Holger Reibold

BGP als kritische Infrastruktur

Warum Routingfehler globale Ausfälle verursachen – und wie man sie beherrscht

BRAIN-MEDIA.DE

Holger Reibold

BGP als kritische Infrastruktur

Warum Routingfehler globale Ausfälle verursachen – und wie man sie beherrscht

BRAIN-MEDIA.DE

ISBN: 978-3-95444-312-3

Cover: Freepik

Druck: Libri Plueros GmbH, Friedensallee 273, 22763 Hamburg

Brain-Media.de – St. Johanner Str. 41-43 – 66111 Saarbrücken

info@brain-media.de – www.brain-media.de

Inhaltsverzeichnis

Epilog – Nähe zur Infrastruktur

Ich arbeite nicht im Maschinenraum des Internets.

Ich sitze auch nicht täglich an Routern oder schreibe Routing-Policies.

Und doch bin ich näher an BGP, als es viele vermuten würden.

Als Key Account Manager bei einem Internet Service Provider bewege ich mich an einer Schnittstelle, die selten als kritisch wahrgenommen wird: zwischen Kundenanforderungen, wirtschaftlichen Rahmenbedingungen und technischer Realität. Genau an dieser Schnittstelle zeigt sich, was BGP tatsächlich ist – und was es nicht ist.

Routing ist für viele Kunden ein abstraktes Versprechen. Konnektivität wird erwartet, Verfügbarkeit vorausgesetzt, Stabilität als gegeben angenommen. Erst wenn etwas nicht mehr funktioniert, rückt das Thema in den Vordergrund. Dann tauchen Fragen auf, die sich erstaunlich ähneln:

Warum ist das passiert?

Warum betrifft uns das, obwohl wir nichts geändert haben?

Warum lässt sich das nicht einfach sofort beheben?

Die ehrliche Antwort ist oft unbequem: Weil globale Konnektivität auf lokalen Entscheidungen basiert, weil Vertrauen ein integraler Bestandteil des Interdomain Routings ist – und weil Fehler sich im Internet nicht linear verhalten. Ein einzelnes falsch angekündigtes Präfix, eine unbedachte Policy-Änderung, ein fehlender Filter kann Auswirkungen entfalten, die weit über den eigenen Verantwortungsbereich hinausgehen.

In Gesprächen mit Kunden, insbesondere mit solchen, die selbst kritische Dienste betreiben, wird deutlich, wie groß die Diskrepanz zwischen Erwartung und Realität ist. Das Internet wird als resilient wahrgenommen, als redundant, als selbstheilend. Und vieles davon stimmt – bis zu einem gewissen Punkt. Doch Resilienz ist kein Naturgesetz. Sie ist das Ergebnis von Designentscheidungen, Betriebserfahrung und koordiniertem Verhalten vieler Akteure. BGP ist dabei kein autonomes System, sondern ein soziales Protokoll: Es funktioniert, weil sich die meisten Beteiligten korrekt verhalten – nicht, weil es sie dazu zwingt.

Gerade in der Rolle eines Key Account Managers wird diese soziale Dimension sichtbar. Routing-Fragen sind selten rein technisch. Sie sind wirtschaftlich motiviert, vertraglich gerahmt, politisch beeinflusst. Wenn Kunden Multi-Homing fordern, erwarten sie Redundanz. Wenn sie Traffic Engineering verlangen, erwarten sie Kontrolle. Wenn sie Ausfälle erleben, erwarten sie Verantwortung – oft unabhängig davon, wo die Ursache tatsächlich liegt.

Diese Nähe zu den Erwartungen auf der einen Seite und zu den technischen Grenzen auf der anderen war einer der Gründe, dieses Buch zu schreiben. Nicht, um BGP zu erklären – das tun andere Werke

ausführlich und besser. Sondern um ein Bewusstsein dafür zu schaffen, dass wir es beim globalen Routing nicht mit einer rein technischen Disziplin zu tun haben, sondern mit einer kritischen Infrastruktur, deren Stabilität von kollektiver Sorgfalt abhängt.

Viele der beschriebenen Probleme sind seit Jahren bekannt. Route Leaks, Hijacks, Instabilitäten, mangelhafte Filter – all das ist kein neues Phänomen. Neu ist jedoch der Kontext: eine zunehmende Abhängigkeit nahezu aller gesellschaftlichen Bereiche vom Internet, eine Verdichtung kritischer Dienste auf IP-basierter Kommunikation und eine steigende Komplexität der Routinglandschaft durch Cloud, CDNs und globale Plattformen.

In dieser Realität reicht es nicht mehr aus, BGP als gegeben hinzunehmen. Es reicht auch nicht, sich auf Best Practices zu berufen, wenn deren Umsetzung freiwillig bleibt. Wer heute Verantwortung für Netze trägt – sei es technisch, organisatorisch oder kaufmännisch –, trägt auch Verantwortung für die Stabilität des Gesamtsystems. Diese Verantwortung beginnt nicht erst beim Incident, sondern bei der täglichen Entscheidung, wie sorgfältig Routing betrieben, dokumentiert, gefiltert und überwacht wird.

Dieses Buch versteht sich als Einladung zur Reflexion. An Betreiber, die im operativen Druck stehen. An Entscheider, die technische Risiken bewerten müssen. Und an alle, die an den Schnittstellen arbeiten, an denen technische Realität auf geschäftliche Erwartungen trifft.

BGP wird bleiben. Nicht, weil es perfekt ist, sondern weil es funktioniert – unter der Voraussetzung, dass wir seine Schwächen kennen und mit

ihnen verantwortungsvoll umgehen. Dieses Bewusstsein zu fördern, ist das Ziel dieses Buches. Und es ist auch der Grund, warum jemand, der täglich mit Kunden spricht, über Routing schreibt.

Nicht aus Distanz zur Technik, sondern aus Nähe zu ihren Konsequenzen.

Viel Vergnügen bei der Reise zu den zentralen Mechanismen des Internets.

Holger Reibold

P.S.: Wer sich im Alltag nicht nur theoretisch, sondern ganz praktisch mit den hier beschriebenen Fragestellungen auseinandersetzen muss, weiß, dass Routing selten ein isoliertes Technikthema ist. Beratung, Design, Betrieb und Incident-Unterstützung greifen ineinander – insbesondere dort, wo BGP geschäftskritisch wird. Die intersaar GmbH bietet genau in diesem Spannungsfeld spezialisierte Dienstleistungen rund um BGP, Interconnection und Routing-Sicherheit an. Weitere Informationen dazu finden Sie unter www.intersaar.de.

.

1 Das Internet als verteilte Infrastruktur

Das Internet wird häufig als etwas Selbstverständliches wahrgenommen. Als Dienst, als Plattform oder als abstrakte „Cloud“, die jederzeit verfügbar ist und zuverlässig funktioniert. In dieser Wahrnehmung verschwindet die eigentliche Struktur des Internets fast vollständig: Es erscheint als homogenes Ganzes, als ein globales System mit klaren Zuständigkeiten und automatischer Resilienz.

Diese Vorstellung ist bequem – und doch ist sie falsch.

Tatsächlich ist das Internet kein einzelnes Netz und keine zentral betriebene Infrastruktur. Es ist das Ergebnis der Zusammenarbeit zehntausender unabhängiger Netzwerke, die sich gegenseitig Konnektivität zusichern, ohne einer übergeordneten Instanz zu unterliegen. Jedes dieser Netzwerke trifft eigene technische, wirtschaftliche und organisatorische Entscheidungen. Dass aus dieser Vielzahl lokaler Entscheidungen eine globale Kommunikationsinfrastruktur entsteht, ist weder selbstverständlich noch garantiert.

Die Stabilität des Internets beruht nicht auf zentraler Kontrolle, sondern auf Dezentralität, Redundanz und gegenseitigem Vertrauen. Diese Eigenschaften haben das Internet skalierbar und erfolgreich gemacht – sie bringen jedoch auch inhärente Risiken mit sich. Fehler, Fehlannahmen oder Fehlkonfigurationen bleiben nicht zwangsläufig lokal begrenzt. Unter bestimmten Umständen können sie sich global auswirken, selbst wenn sie an einer einzelnen Schnittstelle entstehen.

Um zu verstehen, warum Routingfehler globale Ausfälle verursachen können, muss man zunächst verstehen, wie das Internet strukturell aufgebaut ist. Begriffe wie Autonomes System, Transit, Peering oder Redundanz sind dabei keine rein technischen Konzepte. Sie beschreiben zugleich wirtschaftliche Beziehungen, Verantwortlichkeiten und Abhängigkeiten. Das Routing des Internets ist damit immer auch ein Spiegel seiner organisatorischen Realität.

Dieses Kapitel legt das Fundament für alle weiteren Betrachtungen im Buch. Es beschreibt das Internet als verteilte Infrastruktur, erklärt die Rolle autonomer Systeme und zeigt, warum es keine zentrale Steuerung gibt – und auch nie gegeben hat. Erst vor diesem Hintergrund wird verständlich, weshalb das Border Gateway Protocol eine so zentrale Rolle einnimmt und warum seine Schwächen nicht isoliert betrachtet werden können.

Wer BGP als kritische Infrastruktur begreifen will, muss zunächst akzeptieren, dass das Internet kein monolithisches System ist. Es ist ein fragiles Gleichgewicht aus Kooperation, Eigeninteresse und technischem Pragmatismus. Dieses Gleichgewicht zu verstehen ist der erste Schritt, um seine Risiken realistisch einschätzen und verantwortungsvoll mit ihnen umgehen zu können.

1.1 Das Internet als Netzwerk von Netzwerken

Das Internet ist kein einzelnes, zusammenhängendes Netz und auch keine Infrastruktur, die von einer zentralen Stelle geplant, betrieben

oder kontrolliert wird. Vielmehr handelt es sich um ein Netzwerk von Netzwerken: eine lose gekoppelte Gesamtheit tausender unabhängiger Netze, die sich freiwillig miteinander verbinden, um globale Konnektivität zu ermöglichen.

Diese Netzwerke werden als Autonome Systeme bezeichnet. Jedes autonome System steht unter eigener administrativer Kontrolle, verfolgt eigene technische und wirtschaftliche Ziele und entscheidet selbst, mit welchen anderen Netzen es Datenverkehr austauscht. Es gibt keine Instanz, die verbindlich festlegt, wie diese Netze aufgebaut sein müssen oder welche Pfade der Datenverkehr nehmen soll. Die globale Erreichbarkeit des Internets entsteht ausschließlich aus der Summe lokaler Entscheidungen.

Der Begriff „Netzwerk von Netzwerken" beschreibt daher mehr als nur eine technische Topologie. Er steht für ein Organisationsmodell, das auf Dezentralität und Kooperation beruht. Autonome Systeme schließen bilaterale oder multilaterale Vereinbarungen, tauschen Routinginformationen aus und ermöglichen so, dass Datenpakete ihren Weg über zahlreiche Netze hinweg finden. Diese Zusammenarbeit ist in der Regel nicht altruistisch motiviert, sondern folgt klaren wirtschaftlichen Interessen. Transit, Peering und Paid Peering sind Ausdruck dieser Interessen und prägen maßgeblich die Struktur des Internets.

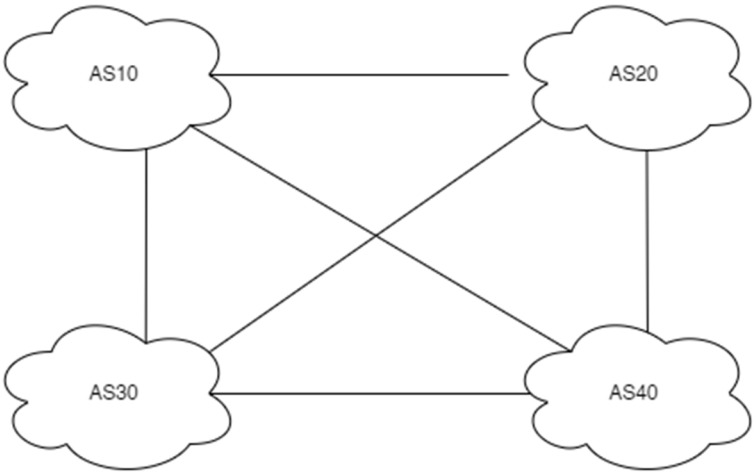
Ein zentrales Merkmal dieses Modells ist die fehlende globale Optimierung. Jedes autonome System optimiert aus seiner eigenen Perspektive: Kosten, Performance, Ausfallsicherheit oder regulatorische Anforderungen. Was für ein einzelnes Netz sinnvoll ist, muss nicht

zwangsläufig zu einem optimalen Gesamtergebnis führen. Dennoch funktioniert das Internet in der Praxis bemerkenswert zuverlässig, weil sich über Jahrzehnte stabile Muster der Zusammenarbeit etabliert haben.

Diese Dezentralität ist eine der größten Stärken des Internets. Sie ermöglicht Skalierbarkeit, Innovation und Resilienz gegenüber lokalen Ausfällen. Gleichzeitig ist sie aber auch die Quelle struktureller Risiken. Da es keine zentrale Instanz gibt, die Routinginformationen validiert oder durchsetzt, basiert die globale Erreichbarkeit auf Vertrauen. Jedes autonome System verlässt sich darauf, dass die von anderen Netzen angekündigten Routinginformationen korrekt sind.

In einem solchen System können Fehler nicht einfach „abgefangen" oder isoliert werden. Wenn ein autonomes System fehlerhafte oder unerwünschte Routinginformationen weitergibt, können diese sich entlang der bestehenden Verbindungen ausbreiten. Je besser ein Netz angebunden ist, desto größer ist potenziell die Reichweite seiner Entscheidungen – unabhängig davon, ob diese absichtlich oder unbeabsichtigt getroffen wurden.

Das Verständnis des Internets als Netzwerk von Netzwerken ist daher essenziell, um die Dynamik von Routingfehlern zu begreifen. Globale Auswirkungen entstehen nicht trotz, sondern wegen der dezentralen Struktur des Internets. Diese Struktur ist kein Mangel, sondern eine bewusste Designentscheidung. Sie macht das Internet leistungsfähig – und zugleich anfällig für systemische Effekte, die nur schwer zentral kontrollierbar sind.



Das Internet als Netzwerk autonomer Systeme mit dezentralen, bilateralen Interconnection-Beziehungen.

1.2 Autonome Systeme als organisatorische Einheiten

Autonome Systeme werden häufig primär als technische Konstrukte verstanden: als nummerierte Einheiten im globalen Routing, identifiziert durch eine ASN und sichtbar in BGP-Tabellen. Diese Sichtweise greift jedoch zu kurz. Ein autonomes System ist vor allem eine organisatorische Einheit, in der technische, wirtschaftliche und strategische Entscheidungen zusammenlaufen.

Formal beschreibt ein autonomes System eine Menge von Routern unter einheitlicher administrativer Kontrolle, die gegenüber der Außenwelt eine konsistente Routing-Policy verfolgt. Entscheidend ist dabei

Literatur- und Quellenverzeichnis

Afanasiev, A., Mohapatra, P., & Zhang, L. (2018). BGP security in partial deployment: Is the juice worth the squeeze? ACM SIGCOMM Computer Communication Review, 48(1), 31–37.

Bush, R., & Austein, R. (2013). The resource public key infrastructure (RPKI) to router protocol (RFC 6810). Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc6810.

Butler, K., Farley, T., McDaniel, P., & Rexford, J. (2010). A survey of BGP security issues and solutions. Proceedings of the IEEE, 98(1), 100–122.

Cisco Systems (2003). BGP student guide (Version 3.0). Cisco Press.

Cisco Systems (n.d.). BGP best practices. https://www.cisco.com.

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., & Polk, W. (2008). Internet X.509 public key infrastructure certificate and CRL profile (RFC 5280). Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc5280.

Gilad, Y., Goldberg, S., Hummon, A., Schapira, M., & Rexford, J. (2017). A survey of interdomain routing security. IEEE Communications Surveys & Tutorials, 19(2), 1071–1095.

Huston, G. (2001). Interconnection, peering, and settlements. Internet Protocol Journal, 4(2), 2–16.

Huston, G. (2020). BGP in 2020. Asia Pacific Network Information Centre (APNIC). https://www.apnic.net.

Kent, S., Lynn, C., & Seo, K. (2000). Secure border gateway protocol (S-BGP). IEEE Journal on Selected Areas in Communications, 18(4), 582–592,

Lepinski, M., & Kent, S. (2012). An infrastructure to support secure Internet routing (RFC 6480). Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc6480.

Lepinski, M., & Kent, S. (2013). Origin validation operation based on the resource public key infrastructure (RPKI) (RFC 6811). Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc6811.

NIST (2018). Cybersecurity framework manufacturing profile (NISTIR 8183). National Institute of Standards and Technology. https://www.nist.gov.

NIST (2020). Securing wireless Internet service provider (WISP) networks (NIST SP 1800-14). National Institute of Standards and Technology.

Norton, W. B. (2014). The Internet peering playbook: Connecting to the core of the Internet. DrPeering Press.

Rekhter, Y., Li, T., & Hares, S. (2006). A border gateway protocol 4 (BGP-4) (RFC 4271). Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc4271.

RIPE NCC (2019). Routing security risk report. https://www.ripe.net

RIPE NCC (2020). RPKI deployment guide. https://www.ripe.net

Tofoni, A., & Luciani, L. (2020). RPKI and route origin validation. RIPE NCC.

Zhang, R., & Bartell, M. (2003). BGP design and implementation. Cisco Press.

Stichwortverzeichnis

E

F

G

H

I

K

L

M

N

O

P

R

S

T

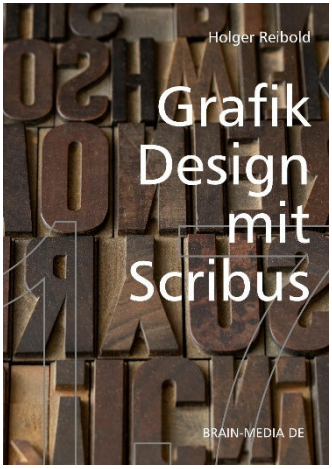
V

W

Y

Z

Mehr von Brain-Media.de



Grafikdesign mit Scribus

In diesem Handbuch erfahren Sie alles, um mit Scribus ein professionelles Projekt umzusetzen – angefangen bei der Entwicklung kreativer Ideen bis zur konkreten Gestaltung.

Preis: 24,99 EUR

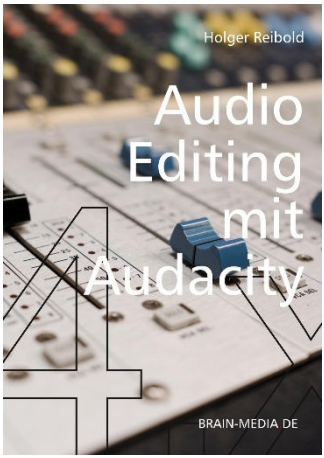
Umfang: 420 Seiten

Virtuelle Maschinen mit VirtualBox 7.x

So verwandeln Sie einen Rechner in ein ganzes Netzwerk oder bauen ein Testumgebung auf. Dieses Handbuch führt Sie in alle wichtigen Funktionen bis hin zur Cloud-Nutzung ein.

Preis: 16,99 EUR

Umfang: 150 Seiten



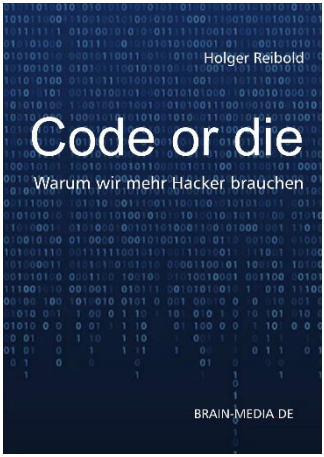
Audio Editing mit Audacity 4.x

Alles Wichtige, was Sie für den erfolgreichen Einsatz des freien Audioeditors wissen müssen.

Umfang: 220 Seiten

Preis: 19,99 EUR

Erscheint: Frühjahr 2026



Code or die – Warum wir mehr Hacker brauchen

Ein Manifest für mehr digitale Selbstbestimmung, Neugierde und Eigenverantwortung. Medienkompetenzen alleine genügen nicht; die Gesellschaft von morgen braucht Digitalkompetenzen.

Umfang: 120 Seiten

Preis: 14,99 EUR

Erscheint Frühjahr 2026

Private KI – KI-Systeme lokal betreiben, kontrollieren und verantworten

Alles Wichtige für den sicheren Einsatz von lokalen KI-Systemen.

Umfang: 160 Seiten

Preis: 16,99 EUR

Erscheint: Frühjahr 2026

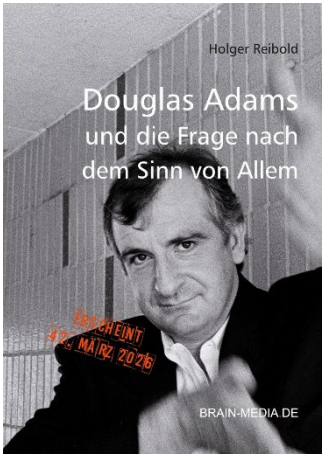
KI Incident Response – Wie man Sicherheitsvorfälle in KI-Systemen erkennt, eindämmt und verantwortet

Ziel- und punktgenaue Reaktionen für kritischen KI-Vorfälle.

Umfang: 220 Seiten

Preis: 16,99 EUR

Erscheint: Frühjahr 2026



42 – Douglas Adams und die Frage nach dem Sinn von Allem

Am 11 Mai 2026 ist Douglas Adams 25 Jahre tot. Der Kultautor hat der Welt wunderbar, skurrile Werke geschenkt. Jetzt ist es an der Zeit, den Autor kennenzulernen.

Umfang: 140 Seiten

Preis: 14,99 EUR

Erscheint: 42. März 2026

Towelday, das ultimative Handtuch für alle Fans

An seinem Todestag, dem Towelday, erinnern sich Fans an Douglas Adams und huldigen dem Kultautor.

100 % intergalaktisch geprüfte Baumwolle, nachhaltig Produktion zum Preis von 42 EUR.

IT-Texter.one

100+ IT-Fachbücher

1500+ Fachartikel

30+ Erfahrung

KOMPLEXE INHALTE PUNKTGENAU AUFZUBEREITEN, IST EINE KUNST. ICH BEHERRSCHE SIE. BEI MIR ERHALTEN SIE FACHTEXTE, DIE KOMPLEXES VERSTÄNDLICH MACHEN.

Seit über 30 Jahren unterstütze ich Unternehmen aus der IT-, Software- und Digitalbranche dabei, ihre technischen Inhalte klar, präzise und zielgruppenorientiert zu kommunizieren. Als promovierter Informatiker und erfahrener IT-Journalist verbinde ich fundiertes Fachwissen mit journalistischem Storytelling. Als Key Account Manager eines IT-Dienstleisters verfüge ich obendrein über konkrete Erfahrungen mit allen gängigen Technologien.

WARUM SIE MIT MIR ARBEITEN SOLLTEN

35 Jahre Erfahrung mit Internet-, Netzwerk- und Webtechnologien

Kooperation mit führenden Akteuren der IT- und Medienbranche

Strategisches Denken: Texte, die nicht nur informieren, sondern auch verkaufen

THEMENSCHWERPUNKTE	WIE KANN ICH SIE UNTERSTÜTZEN
Open-Source	Content Creation
Enterprise IT	Dokumentationen
IT-Consulting	Case Studies
SaaS	Suchmaschinenoptimierung
Künstliche Intelligenz	Tech-Marketing

MEIN VERSPRECHEN

Ich übernehme die inhaltliche und sprachliche Brücke zwischen Technologie und Anwendung. Selbst komplexe Sachverhalte kommen beim Publikum an – fachlich korrekt, prägnant und SEO-wirksam.

PREISMODELLE

Professionelle Leistungen, die ihresgleichen suchen, gibt es nicht umsonst. Sprechen Sie mit an. Gerne vereinbaren wir einen Fixpreis; das vereinfacht Ihre Kalkulation.

KONTAKT AUFNEHMEN

Sprechen wir über Ihr Projekt. Schreibe Sie mir eine Mail (info@it-texter.one). Oder besser noch: Rufen Sie mich an (+49 681 91005698).