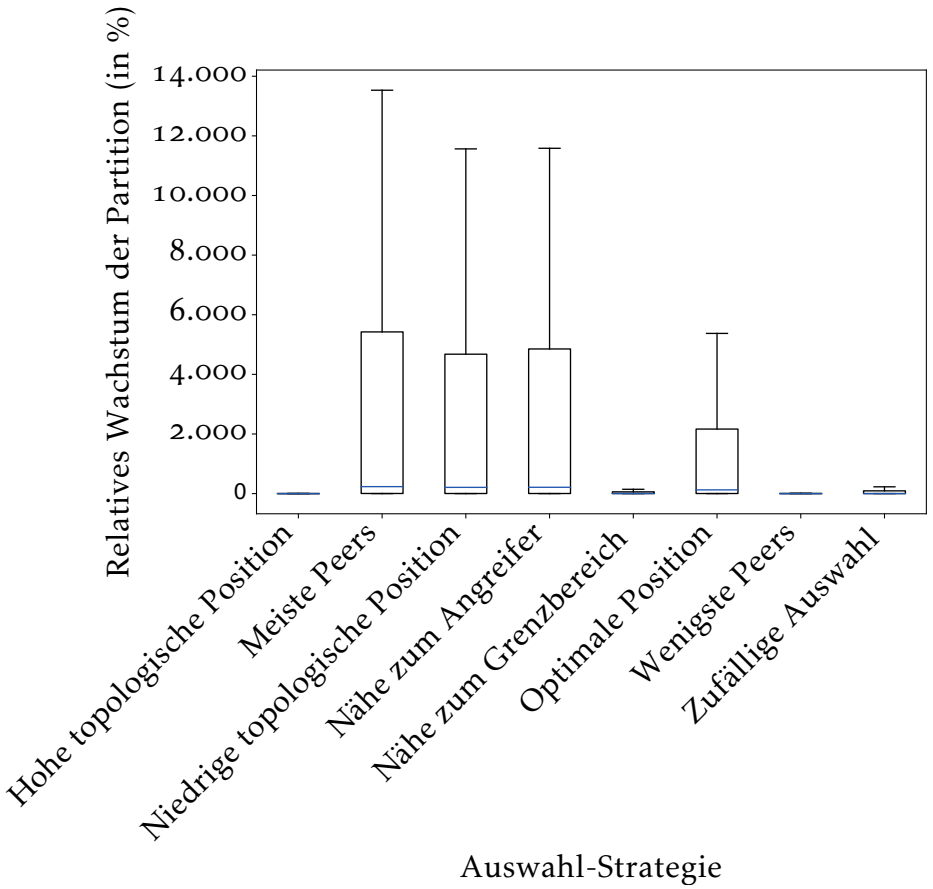

Abbildung 21: *Relative Veränderung der Partition des True Origin (reale Daten)*

Partitionsgröße noch der topologischen Position des True Origin oder des Kooperationspartners.

7.4.2 Ergebnisse der Emulation

Aufgrund der geringen Ressourcen, die für den Versuch zur Verfügung standen, wurde die Emulation auf einem kleinen Netzwerk durchgeführt, das dem Internet aber in der Struktur ähnlich ist. Abbildung 22 zeigt dieses Netzwerk, das insgesamt 34 AS bei 4 Clique-Mitgliedern des Internet-Core enthält. Im Hinblick auf das Verhältnis des Cores zum Rest des Internets, ist die Anzahl von 4 AS sehr groß. Die Zahl wurde bewusst festgesetzt, um die größte Clique des Netzwerks als Core zu betrachten. Nur so sind insbesondere die topologischen Merkmale auch in diesem kleinen Netzwerk entsprechend darstellbar.

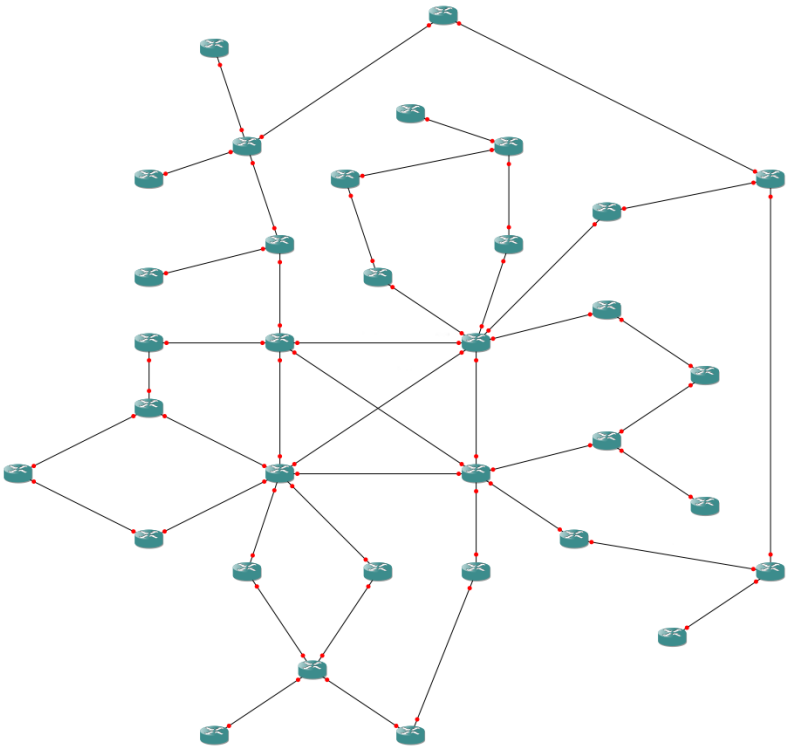

Abbildung 22: *Das erstellte Netzwerk für die Emulation mit GNS3*

Die 13 AS der Ebene 1 sind etwa $\frac{1}{3}$ des gesamten Netzwerks, wie in Kapitel 6 dargestellt. In den Ebenen 2 und 3 finden sich mit 17 AS etwa die Hälfte des gesamten Netzwerks. Dies ist etwas weniger als der Anteil von $\frac{2}{3}$, der sonst im Internet für diese Ebenen vorliegt. Diese Einschränkung wurde zur weiteren Vereinfachung umgesetzt. Da es sich hauptsächlich um periphere AS handelt, sind die zu erwartenden Abweichungen eher gering.

Jedes AS wird bei der Emulation mit einer Routerinstanz dargestellt. Obwohl dies nicht die möglichen AS internen Routingeffekte abbilden kann, ist es geeignet, um BGP-Routing zwischen AS zu emulieren. Alle AS, die nicht Teil eines MOAS-Konflikts sind, werden mit einem individuellen \24-Prefix konfiguriert.

Das Netzwerk wird zusätzlich als Eingabe für den Simulator verwendet. Für jede Kombination der Topologieebenen von True Origin und False Origin wird stellvertretend eine Simulation durchgeführt.

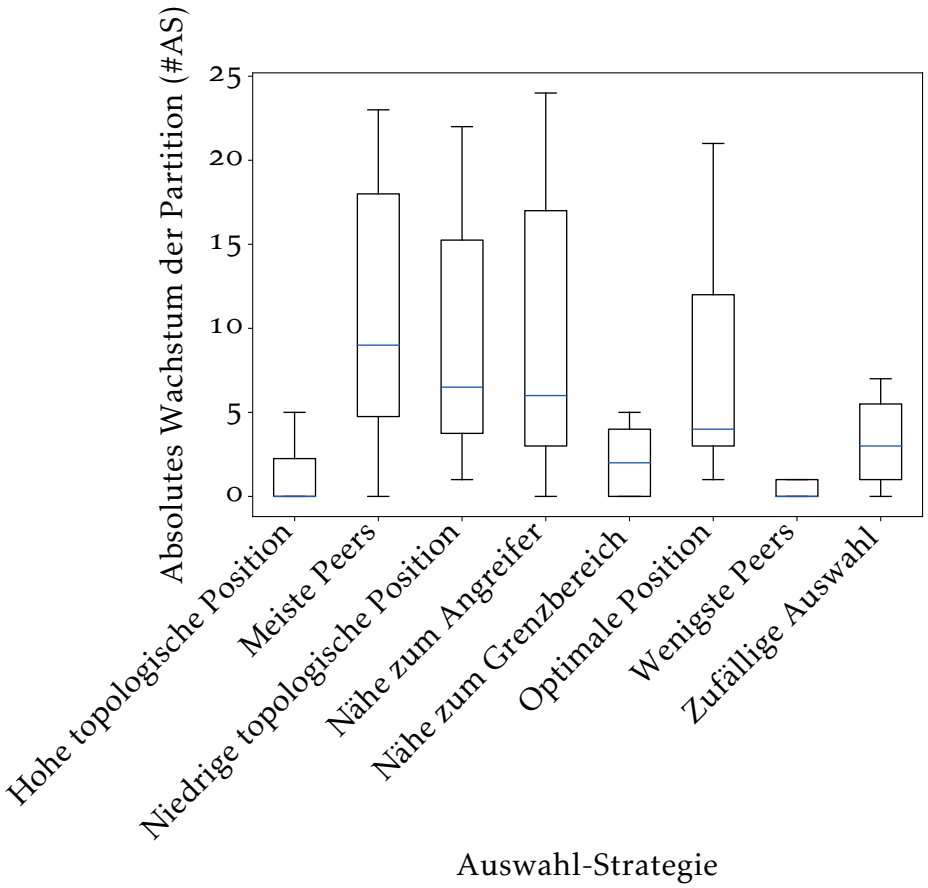

Abbildung 23: *Wachstum der Partition des True Origin (erzeugte Daten)*

Die Ergebnisse sind in Abbildung 23 und 24 dargestellt. Beide Abbildungen zeigen, dass sich das generierte kleine Netzwerk im Hinblick auf Prefix-Hijacking und resultierende Partitionen ähnlich dem realen Internet verhält.

Im Anschluss an die Simulation werden die besten drei Auswahlstrategien innerhalb der Emulation näher untersucht. Basierend auf dem in der Simulation ausgewählten Kooperationspartner werden die Router der Emulation entsprechend konfiguriert und die Ergebnisse gegen die der Simulation gehalten.

Im Gegensatz zum realen Internet erlaubt die Emulationsumgebung die Abfrage jedes einzelnen AS nach der getroffenen Routingentscheidung. Dafür wird für jedes Prefix-Hijacking-Szenario jedes AS der Emulation mit dem Befehl *show ip bgp* abgefragt und die Routingtabelle analysiert. Die Ergebnisse der bes-

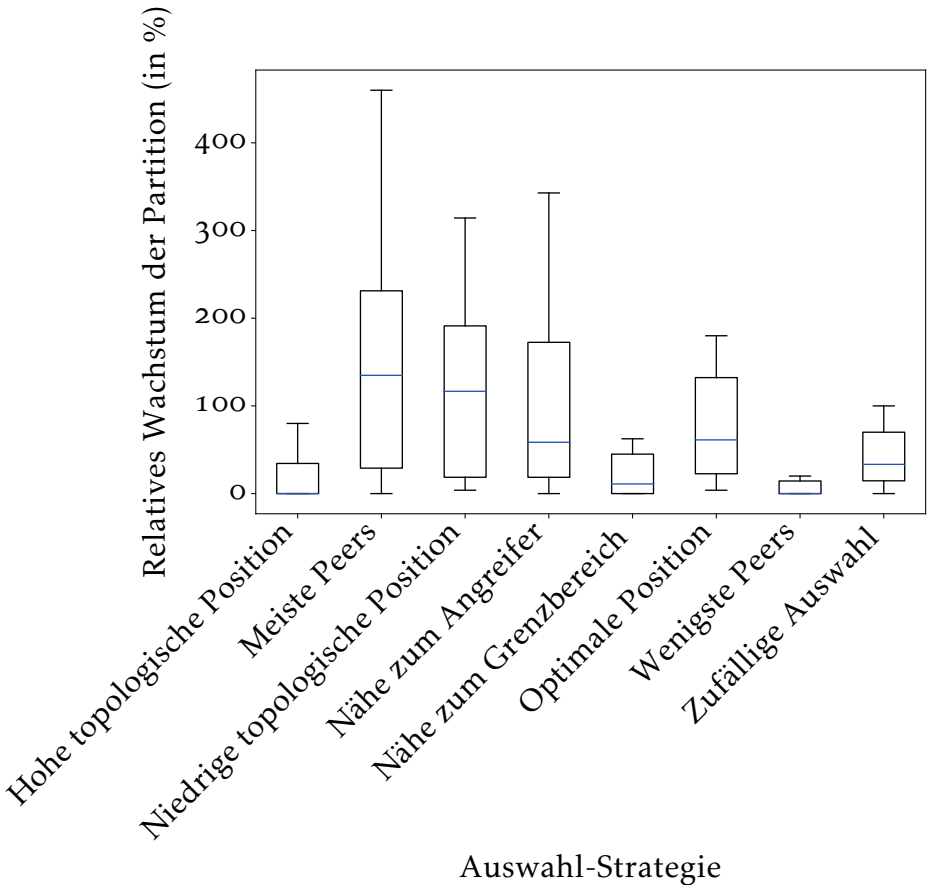

Abbildung 24: *Relative Veränderung der Partition des True Origin (erzeugte Daten)*

ten drei Auswahlstrategien für Kooperationspartner wird in den Abbildungen 25 und 26 dargestellt.

Die Ergebnisse aus der Emulation stützen dabei die Ergebnisse der Simulation. Der größte Zuwachs wurde mit der Auswahlstrategie der „meisten Peers“ erzielt. Der Fehler der Simulation ist dabei auf die Grenzpartition zurückzuführen. Der mittlere Fehler liegt bei -0,7 mit einer Standardabweichung von 3,9372 AS zur durchgeführten Emulation.

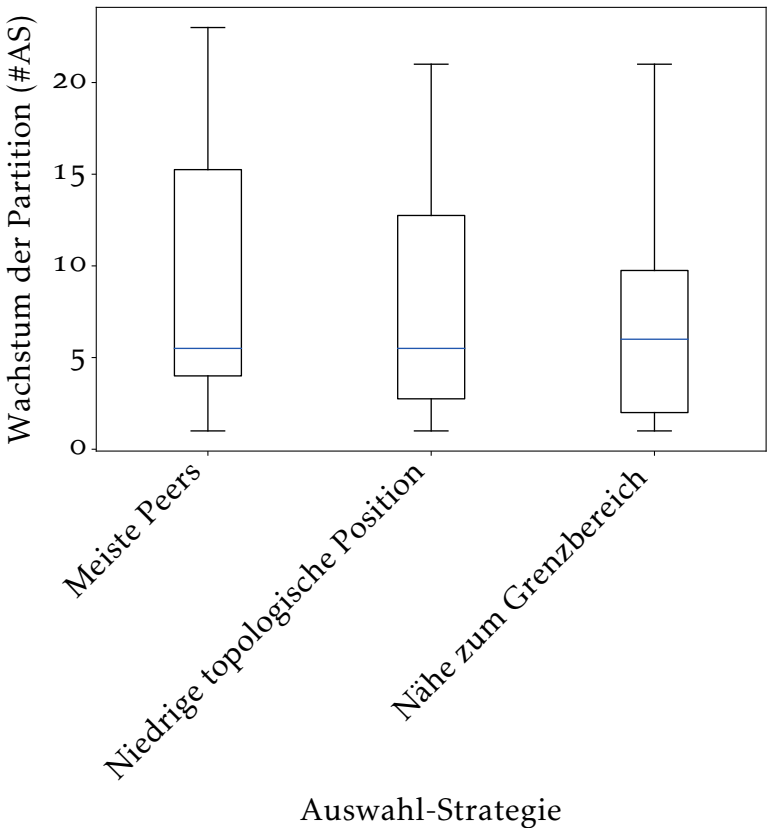

Abbildung 25: *Absolutes Wachstum der True Partition (Emulation)*

7.5 Fazit

In diesem Kapitel wurde gezeigt, dass die Partitionen, die sich aus einem Prefix-Hijacking ergeben gezielt verändert werden können. Durch den Aufbau von Tunneln zwischen AS lassen sich die ausgewählten Routen von Datenpaketen mit geringem Auswand beeinflussen. Insbesondere ergibt sich durch die gezielte Kooperation von AS eine Gegenmaßnahme für den True Origin, um die Erreichbarkeit seines betroffenen Prefix zu verbessern. Darüber hinaus wurde gezeigt, dass es die Möglichkeit gibt, ein deutlich kleineres Netzwerk mit im Hinblick auf Prefix-Hijacking und resultierende Partitionen ähnlichen Eigenschaften wie das Internet zu erzeugen, das sich zur Emulation mit begrenzten Ressourcen eignet. Im Fall eines Prefix-Hijacking-Szenarios lässt sich ein guter Kooperationspartner durch Simulation und Emulation ermitteln und das Ergebnis bereits im Vorfeld abschätzen. Es können auch mehrere Kooperations-

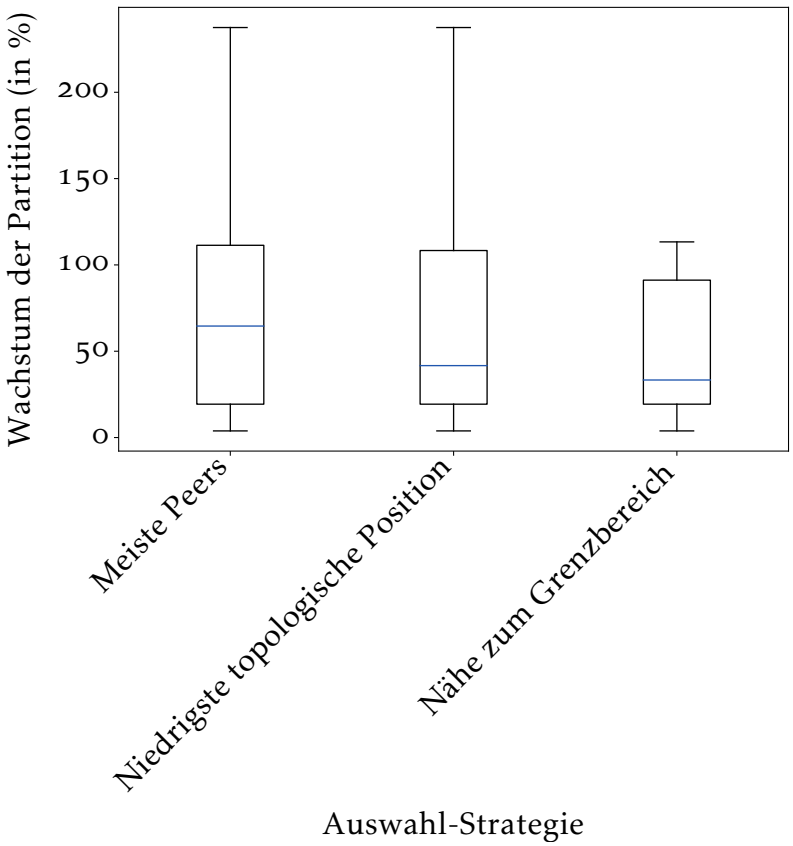

Abbildung 26: *Relatives Wachstum der True Partition (Emulation)*

partner einbezogen werden, was allerdings die Komplexität der Routing- und Tunnel-Konfiguration deutlich erhöht.

Die erstellte Umgebung zur Emulation von Routinganomalien liefert wichtige Hinweise als Ergänzung zu den üblichen Simulationen. Insbesondere auf dem Weg zu einer praktischen Umsetzung von Gegenmaßnahmen spielt die Emulation eine maßgebliche Rolle. So können bereits im Vorfeld mögliche implementierungsspezifische Probleme erkannt und abgeschwächt werden.

8 Fazit und Ausblick

Die vorliegende Arbeit beantwortet vier konkrete Fragestellungen im Forschungskontext von Anomalien im Internetrouting:

- Wie sind die Informationen in Routingarchiven organisiert und wie lassen sich diese zur Erkennung von Anomalien im Internetrouting nutzen?
- Welche Möglichkeiten gibt es, neben öffentlich verfügbaren Routingarchiven, um weitere Daten über das Internetrouting zu sammeln (Monitoring), um die Überwachung der Schutzziele zu verbessern?
- Wie lässt sich die Sicherheit Autonomer Systeme im Bezug auf BGP-Routinganomalien quantifizieren?
- Gibt es Gegenmaßnahmen, um Angriffe auf das Internetrouting abzuwehren und wie lassen sich diese realisieren?

Zunächst wurden in Kapitel 4 Routingarchive und die darin enthaltenen Archivdaten analysiert. Diese Daten bilden nahezu die einzige Datenbasis für die gesamte Forschung im Bereich der Anomalieerkennung im Internetrouting. Die meisten Arbeiten in dem Forschungskontext berücksichtigen die Daten von ein oder zwei Routingarchiven. Es wurden alle vier öffentlich verfügbaren Routingarchive untersucht. Die Ergebnisse ermöglichen den Aufwand der Datenanalyse zu minimieren und die Diversität der 197 betrachteten Beobachtungspunkte so zu berücksichtigen, dass eine möglichst breite Datenbasis zur Verfügung steht. Es wurde für unterschiedliche Grade der Vollständigkeit gezeigt, dass bereits ein gezielt ausgewählter Beobachtungspunkt ausreicht, um mehr als 99% der im Internet aktiven AS zu ermitteln. Die Sichtbarkeit angebotener Prefixe und einzelner Verbindungen zwischen AS ist jedoch durch die

Position der beobachtenden AS eingeschränkt. Während bereits ein Beobachtungspunkt ausreicht, um 75% der im Internet verfügbaren Prefixe zu ermitteln, wurden für 75% der sichtbaren Verbindungen zwischen AS bereits sechs Route-Reflektor-Clients benötigt. Für die umfassende Sichtbarkeit aller Prefixe mussten bis zu 141 Beobachtungspunkte und für alle Verbindungen zwischen AS bis zu 124 Beobachtungspunkte berücksichtigt werden.

Anschließend wurden in Kapitel 5 öffentlich verfügbare Daten verwendet, um die Datenbasis zur Erkennung und Analyse von Anomalien im Internetrouting zu vergrößern. Um dieses Ziel zu erreichen wurden mit Looking-Glass-Servern und den Mitgliederlisten von Internetknotenpunkten zwei zusätzliche Datenquellen nutzbar gemacht. Im Vergleich zu bereits existierenden Ansätzen insbesondere im Bereich der Internetknotenpunkte wurden bis zu 74% mehr Mitgliederinformationen von 66 Internetknotenpunkten gesammelt. Darüber hinaus konnten aus den Mitgliederlisten zusätzliche Hinweise auf die Peeringpolicy von Autonomen System extrahiert werden. Mit diesen Informationen lassen sich Aussagen über die Wahrscheinlichkeit von neuen Verbindungen zwischen AS präziser gestalten.

Die Sicherheit Autonomer Systeme im Hinblick auf Prefix-Hijacking wurde in Kapitel 6 eingehend untersucht. Es wurde gezeigt, dass die bisher in der Literatur verwendete Formel zur Abschätzung von Prefix-Hijacking-Resilienz eine unnötig hohe Ungenauigkeit aufweist. Diese Ungenauigkeit wurde durch eine neu entwickelte Formel deutlich verringert. Auf Basis dieser verbesserten Formel wurden die Effekte zusätzlicher Verbindungen zwischen AS, wie sie bei Internetknotenpunkten mit geringem Ressourcenaufwand erstellt werden können, untersucht und es wurde gezeigt, dass allein eine hohe Anzahl an Peeringpartnern die Resilienz nicht grundsätzlich verbessert. Vielmehr ist die Auswahl der Peeringpartner maßgeblich für eine Erhöhung der Resilienz und damit der Sicherheit für die Prefixe eines AS.

Die Auswahl der Kooperationspartner ist in Kapitel 7 relevant. In diesem Kapitel wurde gezeigt, dass es Maßnahmen zur Mitigation von Prefix-Hijacking gibt und dass gemeinsam mit einem Kooperationspartner die resultierende Partitionierung im Internet deutlich verändert werden kann. Es wurden verschiedene Auswahlstrategien für die Wahl eines Kooperationspartners sowohl

in einer Simulation als auch in einer Emulation des Internetroutings evaluiert. Dabei war es durch die Emulation möglich, bestimmte Effekte der Simulation abzuschwächen und die Ergebnisse noch näher an die tatsächlichen Verhältnisse im Internet anzupassen. Dafür wurde ein Emulationsnetzwerk erstellt, das sich trotz der deutlich geringeren Größe im Hinblick auf Routingdynamiken ähnlich dem Internet verhält.

Die Ergebnisse dieser Arbeit bilden eine Grundlage für nachfolgende Arbeiten in dem Forschungsbereich. Für eine optimale Datenbasis in der Forschung und beim Monitoring von Anomalien im Internetrouting ist es notwendig, Verfahren zur kontinuierlichen Beobachtung der Routingarchive zu etablieren und dynamischen Zugang zu den vollständigen Informationen anzubieten. Die bisher nur für europäische Internetknotenpunkte durchgeführte Untersuchung der Mitgliederinformationen gilt es für möglichst alle Internetknotenpunkte weltweit zu erweitern. Im Hinblick auf die Abschätzung neuer Verbindungen zwischen AS ist eine Längsschnitterhebung notwendig, um die ermittelten Daten zukünftig für die Anomalieerkennung zu verwenden. Die einfachere Umsetzung von Maßnahmen zur Mitigation von Prefix-Hijacking und der Transfer weiterer Möglichkeiten zur Erhöhung der Prefix-Hijacking-Resilienz aus der Forschung in die Anwendung sind weitere wichtige Schritte zur Verbesserung der Sicherheit im Internetrouting.

Literatur

[1] J. Abley und K. Lindqvist. *Operation of Anycast Services*. RFC 4786. IETF, 2006.

[2] B. Ager, N. Chatzis, A. Feldmann, N. Sarrar, S. Uhlig und W. Willinger. „Anatomy of a large european IXP“. In: *ACM SIGCOMM Computer Communication Review* 42 (2012).

[3] B. Al-Musawi, P. Branch und G. Armitage. „Detecting BGP instability using Recurrence Quantification Analysis (RQA)“. In: *2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)*. 2015.

[4] C. Amin. *RIS Live BGP Message Stream*. https://labs.ripe.net/Members/chris_amin/ris-live-bgp-message-stream (Letzter Zugriff: 23. April 2019). 2019.

[5] L. Amini, A. Shaikh und H. Schulzrinne. „Issues with Inferring Internet Topological Attributes“. In: *Comput. Commun.* 27.6 (2004).

[6] B. Augustin, X. Cuvellier, B. Orgogozo, F. Viger, T. Friedman, M. Latapy, C. Magnien und R. Teixeira. „Avoiding Traceroute Anomalies with Paris Traceroute“. In: *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*. IMC '06. Rio de Janeriro, Brazil: ACM, 2006.

[7] H. Ballani, P. Francis und X. Zhang. „A Study of Prefix Hijacking and Interception in the Internet“. In: *Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*. SIGCOMM '07. Kyoto, Japan: ACM, 2007.

[8] P. Barford, A. Bestavros, J. Byers und M. Crovella. „On the Marginal Utility of Network Topology Measurements“. In: *Proceedings of the 1st ACM*

SIGCOMM Workshop on Internet Measurement. IMW '01. San Francisco, California, USA: ACM, 2001.

[9] J. Barnes. *High Integrity Software: The SPARK Approach to Safety and Security*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2003.

[10] T. Bates, P. Smith und G. Huston. *CIDR Report*. https://www.cidr-report.org/as2.0/ (Letzter Zugriff: 25. April 2019).

[11] D. Bayer. *Visibility of Prefix Lengths in IPv4 and IPv6*. https://labs.ripe.net/Members/dbayer/visibility-of-prefix-lengths (Letzter Zugriff: 24. April 2019). 2010.

[12] L. Benkins. *White paper: Practical BGP Security: Architecture, Techniques and Tools*. Techn. Ber. Manchester: Renesys, 2005.

[13] H. Berkowitz, E Davies und L. Andersson. *An Experimental Methodology for Analysis of Growth in the Global Routing Table*. https://tools.ietf.org/html/draft-berkowitz-tblgrow-00 (Letzter Zugriff: 24. April 2019). 2001.

[14] BGP Looking Glass. *Database*. http://www.bgplookingglass.com/ (Letzter Zugriff: 23. April 2019).

[15] BGP4.as. *BGP Looking Glasses for IPv4/IPv6, Traceroute & BGP Route Servers*. https://www.bgp4.as/looking-glasses (Letzter Zugriff: 23. April 2019).

[16] BGP4.net. *IPv4 Looking Glass Sites, listed by ASN*. http://www.bgp4.net/lg (Letzter Zugriff: 23. April 2019).

[17] E. Biersack, Q. Jacquemart, F. Fischer, J. Fuchs, O. Thonnard, G. Theodoridis, D. Tzovaras und P. Vervier. „Visual analytics for BGP monitoring and prefix hijacking identification". In: *IEEE Network* 26.6 (2012).

[18] L. Blunk, M. Karir und C. Labovitz. *Multi-Threaded Routing Toolkit (MRT) Routing Information Export Format*. RFC 6396. IETF, 2011.

[19] BMI. *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)*. Hrsg. von Bundesministerium des Innern. Berlin, 2009.

[20] BMI. „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV)“. In: *Bundesgesetzblatt* Teil I.20 (2016). Hrsg. von Bundesministerium des Innern.

[21] V. J. Bono. *7007 Explanation and Apology*. https://seclists.org/nanog/1997/Apr/444 (Letzter Zugriff: 24. April 2019).

[22] R. Braden, L. Zhang, S. Berson, S. Herzog und S. Jamin. *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*. RFC 2205. IETF, 1997.

[23] T. Brisco. *DNS Support for Load Balancing*. RFC 1794. IETF, 1995.

[24] BSI. *IT-Grundschutz-Kompendium*. Hrsg. von Bundesamt für Sicherheit in der Informationstechnik. 2. Ausgabe. Köln/Bonn: Bundesanzeiger Verlag GmbH, 2019.

[25] Center for Applied Internet Data Analysis (CAIDA). *AS Relationships*. https://www.caida.org/data/as-relationships/ (Letzter Zugriff: 25. April 2019).

[26] Center for Applied Internet Data Analysis (CAIDA). *Skitter AS Links Dataset*. https://www.caida.org/data/active/skitter_aslinks_dataset.xml (Letzter Zugriff: 23. April 2019).

[27] H. Chang, R. Govindan, S. Jamin, S. J. Shenker und W. Willinger. „Towards Capturing Representative AS-level Internet Topologies“. In: *Computer Networks: The International Journal of Computer and Telecommunications Networking* 44.6 (2004).

[28] H. Chang, S. Jamin und W. Willinger. „Inferring AS-level Internet Topology from Router-Level Path Traces“. In: *Proceedings of SPIE - The International Society for Optical Engineering* 4526 (2001).

[29] N. Chatzis, G. Smaragdakis, A. Feldmann und W. Willinger. „There is More to IXPs Than Meets the Eye“. In: *SIGCOMM Comput. Commun. Rev.* 43.5 (2013).

[30] K. Chen, C. Hu, W. Zhang, Y. Chen und B. Liu. „On the Eyeshots of BGP Vantage Points“. In: *GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference*. 2009.

[31] CISCO. *Software: IOS*. https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-technologies/index.html (Letzter Zugriff: 24. April 2019).

[32] CNET News Staff. *Router glitch cuts Net access*. https://www.cnet.com/news/router-glitch-cuts-net-access/(Letzter Zugriff: 24. April 2019).

[33] J. Cordasco und S. Wetzel. „An Attacker Model for MANET Routing Security". In: *Proceedings of the Second ACM Conference on Wireless Network Security*. WiSec '09. Zurich, Switzerland: ACM, 2009.

[34] R. B. da Silva und E. Souza Mota. „A Survey on Approaches to Reduce BGP Interdomain Routing Convergence Delay on the Internet". In: *IEEE Communications Surveys Tutorials* 19.4 (2017).

[35] DE-CIX. *Frankfurt bleibt europäische Hauptstadt des Peerings – Rasantes internationales Wachstum für DE-CIX in New York, Dallas und Madrid*. https://www.de-cix.net/de/about-de-cix/media-center/press-releases/frankfurt-continues-as-european-capital-for-peering-rapid-international-growth-for-de-cix-in-new-york-dallas-and-madrid/ (Letzter Zugriff: 23. April 2019). 2017.

[36] C. C. Demchak und Y. Shavitt. „China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking". In: *Military Cyber Affairs* 3.1 (2018).

[37] S. Deshpande, M. Thottan, T. K. Ho und B. Sikdar. „An Online Mechanism for BGP Instability Detection and Analysis". In: *IEEE Transactions on Computers* 58.11 (2009).

[38] D. Dolev und A. C. Yao. „On the Security of Public Key Protocols". In: *Proceedings of the 22Nd Annual Symposium on Foundations of Computer Science*. SFCS '81. Washington, DC, USA: IEEE Computer Society, 1981.

[39] Duden. *Anomalie*. https://www.duden.de/rechtschreibung/Anomalie (Letzter Zugriff: 24. April 2019).

[40] C. Eckert. *IT-Sicherheit: Konzepte - Verfahren - Protokolle*. 9., aktualisierte und korr. Aufl. München: Oldenbourg, 2013.

[41] O. Eissa. „Security Analysis of Autonomic Networking on Cisco Gear". Masterarbeit. University of Bonn, 2017.

[42] A. Faggiani, E. Gregori, A. Improta, L. Lenzini, V. Luconi und L. Sani. „A study on traceroute potentiality in revealing the Internet AS-level topology“. In: *2014 IFIP Networking Conference*. 2014.

[43] H. Federrath und A. Pfitzmann. „Datenschutz und Datensicherheit“. In: *Taschenbuch der Informatik*. Hrsg. von U. Schneider und D. Werner. 3. Auflage. München: Carl Hanser Verlag, 2000.

[44] U. Feige. „A Threshold of Ln N for Approximating Set Cover“. In: *J. ACM* 45.4 (1998).

[45] R. Fielding und J. Reschke. *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content*. RFC 7231. IETF, 2014.

[46] S. Fischer-Hübner. *IT-security and Privacy: Design and Use of Privacy-enhancing Security Mechanisms*. Berlin, Heidelberg: Springer-Verlag, 2001.

[47] K. D. Frazer. *NSFNET: A Partnership for High-Speed Networking*. Techn. Ber. Merit Network, Inc., 1995.

[48] V. Fuller, T. Li, J. Yu und K. Varadhan. *Supernetting: an Address Assignment and Aggregation Strategy*. RFC 1338. IETF, 1992.

[49] Galaxy Technologies, LLC. *Software: Graphical Network Simulator 3*. https://www.gns3.com/software (Letzter Zugriff: 24. April 2019).

[50] L. Gao. „On Inferring Autonomous System Relationships in the Internet“. In: *IEEE/ACM Trans. Netw.* 9.6 (2001).

[51] V. Giotsas und S. Zhou. „Improving the Discovery of IXP Peering Links through Passive BGP Measurements“. In: *2013 Proceedings IEEE INFOCOM*. 2013.

[52] Github-Projekt GNS3. *Software: Dynamips*. https://github.com/GNS3/dynamips (Letzter Zugriff: 24. April 2019).

[53] D. Goodin. *Google goes down after major BGP mishap routes traffic through China*. https://arstechnica.com/information-technology/2018/11/major-bgp-mishap-takes-down-google-as-traffic-improperly-travels-to-china/ (Letzter Zugriff: 25. April 2019). 2018.

[54] R. Govindan und A. Reddy. „An Analysis of Internet Inter-Domain Topology and Route Stability“. In: *Proceedings of the INFOCOM '97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution*. INFOCOM '97. Washington, DC, USA: IEEE Computer Society, 1997.

[55] R. Govindan und H. Tangmunarunkit. „Heuristics for Internet map discovery“. In: *Proceedings IEEE INFOCOM 2000. Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies*. Bd. 3. 2000.

[56] E. Gregori, A. Improta, L. Lenzini, L. Rossi und L. Sani. „On the Incompleteness of the AS-level Graph: A Novel Methodology for BGP Route Collector Placement“. In: *Proceedings of the 2012 Internet Measurement Conference*. IMC '12. Boston, Massachusetts, USA: ACM, 2012.

[57] M. Grey, M. Rossberg und G. Schaefer. „Automatic Creation of VPN Backup Paths for Improved Resilience Against BGP-attackers“. In: *Proceedings of the 27th Annual ACM Symposium on Applied Computing*. SAC '12. Trento, Italy: ACM, 2012.

[58] J. Hawkinson und T. Bates. *Guidelines for creation, selection, and registration of an Autonomous System (AS)*. RFC 1930. IETF, 1996.

[59] Y. He, G. Siganos, M. Faloutsos und S. Krishnamurthy. „A Systematic Framework for Unearthing the Missing Links: Measurements and Impact“. In: *Proceedings of the 4th USENIX Conference on Networked Systems Design & Implementation*. NSDI'07. Cambridge, MA: USENIX Association, 2007.

[60] M. Hollick, C. Nita-Rotaru, P. Papadimitratos, A. Perrig und S. Schmid. „Toward a Taxonomy and Attacker Model for Secure Routing Protocols“. In: *SIGCOMM Comput. Commun. Rev.* 47.1 (2017).

[61] X. Hu und Z. M. Mao. „Accurate Real-time Identification of IP Prefix Hijacking“. In: *2007 IEEE Symposium on Security and Privacy (SP '07)*. 2007.

[62] Hurricane Electric. *BGP Toolkit*. https://bgp.he.net/ (Letzter Zugriff: 26. April 2019).

[63] Y. Hyun, A. Broido und K. Claffy. „On Third-party Addresses in Traceroute Paths“. In: *Passive and Active Network Measurement Workshop (PAM)*. San Diego, CA: PAM, 2003.

[64] IANA. *Root Servers*. https://www.iana.org/domains/root/servers (Letzter Zugriff: 26. April 2019).

[65] Instituto di Informatica e Telematica. *Isolario Project*. https://www.isolario.it/ (Letzter Zugriff: 23. April 2019).

[66] Internet Research Lab (UCLA). *Cyclops AS Relationship Downloads*. http://irl.cs.ucla.edu/topology/ipv4/relationship/ (Letzter Zugriff: 25. April 2019).

[67] IRR.net. *List of Routing Registries*. http://www.irr.net/docs/list.html (Letzter Zugriff 25. April 2019).

[68] ISO/IEC 7498-1:1994(E). *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*. Standard. International Organization for Standardization, 1994.

[69] Q. Jacquemart. „Towards uncovering BGP hijacking attacks“. Diss. Paris: Télécom ParisTech, 2015.

[70] D. S. Johnson. „Approximation Algorithms for Combinatorial Problems“. In: *Journal of Computer and System Sciences* 9.3 (1974).

[71] R. M. Karp. „Reducibility Among Combinatorial Problems“. In: *Complexity of Computer Computations*. Springer, 1972.

[72] S. Kent und A. Chi. *Threat Model for BGP Path Security*. RFC 7132. IETF, 2014.

[73] S. Kent, C. Lynn und K. Seo. „Secure Border Gateway Protocol (S-BGP)“. In: *IEEE Journal on Selected Areas in Communications* 18.4 (2000).

[74] A. Khan, T. Kwon, H.-c. Kim und Y. Choi. „AS-level Topology Collection Through Looking Glass Servers“. In: *Proceedings of the 2013 Conference on Internet Measurement Conference*. IMC '13. Barcelona, Spain: ACM, 2013.

[75] V. Khare, Q. Ju und B. Zhang. „Concurrent Prefix Hijacks: Occurrence and Impacts“. In: *Proceedings of the 2012 Internet Measurement Conference*. IMC '12. Boston, Massachusetts, USA: ACM, 2012.

[76] J. Klensin. *Simple Mail Transfer Protocol*. RFC 5321. IETF, 2008.

[77] J. F. Kurose und K. W. Ross. *Computernetzwerke*. 5., aktualisierte Auflage. Pearson Studium, 2012.

[78] C. Labovitz, A. Ahuja, A. Bose und F. Jahanian. „Delayed Internet routing convergence". In: *IEEE/ACM Transactions on Networking* 9.3 (2001).

[79] C. Labovitz, G. R. Malan und F. Jahanian. „Origins of Internet Routing Instability". In: *IEEE INFOCOM '99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now*. Bd. 1. 1999.

[80] C. Labovitz, A. Ahuja und F. Jahanian. „Experimental Study of Internet Stability and Backbone Failures". In: *Proceedings of the Twenty-Ninth Annual International Symposium on Fault-Tolerant Computing*. FTCS '99. Washington, DC, USA: IEEE Computer Society, 1999.

[81] M. Lad, R. Oliveira, B. Zhang und L. Zhang. „Understanding Resiliency of Internet Topology against Prefix Hijack Attacks". In: *37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07)*. 2007.

[82] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang und L. Zhang. „PHAS: A Prefix Hijack Alert System". In: *Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15*. USENIX-SS'06. Vancouver, B.C., Canada: USENIX Association, 2006.

[83] A. Lakhina, M. Crovella und C. Diot. „Diagnosing Network-wide Traffic Anomalies". In: *Proceedings of the 2004 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*. SIGCOMM '04. Portland, Oregon, USA: ACM, 2004.

[84] M. Lepinski und S. Kent. *An Infrastructure to Support Secure Internet Routing*. RFC 6480. IETF, 2012.

[85] R. Lychev, S. Goldberg und M. Schapira. „BGP Security in Partial Deployment: Is the Juice Worth the Squeeze?" In: *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*. SIGCOMM '13. Hong Kong, China: ACM, 2013.

[86] H. V. Madhyastha, T. Isdal, M. Piatek, C. Dixon, T. Anderson, A. Krishnamurthy und A. Venkataramani. „iPlane: An Information Plane for Distributed Services“. In: *Proceedings of the 7th Symposium on Operating Systems Design and Implementation*. OSDI '06. Seattle, Washington: USENIX Association, 2006.

[87] D. Madory. *BGP Hijack of Amazon DNS to Steal Crypto Currency*. https://dyn.com/blog/bgp-hijack-of-amazon-dns-to-steal-crypto-currency/ (Letzter Zugriff: 25. April 2019). 2018.

[88] P. Mahadevan, D. Krioukov, M. Fomenkov, B. Huffaker, X. Dimitropoulos, K. Claffy und A. Vahdat. „The Internet AS-Level Topology: Three Data Sources and One Definitive Metric“. In: *ACM SIGCOMM Computer Communication Review (CCR)* 36 No 1 (2006).

[89] R. Mahajan, D. Wetherall und T. Anderson. „Understanding BGP misconfiguration“. In: *Proceedings of the 2002 conference on Applications, technologies, architectures, and protocols for computer communications*. SIGCOMM '02. Pittsburgh, Pennsylvania, USA: ACM, 2002.

[90] G. Malkin. *RIP Version 2*. RFC 2453. IETF, 1998.

[91] Z. M. Mao, J. Rexford, J. Wang und R. H. Katz. „Towards an Accurate AS-level Traceroute Tool“. In: *Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*. SIGCOMM '03. Karlsruhe, Germany: ACM, 2003.

[92] A. Maria, Z. Aviv und V. Laurent. „Hijacking Bitcoin: Routing Attacks on Cryptocurrencies“. In: *Security and Privacy (SP), 2017 IEEE Symposium on*. IEEE. 2017.

[93] S. A. Misel. *Wow, AS7007!* https://www.nanog.org/mailinglist/mailarchives/old_archive/1997-04/msg00340.html (Letzter Zugriff: 24. April 2019).

[94] J. Moy. *OSPF Version 2*. RFC 2328. IETF, 1998.

[95] S. Murphy. *BGP Security Vulnerabilities Analysis*. RFC 4272. IETF, 2006.

[96] B. Musawi, P. Branch und G. Armitage. „BGP Anomaly Detection Techniques: A Survey“. In: *IEEE Communications Surveys & Tutorials* PP (2016).

[97] National Security Agency (NSA). *Network Shaping 101*. https://www.documentcloud.org/documents/3871807-Network-Shaping-NSA-document.html (Letzter Zugriff: 24. April 2019). 2007.

[98] NIST. *Global Prefix/Origin Validation using RPKI*. https://rpki-monitor.antd.nist.gov/ (Letzter Zugriff: 24. April 2019).

[99] NLNOG RING. *Participants*. https://ring.nlnog.net/participants/ (Letzter Zugriff: 23. April 2019).

[100] W. B. Norton und H. A. Summa. *Internet Peering Playbook*. Übersetzte und bearbeitete Ausgabe. Frankfurt: DE-CIX, 2014.

[101] R. V. Oliveira, D. Pei, W. Willinger, B. Zhang und L. Zhang. „In Search of the Elusive Ground Truth: The Internet's AS-Level Connectivity Structure". In: *Proceedings of the 2008 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems*. SIGMETRICS '08. Annapolis, MD, USA: ACM, 2008.

[102] OpenDNS - BGPMon. *Webseite*. https://bgpmon.net/ (Letzter Zugriff: 24. April 2019).

[103] ORACLE Dyn. *DNS Analytics and Monitoring*. https://www.dyn.com/monitoring-analytics/ (Letzter Zugriff 24. April 2019).

[104] P. Papadimitratos, Z. J. Haas und J. Hubaux. „How to Specify and How to Prove Correctness of Secure Routing Protocols for MANET". In: *2006 3rd International Conference on Broadband Communications, Networks and Systems*. 2006.

[105] S. Papadopoulos, K. Moustakas, A. Drosou und D. Tzovaras. „Border gateway protocol graph: detecting and visualising internet routing anomalies". In: *IET Information Security* 10.3 (2016).

[106] PCH - Packet Clearinghouse. *Internet Exchange Directory*. https://www.pch.net/ (Letzter Zugriff: 23. April 2019).

[107] PeeringDB. *The Interconnection Database*. https://www.peeringdb.com/.

[108] L. L. Peterson und B. S. Davie. *Computer Networks, Fifth Edition: A Systems Approach*. 5th. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2011.

[109] Planetlab. *An open platform for developing, deploying and accessing planetary-scale services*. https://www.planet-lab.org (Letzter Zugriff: 23. April 2019).

[110] J. Postel und J. Reynolds. *Telnet Protocol Specification*. RFC 854. IETF, 1983.

[111] J. Qiu, L. Gao, S. Ranjan und A. Nucci. „Detecting bogus BGP route information: Going beyond prefix hijacking". In: *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm 2007*. 2007.

[112] T. Qiu, L. Ji, D. Pei, J. Wang, J. Xu und H. Ballani. „Locating Prefix Hijackers Using LOCK". In: *Proceedings of the 18th Conference on USENIX Security Symposium*. SSYM'09. Montreal, Canada: USENIX Association, 2009.

[113] Y. Rekhter und T. Li. *A Border Gateway Protocol 4 (BGP-4)*. RFC 1654. IETF, 1994.

[114] Y. Rekhter, T. Li und S. Hares. *A Border Gateway Protocol 4 (BGP-4)*. RFC 4271. IETF, 2006.

[115] P. Richter, G. Smaragdakis, A. Feldmann, N. Chatzis, J. Boettger und W. Willinger. „Peering at Peerings: On the Role of IXP Route Servers". In: *Proceedings of the 2014 Conference on Internet Measurement Conference*. IMC '14. Vancouver, BC, Canada: ACM, 2014.

[116] RIPE. *Evaluating The Effects Of Anycast On DNS Root Nameservers*. https://www.ripe.net/publications/docs/ripe-393 (Letzter Zugriff: 24. April 2019). 2006.

[117] RIPE. *Routing Information Service Live (RIS Live)*. https://ris-live.ripe.net/ (Letzter Zugriff: 23. April 2019).

[118] RIPE. *Routing Information Service (RIS)*. http://ris.ripe.net (Letzter Zugriff: 23. April 2019).

[119] RIPE. *YouTube Hijacking: A RIPE NCC RIS case study*. https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study (Letzter Zugriff: 25. April 2019). 2008.

[120] RIPE NCC. *Software: libbgpdump*. https://bitbucket.org/ripencc/bgpdump/wiki/Home (Letzter Zugriff: 24. April 2019).

[121] A. de la Rocha Gómez-Arevalillo und P. Papadimitratos. „Blockchain-based Public Key Infrastructure for Inter-Domain Secure Routing“. In: *International Workshop on Open Problems in Network Security (iNetSec)*. Hrsg. von J. Camenisch und D. Kesdoğan. Bd. IFIP eCollection-1. Open Problems in Network Security. Rome, Italy, 2017.

[122] Routeviews. *University of Oregon Route Views Project*. http://www.routeviews.org/routeviews/ (Letzter Zugriff: 23. April 2019).

[123] A. Scherr. „Werte und Normen“. In: *Soziologische Basics: Eine Einführung für pädagogische und soziale Berufe*. Hrsg. von A. Scherr. Wiesbaden: VS Verlag für Sozialwissenschaften, 2013.

[124] J. Schlamp, G. Carle und E. W. Biersack. „A Forensic Case Study on As Hijacking: The Attacker's Perspective“. In: *SIGCOMM Comput. Commun. Rev.* 43.2 (2013).

[125] J. Schlamp. „An Evaluation of Architectural Threats to Internet Routing“. Diss. Technical University of Munich, 2016.

[126] P. Sermpezis, V. Kotronis, P. Gigis, X. Dimitropoulos, D. Cicalese, A. King und A. Dainotti. „ARTEMIS: Neutralizing BGP Hijacking Within a Minute“. In: *IEEE/ACM Transactions on Networking* 26.6 (2018).

[127] P. Sermpezis, V. Kotronis, A. Dainotti und X. Dimitropoulos. „A Survey Among Network Operators on BGP Prefix Hijacking“. In: *SIGCOMM Comput. Commun. Rev.* 48.1 (2018).

[128] Y. Shavitt und E. Shir. „DIMES: Let the Internet Measure Itself“. In: *SIGCOMM Comput. Commun. Rev.* 35.5 (2005).

[129] X. Shi, Y. Xiang, Z. Wang, X. Yin und J. Wu. „Detecting Prefix Hijackings in the Internet with Argus“. In: *Proceedings of the 2012 Internet Measurement Conference*. IMC '12. Boston, Massachusetts, USA: ACM, 2012.

[130] G. Siganos und M. Faloutsos. „Detection of BGP routing misbehavior against cyber-terrorism“. In: *MILCOM 2005 - 2005 IEEE Military Communications Conference*. 2005.

[131] G. Siganos und M. Faloutsos. „Analyzing BGP Policies: Methodology and Tool“. In: *Proceedings IEEE INFOCOM 2004, 23rd Annual Joint Conference of the IEEE Computer and Communications Societies*. 2004.

[132] Spamhaus. *Network Hijacking on the Rise*. https://www.spamhaus.org/news/article/732/ (Letzter Zugriff: 29. April 2019).

[133] D. Spirin. *Prefix hijacking by Michael Lindsay via Internap*. https://mailman.nanog.org/pipermail/nanog/2011-August/039379.html (Letzter Zugriff: 29. April 2019).

[134] N. Spring, R. Mahajan, D. Wetherall und T. Anderson. „Measuring ISP Topologies with Rocketfuel". In: *IEEE/ACM Trans. Netw.* 12.1 (2004).

[135] M. Steenstrup. *Inter-Domain Policy Routing Protocol Specification: Version 1*. RFC 1479. IETF, 1993.

[136] Q. R. Suite. *Webseite*. https://www.quagga.net/ (Letzter Zugriff: 24. April 2019).

[137] A. S. Tanenbaum. *Computernetzwerke*. 3. revidierte Auflage. München: Pearson Studium, 2000.

[138] A. Toonk. *How Hacking Team Helped Italian Special Operations Group with BGP Route Hijack*. https://bgpmon.net/how-hacking-team-helped-italian-special-operations-group-with-bgp-routing-hijack/ (Letzter Zugriff: 24. April 2019). 2015.

[139] I. Van Beijnum. *BGP - Building Reliable Networks with the Border Gateway Protocol*. O'Reilly & Associates, Inc., 2002.

[140] T. Wan, E. Kranakis und P. C. van Oorschot. „Pretty Secure BGP (psBGP)". In: *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. San Diego, California, USA, 2005.

[141] F. Wang und L. Gao. „On Inferring and Characterizing Internet Routing Policies". In: *Proceedings of the 3rd ACM SIGCOMM Conference on Internet Measurement*. IMC '03. Miami Beach, FL, USA: ACM, 2003.

[142] R. White. „Securing BGP Through Secure Origin BGP". In: *The Internet Protocol Journal* 6.3 (2003).

[143] R. White, A. Retana und D. Slice. *Optimal Routing Design*. 1st. Cisco Press, 2010.

[144] G. Wolf und A Pfitzmann. „Charakteristika von Schutzzielen und Konsequenzen für Benutzungsschnittstellen". In: *Informatik-Spektrum* 23.3 (2000).

[145] M. Wübbeling, T. Elsner und M. Meier. „Inter-AS routing anomalies: Improved detection and classification“. In: *2014 6th International Conference On Cyber Conflict (CyCon 2014)*. 2014.

[146] M. Wübbeling und M. Meier. „Improved Calculation of AS Resilience against IP Prefix Hijacking“. In: *2016 IEEE 41st Conference on Local Computer Networks Workshops (LCN Workshops)*. 2016.

[147] M. Wübbeling und M. Meier. „Reclaim Your Prefix: Mitigation of Prefix Hijacking Using IPsec Tunnels“. In: *2017 IEEE 42nd Conference on Local Computer Networks (LCN)*. 2017.

[148] Q. Xing, B. Wang und X. Wang. „BGPcoin: Blockchain-Based Internet Number Resource Authority and BGP Security Solution“. In: *Symmetry* 10.9 (2018).

[149] Z. Zhang, Y. Zhang, Y. C. Hu und Z. M. Mao. „Practical Defenses Against BGP Prefix Hijacking“. In: *Proceedings of the 2007 ACM CoNEXT Conference*. New York, New York: ACM, 2007.

[150] Z. Zhang, Y. Zhang, Y. C. Hu, Z. M. Mao und R. Bush. „Ispy: Detecting Ip Prefix Hijacking on My Own“. In: *Proceedings of the ACM SIGCOMM 2008 Conference on Data Communication*. SIGCOMM '08. Seattle, WA, USA: ACM, 2008.

[151] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S. F. Wu und L. Zhang. „An Analysis of BGP Multiple Origin AS (MOAS) Conflicts“. In: *Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement*. IMW '01. San Francisco, California, USA: ACM, 2001.

[152] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S. F. Wu und L. Zhang. „Detection of Invalid Routing Announcement in the Internet“. In: *Proceedings of the 2002 International Conference on Dependable Systems and Networks*. DSN '02. Washington, DC, USA: IEEE Computer Society, 2002.

[153] C. Zheng, L. Ji, D. Pei, J. Wang und P. Francis. „A Light-weight Distributed Scheme for Detecting Ip Prefix Hijacks in Real-time“. In: *Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*. SIGCOMM '07. Kyoto, Japan: ACM, 2007.