



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

Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des Verlags ist es nicht gestattet, das Buch oder Teile daraus in irgendeiner Form durch Fotokopien oder ein anderes Verfahren zu vervielfältigen oder zu verbreiten. Dasselbe gilt auch für das Recht der öffentlichen Wiedergabe. Der Verlag macht darauf aufmerksam, dass die genannten Firmen- und Markennamen sowie Produktbezeichnungen in der Regel marken-, patent- oder warenrechtlichem Schutz unterliegen.

Verlag und Autor übernehmen keine Gewähr für die Funktionsfähigkeit beschriebener Verfahren und Standards.

© 2026 Brain-Media.de

ISBN: 978-3-95444-312-3

Cover: Freepik

Brain-Media.de

Dr. Holger Reibold – Hubert-Müller-Str. 52c – 66113 Saarbrücken

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

Inhaltsverzeichnis

Inhaltsverzeichnis	I
Vorwort	1
1 Das Internet als verteilte Infrastruktur	5
1.1 Das Internet als Netzwerk von Netzwerken	6
1.2 Autonome Systeme als organisatorische Einheiten	9
1.3 Ökonomische und politische Grenzen von Konnektivität	12
1.4 Warum es keine „zentrale Instanz“ gibt	15
1.5 Redundanz, Dezentralität und ihre Grenzen	17
2 Basics des Border Gateway Protocol	21
2.1 Rolle von BGP im Interdomain Routing	23
2.2 Unterschied zwischen IGP und EGP	25
2.3 Pfadvektorprinzip und AS_Path	28
2.4 BGP-Attribute und ihre Bedeutung	32
2.5 Policy-basiertes Routing statt Metriken	36
2.6 Zustandsautomat und Sitzungsaufbau	39
3 Vertrauen als Fundament des Routings	43
3.1 Historische Designziele von BGP	43
3.2 Implizites Vertrauen	46

3.3	Fehlende Authentizität und Integrität	49
3.4	Skalierbarkeit versus Sicherheit	52
3.5	Technische Schulden im globalen Routing	54
4	Typische Fehler- und Störungsklassen	57
4.1	Fehlkonfigurationen im operativen Betrieb.....	57
4.2	Route Leaks und ihre Ursachen.....	60
4.3	Prefix Hijacking	63
4.4	AS-Path-Manipulation	66
4.5	Unbeabsichtigt versus böswillig	68
4.6	Warum BGP Fehler nicht lokal bleiben	70
5	Globale Effekte lokaler Entscheidungen	73
5.1	Verteilung von Routinginformationen	73
5.2	Kaskadeneffekte und Rückkopplungen.....	76
5.3	Die Rolle von Transit-Providern	79
5.4	IXPs als Verstärker oder Puffer.....	81
5.5	Abhängigkeiten durch Cloud und CDNs.....	83
5.6	Zeitverzögerungen und Erkennungsprobleme	84
6	Instabilität, Konvergenz und Nebenwirkungen	87
6.1	Konvergenz im globalen Maßstab	87
6.2	Path Hunting und Routing-Oszillationen	89
6.3	Route Flap Damping – Theorie und Praxis.....	91

6.4	Nebenwirkungen gut gemeinter Mechanismen	93
6.5	Warum Stabilität kein lokales Ziel ist.....	94
7	Routing als Angriffsziel.....	97
7.1	Warum Routing attraktiv für Angreifer ist.....	97
7.2	Umleitung statt Zerstörung.....	100
7.3	Abhören, Manipulation und Blackholing.....	101
7.4	Abgrenzung zu klassischen Cyberangriffen	103
7.5	Attribution und Verantwortung	104
8	Erkennung und Sichtbarkeit von Routingproblemen	107
8.1	Lokale versus globale Sicht	107
8.2	Monitoring-Ansätze und ihre Grenzen.....	109
8.3	False Positives und Fehllarme	110
8.4	Zeitkritische Erkennung.....	112
8.5	Informationsasymmetrien zwischen Akteuren	113
9	Klassische Schutzmaßnahmen	115
9.1	Prefix-Filter und ihre Pflege	115
9.2	AS-Path-Filter	117
9.3	Max-Prefix-Limits.....	118
9.4	Dokumentation und Policy-Disziplin	119
9.5	Grenzen traditioneller Best Practices	120
10	RPKI und Route Origin Validation.....	121

10.1	Motivation und Grundidee von RPKI	121
10.2	Architektur und Vertrauensmodell.....	123
10.3	Route Origin Authorizations	124
10.4	Valid, Invalid und Not Found.....	126
10.5	Einführung im operativen Betrieb.....	127
10.6	Akzeptanzprobleme und Fehlkonfigurationen.....	128
11	Betrieb, Incident Response und Kooperation	131
11.1	Vorbereitung auf Routing-Incidents.....	131
11.2	Reaktionszeiten und Eskalationspfade	132
11.3	Kommunikation mit Kunden und Partnern	133
11.4	Zusammenarbeit in der Internet-Community	134
11.5	MANRS und freiwillige Selbstverpflichtungen.....	135
12	Verantwortung und Governance	137
12.1	Routing als Teil kritischer Infrastruktur	137
12.2	Freiwilligkeit versus Regulierung.....	138
12.3	Nationale und internationale Perspektiven	140
12.4	Verantwortung von Netzbetreibern	141
12.5	Wirtschaftliche Anreize und Zielkonflikte.....	142
13	Die Zukunft des Interdomain Routings	145
13.1	Warum BGP nicht abgelöst wird.....	145
13.2	Evolutionäre Verbesserungen	147

13.3	Technische, organisatorische und kulturelle Hebel	148
13.4	Responsible Routing als Leitbild	149
13.5	Ausblick auf kommende Herausforderungen	150
	Zum Schluss	153
	Glossar	VII
	Literatur- und Quellenverzeichnis	XI
	Stichwortverzeichnis	XIII
	Mehr von Brain-Media.de	XVII
	IT-Texter.one	XXI

Vorwort

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 zu sichern, 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.

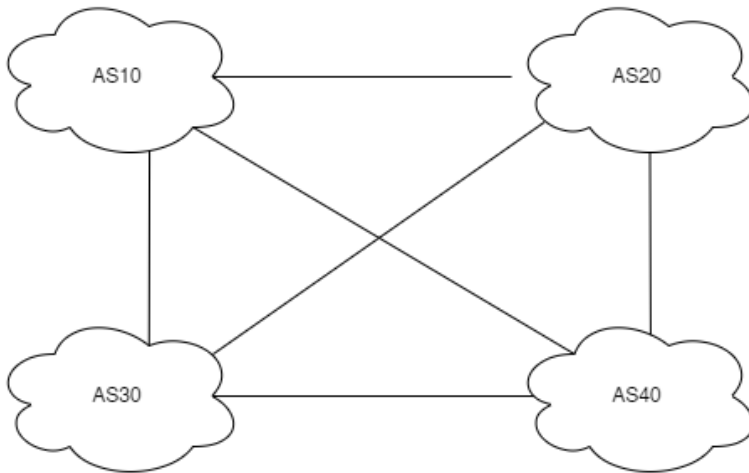
Ein zentrales Merkmal dieses Modells ist die fehlende globale Optimierung. Jedes autonome System optimiert aus seiner eigenen Perspektive: Kosten, Performance, Ausfallsicherheit oder regulatorische Anforderungen. Was für ein einzelnes Netz sinnvoll ist, muss nicht

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

nicht die interne Struktur eines Netzes, sondern seine Rolle im globalen Kontext. Nach außen tritt ein autonomes System als geschlossene Einheit auf, unabhängig davon, wie komplex oder heterogen seine interne Architektur ist.

Diese Abstraktion ist notwendig, um das Internet skalierbar zu halten. Anstatt jede interne Topologie berücksichtigen zu müssen, reduziert BGP die Sicht auf das Wesentliche: Welche Präfixe werden von welchem autonomen System erreicht, und über welche anderen autonomen Systeme führt der Pfad dorthin? Diese Reduktion ermöglicht globale Konnektivität – verschleiert jedoch zugleich interne Abhängigkeiten und Verantwortlichkeiten.

Organisatorisch können autonome Systeme sehr unterschiedlich ausgestaltet sein. Sie reichen von kleinen Unternehmensnetzen mit wenigen Routern bis hin zu globalen Service Providern mit tausenden von Knoten und komplexen internen Strukturen. Auch Internet Exchange Points, Content Delivery Networks oder Cloud-Anbieter agieren über eigene autonome Systeme, oft mit speziellen Routing-Strategien. Gemeinsam ist ihnen, dass sie nach außen als eine administrative Instanz erscheinen, intern jedoch völlig unterschiedliche Entscheidungsprozesse und Reifegrade aufweisen können.

Gerade diese Heterogenität ist ein zentraler Faktor für die Stabilität – und Instabilität – des Internets. BGP macht keinen Unterschied zwischen einem hochautomatisierten Backbone-Netz und einem kleinen, manuell betriebenen AS. Beide sind im globalen Routing gleichberechtigte Teilnehmer. Die Qualität der internen Prozesse, das Maß an operativer

Erfahrung oder die Verfügbarkeit von Ressourcen sind für das Protokoll irrelevant. Ein autonomes System erhält Vertrauen allein durch seine Existenz und seine Konnektivität.

Aus organisatorischer Sicht bedeutet dies, dass technische Entscheidungen im Routing selten rein technisch motiviert sind. Sie werden beeinflusst von Kostenstrukturen, vertraglichen Verpflichtungen, regulatorischen Anforderungen und personellen Ressourcen. Routing-Policies spiegeln daher nicht nur Netzarchitektur wider, sondern auch Geschäftsmodelle und Verantwortlichkeiten. Ein Transit-Anbieter verfolgt andere Ziele als ein Content-Anbieter oder ein Unternehmensnetz – und diese Unterschiede prägen das globale Routingverhalten.

Diese organisatorische Dimension erklärt, warum Routingprobleme oft schwer eindeutig zuzuordnen sind. Wenn fehlerhafte Routen im Internet auftauchen, ist nicht immer sofort klar, ob es sich um einen technischen Fehler, eine Fehlinterpretation einer Policy oder um eine bewusste Entscheidung handelt. Die Grenze zwischen Betrieb und Strategie ist im Routing fließend.

Autonome Systeme sind somit nicht nur technische Bausteine des Internets, sondern dessen institutionelle Akteure. Sie handeln eigenständig, verfolgen eigene Interessen und tragen dennoch Mitverantwortung für die Stabilität des Gesamtsystems. Dieses Spannungsfeld zwischen Autonomie und kollektiver Abhängigkeit ist ein zentrales Merkmal des Internets – und eine wesentliche Voraussetzung dafür, Routing als kritische Infrastruktur zu begreifen.

1.3 Ökonomische und politische Grenzen von Konnektivität

Obwohl das Internet technisch als globales Kommunikationssystem erscheint, ist seine Konnektivität weder grenzenlos noch ausschließlich technisch bestimmt. Tatsächlich wird der Datenverkehr im Internet maßgeblich durch wirtschaftliche und politische Rahmenbedingungen geprägt. Diese Faktoren setzen klare Grenzen dafür, welche Verbindungen existieren, wie stabil sie sind und unter welchen Bedingungen sie genutzt werden dürfen.

Aus wirtschaftlicher Sicht ist Konnektivität ein Produkt. Netzbetreiber investieren in Infrastruktur, Bandbreite, Redundanz und Betrieb, um Erreichbarkeit anbieten zu können. Der Austausch von Datenverkehr zwischen autonomen Systemen folgt daher in der Regel vertraglichen Vereinbarungen. Transit-Verträge, Peering-Abkommen oder kostenpflichtige Interconnection-Modelle bestimmen, welche Routen akzeptiert, weitergegeben oder bevorzugt werden. BGP dient dabei als technisches Instrument zur Umsetzung dieser Geschäftsbeziehungen.

Diese ökonomische Realität hat unmittelbare Auswirkungen auf das Routing. Nicht jeder technisch mögliche Pfad ist auch wirtschaftlich gewollt. Routing-Policies spiegeln Kostenstrukturen wider: Verkehr wird über bestimmte Pfade gelenkt, weil sie günstiger, vertraglich vereinbart oder strategisch sinnvoll sind. Umgekehrt werden andere Pfade bewusst ausgeschlossen, selbst wenn sie aus technischer Sicht kürzer oder performanter wären. Globale Konnektivität ist daher das Ergebnis

zahlreicher bilateraler Entscheidungen, nicht einer globalen Optimierung.

Neben wirtschaftlichen Faktoren spielen politische und regulatorische Rahmenbedingungen eine zunehmend wichtige Rolle. Nationale Gesetzgebungen, Exportkontrollen, Sanktionsregime oder Vorgaben zur Datenhoheit beeinflussen, mit welchen Partnern Netzbetreiber zusammenarbeiten dürfen und wie Datenverkehr geroutet wird. In manchen Regionen führen staatliche Eingriffe zu einer bewussten Segmentierung des Internets, etwa durch Filterung, Traffic-Steuerung oder Vorgaben zur lokalen Datenverarbeitung.

Diese politischen Eingriffe sind für das Routing zunächst unsichtbar, da BGP keine Informationen über die Motivation hinter einer Routing-Policy transportiert. Für das Protokoll sind alle Entscheidungen gleichwertig, unabhängig davon, ob sie aus wirtschaftlichen, technischen oder politischen Gründen getroffen wurden. Die Konsequenzen können jedoch global spürbar sein, etwa wenn Verkehrsströme umgeleitet oder bestimmte Pfade dauerhaft ausgeschlossen werden.

Die Kombination aus wirtschaftlichen Interessen und politischen Vorgaben führt dazu, dass Konnektivität immer kontextabhängig ist. Sie ist das Ergebnis von Verhandlungen, Kompromissen und Machtverhältnissen zwischen autonomen Systemen. Dabei entstehen asymmetrische Abhängigkeiten: Große Netzbetreiber oder Plattformen verfügen über mehr Verhandlungsmacht und können Routing-Entscheidungen stärker beeinflussen als kleinere Akteure. Diese Asymmetrien prägen die Topologie des Internets ebenso wie seine Anfälligkeit für Störungen.

Vor diesem Hintergrund wird deutlich, dass technische Resilienz allein nicht ausreicht, um stabile Konnektivität zu gewährleisten. Selbst ein redundant ausgelegtes Netz kann von Entscheidungen betroffen sein, die außerhalb des eigenen Einflussbereichs liegen. Routingfehler oder -änderungen sind daher nicht immer das Ergebnis technischer Mängel, sondern häufig Ausdruck wirtschaftlicher oder politischer Dynamiken.

Das Verständnis dieser Grenzen ist entscheidend, um Routingprobleme realistisch einzuordnen. Globale Ausfälle oder unerwartete Verkehrswege sind selten rein technische Phänomene. Sie entstehen an der Schnittstelle von Technik, Wirtschaft und Politik – genau dort, wo das Internet als kritische Infrastruktur besonders verletzlich ist.

Exkurs: Pakistan Telecom und YouTube (2008)

Im Jahr 2008 versuchte die pakistanische Regierung, den Zugang zu YouTube innerhalb des Landes zu sperren. Pakistan Telecom setzte hierzu ein klassisches Verfahren ein: Sie kündigten intern eine spezifischere Route für das YouTube-Netzwerk an, die ins „Nichts“ (Blackhole) führte.

Der fatale Fehler: Diese spezifischere Route wurde versehentlich an den internationalen Transit-Provider PCCW weitergegeben. Da BGP den spezifischeren Pfad (Longest Prefix Match) gegenüber der legitimen, aber allgemeineren Ankündigung von YouTube bevorzugte, wurde innerhalb weniger Minuten ein Großteil des weltweiten YouTube-Traffics nach Pakistan geleitet – wo er einfach verworfen wurde. YouTube war

weltweit für mehrere Stunden nicht erreichbar. Dieser Fall ist das Paradebeispiel dafür, wie politische Eingriffe durch BGP-Fehler globale Konnektivität zerstören können.

1.4 Warum es keine „zentrale Instanz“ gibt

Angesichts der zentralen Bedeutung des Internets liegt die Annahme nahe, es müsse eine übergeordnete Instanz geben, die den Betrieb steuert, Fehler korrigiert oder im Krisenfall eingreift. Diese Vorstellung entspricht vertrauten Modellen aus anderen Infrastrukturen wie die Energieversorgung, den Luftverkehr oder die Telekommunikation. Für das Internet – und insbesondere für das globale Routing – trifft sie jedoch nicht zu. Es gibt keine zentrale Stelle, die entscheidet, wie Daten im Internet geroutet werden. Es existiert weder eine globale Leitwarte noch eine Autorität, die Routinginformationen verbindlich prüft oder durchsetzt. Diese Abwesenheit ist kein Versäumnis, sondern eine bewusste Designentscheidung, die tief in der Entstehungsgeschichte des Internets verankert ist.

Das Internet wurde von Anfang an als dezentrales System konzipiert. Ziel war es, Kommunikation auch dann aufrechtzuerhalten, wenn einzelne Netze oder Verbindungen ausfallen. Eine zentrale Steuerung hätte diesem Ziel widersprochen, da sie selbst einen Single Point of Failure dargestellt hätte. Stattdessen wurde auf verteilte Intelligenz gesetzt: Jedes Netz trifft eigenständig Entscheidungen, basierend auf den Informationen, die es von seinen Nachbarn erhält.

Institutionen wie die IANA, regionale Internet-Registries oder Standardisierungsgremien werden in diesem Zusammenhang häufig missverstanden. Sie vergeben Ressourcen wie IP-Adressräume oder AS-Nummern und entwickeln technische Standards, greifen jedoch nicht in den operativen Routingbetrieb ein. Sie besitzen weder die technische Möglichkeit noch das Mandat, Routingfehler zu verhindern oder zu korrigieren. Ihre Rolle ist koordinierend, nicht steuernd.

Auch das Border Gateway Protocol selbst sieht keine zentrale Kontrollinstanz vor. BGP basiert auf dem Prinzip, dass jedes autonome System die von anderen Systemen erhaltenen Routinginformationen grundsätzlich akzeptiert und auf Basis eigener Policies weiterverarbeitet. Es gibt keine globale Validierung, keinen verbindlichen Abgleich mit einer „richtigen“ Sicht auf das Internet. Konsistenz entsteht allein durch Konvergenz, nicht durch Autorität.

Diese Struktur hat weitreichende Konsequenzen. Zum einen macht sie das Internet außergewöhnlich skalierbar. Neue Netze können sich anschließen, ohne Genehmigungen einzuholen oder zentrale Anpassungen zu erfordern. Zum anderen bedeutet sie, dass die Verantwortung fragmentiert ist. Jeder Netzbetreiber ist für seine eigenen Entscheidungen verantwortlich, aber niemand ist für das Gesamtsystem zuständig.

In der Praxis führt dies zu einem Spannungsfeld zwischen Autonomie und Abhängigkeit. Ein einzelnes autonomes System kann globale Auswirkungen haben, ohne über globale Verantwortung oder Einsicht zu verfügen. Umgekehrt können betroffene Netze keine zentrale Stelle anrufen, um fehlerhafte Routen „abschalten“ zu lassen. Korrekturen

erfolgen indirekt, durch Kommunikation, Koordination und – im besten Fall – Kooperation zwischen den beteiligten Akteuren.

Die fehlende zentrale Instanz ist damit Stärke und Schwäche zugleich. Sie ermöglicht Offenheit, Innovation und Widerstandsfähigkeit gegenüber zentralen Ausfällen. Gleichzeitig erschwert sie gezielte Eingriffe und systematische Absicherung. Routingprobleme lassen sich nicht einfach eskalieren oder delegieren; sie müssen im verteilten System selbst gelöst werden.

Dieses Verständnis ist entscheidend für die Bewertung von Routingrisiken. Wer nach einer zentralen Lösung sucht, verkennt die grundlegende Architektur des Internets. Stabilität entsteht nicht durch Kontrolle von oben, sondern durch verantwortungsvolles Handeln vieler unabhängiger Akteure. Genau darin liegt die besondere Herausforderung – und Verantwortung – des Interdomain Routings.

1.5 Redundanz, Dezentralität und ihre Grenzen

Redundanz und Dezentralität gelten als die zentralen Erfolgsfaktoren des Internets. Sie prägen sowohl die technische Architektur als auch das Selbstverständnis vieler Netzbetreiber. Mehrfache Anbindungen, alternative Pfade und die Abwesenheit zentraler Steuerung werden häufig als Garant für Ausfallsicherheit und Stabilität betrachtet. Tatsächlich haben diese Prinzipien maßgeblich dazu beigetragen, dass das Internet trotz seines Wachstums und seiner Komplexität über Jahrzehnte funktionsfähig geblieben ist.

Redundanz bedeutet jedoch nicht automatisch Resilienz. Zusätzliche Verbindungen und alternative Routen erhöhen zwar die Anzahl möglicher Pfade, garantieren aber nicht, dass diese im Fehlerfall sinnvoll genutzt werden. Im globalen Routing entscheidet nicht allein die physische Topologie über den Datenfluss, sondern die Gesamtheit der Routing-Policies aller beteiligten autonomen Systeme. Eine physisch redundante Anbindung kann wirkungslos sein, wenn sie durch Policies ausgeschlossen oder im Fehlerfall nicht korrekt beworben wird.

Dezentralität verstärkt diesen Effekt. Da jedes autonome System eigenständig entscheidet, welche Routen es annimmt, bevorzugt oder weitergibt, existiert keine Garantie, dass alternative Pfade im Ernstfall verfügbar sind. Redundanz ist damit immer relativ: Sie existiert nur innerhalb der Grenzen der jeweils geltenden wirtschaftlichen, technischen und organisatorischen Rahmenbedingungen. Was aus lokaler Sicht redundant erscheint, kann global betrachtet ein Engpass sein. Hinzu kommt, dass Redundanz häufig aus Kostengesichtspunkten asymmetrisch umgesetzt wird. Viele Netze verfügen über mehrere Upstreams, nutzen diese jedoch nicht gleichwertig. Primäre und sekundäre Anbindungen werden bewusst unterschiedlich priorisiert, um Kosten zu optimieren. In solchen Szenarien ist Redundanz zwar vorhanden, aber nicht neutral. Im Störfall kann es zu unerwarteten Verkehrsverschiebungen kommen, die zusätzliche Belastungen oder neue Abhängigkeiten erzeugen.

Dezentralität erschwert zudem die Koordination im Fehlerfall. Während zentrale Systeme gezielt umkonfiguriert oder gesteuert werden können, müssen im Internet viele unabhängige Akteure parallel reagieren. Die

Konvergenz auf einen stabilen Zustand benötigt Zeit, und während dieser Phase können temporäre Instabilitäten auftreten. Redundanz sorgt in solchen Situationen nicht zwangsläufig für Ruhe, sondern kann durch zusätzliche Pfadoptitionen sogar zu verstärkter Dynamik führen.

Ein weiterer limitierender Faktor ist die Sichtbarkeit. Kein einzelner Netzbetreiber hat einen vollständigen Überblick über alle verfügbaren Alternativpfade oder deren aktuelle Nutzung. Entscheidungen werden auf Basis lokaler Informationen getroffen, die im globalen Kontext unvollständig oder verzögert sein können. Redundanz entfaltet ihren Nutzen daher nur, wenn sie mit ausreichender Transparenz und operativer Disziplin kombiniert wird.

Die Grenzen von Redundanz und Dezentralität zeigen sich besonders deutlich bei großflächigen Routingproblemen. In solchen Fällen versagen nicht einzelne Verbindungen, sondern ganze Pfadklassen oder Policy-Kombinationen. Alternative Routen existieren zwar theoretisch, sind jedoch praktisch nicht nutzbar oder führen zu weiteren Instabilitäten. Das System reagiert nicht linear, sondern komplex und teilweise unvorhersehbar. Redundanz und Dezentralität sind somit notwendige, aber nicht hinreichende Voraussetzungen für stabile Konnektivität. Sie bilden das Fundament des Internets, ersetzen jedoch nicht verantwortungsbewussten Betrieb, saubere Policies und koordiniertes Handeln. Wer sich allein auf technische Vielfalt verlässt, unterschätzt die systemischen Risiken des globalen Routings. Dieses Spannungsfeld markiert den Übergang von der strukturellen Beschreibung des Internets zur Rolle des Border Gateway Protocols.

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

7

768k Day 89

A

Abhören 101

Angriffsvektor..... 98

Angriffsziel..... 97

AS_Path 28

AS-Nummer 30

AS-Path-Filter 117

AS-Path-Manipulation 66

AS-Path-Prepending 31, 66

Asynchronität..... 85

Attribution 104

Ausfallsicherheit 7

Authentizität 49

Automatisierung 93

Autonomes System 6, 7, 9

B

Backbone 10

Best Practices 120

BGP..... 10

BGP Fehler 70

BGP-Attribute..... 32

Blackhole..... 64

Blackholing 102

Border Gateway Protocol..... 6, 21

C

CDN 83

Change-Management..... 119

Cloud 5, 83

Content Delivery Network..... 10

Cyberangriff 103

D

Denial-of-Service 98

Designfaktor..... 45

Designziele..... 43

Dezentrales System..... 15

Dezentralität..... 5, 8, 18

Dokumentation 119

Dynamik 45

E

EGP	26, 44
Erkennung	112
Erkennungsproblem	84
Erreichbarkeit	21
Eskalationspfad	132
Export-Policy	74
Exterior-Gateway-Protokoll	26

F

Facebook.....	60
False Positive.....	110
Fehleranfälligkeit.....	58
Fehlkonfiguration.....	58
Filter	82
Flapping	41
Freiwilligkeit	138

G

Globales Routing	55
Governance	140
Grundlagen.....	22

H

Hebelwirkung	97
Heuristik.....	110
Hijack	49

I

IANA	16, 123
IGP	25
Incident Response	131
Informationsasymmetrie	113
Infrastruktur	6
Infrastrukturkonflikt	53
Integrität.....	50
Interdomain Routing	23, 145
Interior-Gateway-Protokoll	25
Internet	5
Internet Exchange Point.....	10, 81
IXP	81

K

Kaskadeneffekt.....	76
KEEPALIVE	40
Kommunikation	133
Konvergenz	87
Koordinator	25
Kosten	7
Kritische Infrastruktur.....	6

L

LOCAL_PREF	33
------------------	----

M

Manipulation	102
MANRS	135
Max-Prefix-Limit.....	118
MED	33
Mesh	44
Meta	60
Metrik.....	21
Metrikenbasiertes Routing	38
Monitoring.....	109
MTU	41
Multi-Exit Discriminator.....	33
Mutually Agreed Norms for Routing Security	135
MyEtherWallet.....	99

N

Netzbetreiber.....	12, 141
Netzwerk von Netzwerken.....	6
Next Hop.....	32
NEXT_HOP.....	33

O

Organisation.....	11
ORIGIN	34

P

Pakistan Telecom.....	14
Path Hunting	89
PCCW.....	14
Peering	6
Performance.....	7
Pfadvektorprinzip.....	28
Pfadwahl	32
Policy-Anpassung.....	58
Policy-basiertes Routing	36
Präfix	32
Prefix	68
Prefix Hijacking	63
Prefix-Filter.....	115

R

Redundanz	5, 6, 17
Regulierung.....	139
Responsible Routing	149
RFD	91
RIPE RIS.....	108
ROA	124
Route Flap Damping.....	91
Route Leak	60
Route Origin Authorization.....	124
Route Origin Validation.....	51, 126
Routing-Entscheidung.....	13
Routingfehler	6, 8, 49

Routinginformation	8, 24
Routing-Loop.....	30
Routing-Oszillation	91
Routing-Policy	9, 12
Routingproblem	11
Routingrisiko	17
RPKI.....	51, 82, 121
Rückkopplung.....	77

S

Schutzmaßnahme	115
Sicherheit.....	45, 52
Sichtbarkeit.....	19
Sitzungsaufbau	39
Skalierung.....	52
Stabilität.....	5, 45, 94

T

TCP	40
TCP-Reset	41
Timer.....	40
Topologie.....	7, 21
Topologiesicht.....	44
Traceroute	109
Traffic Engineering	94
Transit.....	6

Transit-Provider.....	79U
Umleitung	100
Update.....	42
UPDATE.....	40

V

Validator.....	124
Valley-Free	61
Verteilsystem	23
Verteilung.....	73
Vertrauen	5, 43
Vertrauensmodell	46

W

Weitergabe.....	47
Withdraw.....	42, 74

Y

YouTube.....	14
--------------	----

Z

Zeitverzögerung.....	84
Zusammenarbeit	134
Zustandsautomat.....	39

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



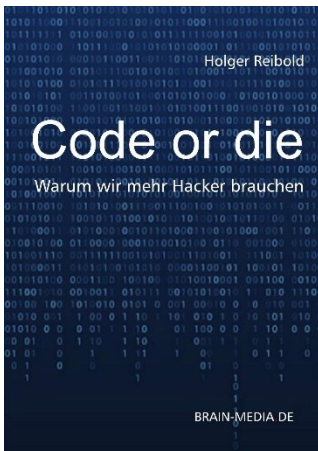
Audio Editing mit Audacity 4.x

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



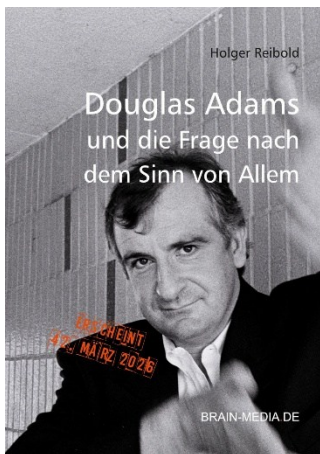
KI Incident Response – Wie man Sicherheitsvorfälle in KI-Systemen erkennt, eindämmt und verantwortet

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 FACH-TEXTE, 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).