Das „Schengen-Routing“ zu Ende gedacht

Direktvermittlung

Norbert Pohlmann, Illya Siromaschenko, Michael Sparenberg

Die Telekom hat als Antwort auf die NSA-Schnüffeleien ein „nationales Routing“ ins Spiel gebracht, damit die Daten Deutschland nicht verlassen müssen. Realistische Alternative oder populistische Effekthascherei?

Einer allseits bekannten Metapher zufolge ist das Internet ein globales Dorf, in dem der Rest der Welt nur einen Mausklick entfernt liegt. Die schnelle und einfache Überwindung räumlicher Distanzen hat zusammen mit der kostengünstigen Nutzung den Siegeszug des Mediums begründet. Das Internet hat zudem die Ansprüche an Kommunikationsmedien neu definiert. Es bietet scheinbar unbegrenzte Verfügbarkeit und verbirgt die Komplexität des globalen Netzwerks hinter anwenderfreundlichen Lösungen. In welcher Form die Daten übertragen werden und welchen Weg sie nehmen, schien in Anbetracht der transparenten Funktionsweise bislang belanglos zu sein.

Doch dann legten die Enthüllungen des Whistleblowers Edward Snowden umfangreiche Abhörpraktiken offen, und die Frage des Datentransports wurde zum Politikum. Trotz verbaler Deeskalation hält die US-Regierung ihr Handeln zum Schutz amerikanischer Interessen für gerechtfertigt und lässt bisher wenig Bereitschaft erkennen, davon abzurücken. Zwar gab es international durchaus unterschiedliche Reaktionen auf die Aktivitäten der amerikanischen NSA und des britischen GCHQ, in der deutschen Öffentlichkeit fiel die Missbilligung jedoch besonders deutlich aus. Die Ausspähung des Datenverkehrs durch ausländische Geheimdienste wird nahezu einhellig als Rechts- und Vertrauensbruch bewertet, dem mit geeigneten Mitteln zu begegnen sei. Das wirft die Frage nach adäquaten Maßnahmen auf, mit denen deutsches und europäisches Recht wirksam durchgesetzt werden kann.

Die Deutsche Telekom hat im Zuge der aktuellen Diskussion den Vorschlag unterbreitet, gesetzliche Verpflichtungen für das Routing des Internetverkehrs einzuführen (siehe „Alle Links“). Diese unter Stichworten wie „DE-Routing“ oder „Schengen-Netz“ diskutierten Ideen bezeichnen im Kern ein regional begrenztes Routing von Datenverkehr im nationalen oder europäischen Raum. Das soll Abhörmaßnahmen ausländischer respektive außereuropäischer Akteure verhindern oder wenigstens wesentlich erschweren sowie den Schutz persönlicher Daten und die Abwehr von Wirtschaftsspionage auf Transportebene verbessern.

Weltweit Gedankenspiele zum Routing

Überlegungen, den innerstaatlichen Datenverkehr nicht über Drittländer abzuwickeln, sind weder auf Europa beschränkt noch neu. Brasilien strebt nach den Überwachungsenthüllungen an, lokale Telekommunikationsstrukturen enger an eigene Dienste zu koppeln, etwa durch einen eigenständigen, abhörsicheren E-Mail-Dienst. Unternehmen wie Facebook und Google sollen künftig Daten brasilianischer Kunden ausschließlich auf Servern innerhalb des Landes speichern. Durch neue Seekabel will man hierfür Routing-Lösungen bieten, die schwerer abzuhören sind und die Abhängigkeit von US-amerikanischer Infrastruktur verringern. Und an der University of Toronto diskutierte man schon vor den Snowden-Enthüllungen, ob man nicht das „Boomerang Routing“, also das Umleiten kanadischen Traffics über US Ex-

change Points, eindämmen könne („Alle Links“).

In beiden Fällen wird eine mehrgliedrige Strategie vorgeschlagen, die den gesetzlichen Schutz der Daten durch Erweiterung bestehender Gesetze stärken soll, wofür das innerstaatliche Netz durch die Errichtung neuer Exchange Points ausgebaut werden soll.

Globaler Datentransport

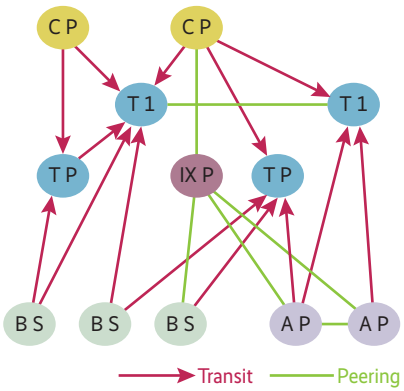
Um diese Ideen besser beurteilen zu können, ist ein Exkurs zu den Grundlagen des Datentransports im Internet nötig. Physisch gesehen, stellt das Internet einen Zusammenschluss von gegenwärtig etwa 50 000 einzelnen Teilnetzen dar, als autonome Systeme (kurz: AS) bezeichnet und als organisatorische Einheit vom jeweiligen Betreiber autark verwaltet. Durch die gegenseitige Anbindung autonomer Systeme und standardisierte Transportmechanismen lassen sich Daten global zwischen beliebigen Endpunkten im Internet austauschen.

Ein autonomes System ist ein IP-Netz aus Routern und Teilnetzen und untersteht einer einzigen administrativen Instanz. Diese IP-Netze, die sich in Größe und räumlicher Ausdehnung immens unterscheiden, handeln autark, das heißt, sie werden unabhängig voneinander betrieben und verwaltet. Das bedeutet auch, dass sie eine unabhängige Strategie haben, wie sie mithilfe von Routing-Protokollen die Kommunikation der Pakete in ihrem Netz organisieren.

Damit nun ein autonomes System vollständig und redundant in das Verbundnetz Internet integriert ist, sorgt der Betreiber für möglichst viele unterschiedliche Verbindungen zu anderen autonomen Systemen. Dabei verfolgt jeder AS-Provider unterschiedliche Strategien, abhängig vom Kerngeschäft des Unternehmens und der Größe und Ausdehnung des autonomen Systems.

Unterschieden wird dabei zwischen zwei grundlegenden Verbindungstypen: Transit und Peering. Regional begrenzte AS sind auf Verbindungen zu großen nationalen und globalen Transit-Providern angewiesen, um am Internet teilnehmen zu können. In diesem Fall schließt ein regionaler Provider ein Transit-Abkommen mit einem Provider nationaler, europäischer oder globaler Ausdehnung ab. Dabei zahlt er für den „Upstream“, sein gesendetes Datenvolumen.

Anders bei einer Peering-Vereinbarung, bei der zwei Provider verabreden, kostenneutral Daten zwischen ihren Netzen auszutauschen. Hierbei handelt es sich um ein sogenanntes Private Peering. Beim Peering wird nur der Verkehr der autonomen Systeme selbst und der Kunden des AS ausgetauscht. Ein autonomes System erlaubt im Regelfall keinen Durchgangsverkehr von einem Peering-Partner zu seinem Transit-Provider. Diese Einstellungen können die Provider vorab durch Richtlinien (Policies) beim Routing festlegen.



Autonome Systeme können verschiedene Rollen einnehmen: Content Provider (CP), Transit Provider (TP), Tier One Provider (T1), Access Provider (AP), Business Customer (BS) und mittendrin die Internet Exchange Points (IXP) (Abb. 1).

Das Zustandekommen einer Peering-Vereinbarung ist abhängig von vielen Faktoren, und die Provider gehen mit unterschiedlichsten Standpunkten in die Verhandlungen. Dabei versuchen sie ihre eigene Größe und Stärke zu nutzen. Die entscheidende Frage lautet wie immer: „Wer bezahlt wen?“ Die Provider möchten für möglichst geringe Kosten eine hochwertige Dienstleistung für ihre Kunden erbringen. Das Peering ist dabei meist eine Vereinbarung von Partnern auf Augenhöhe. Andererseits ist es auch möglich, dass große Provider mit kleineren Providern peeren, wenn sie sich einen wirtschaftlichen Vorteil durch dieses Abkommen erhoffen. Zur Absicherung existieren in den Peering-Verträgen meist Vereinbarungen über maximale Datenvolumen.

Auch beim Peering geht es um Geld

Eine andere Möglichkeit ist ein Peering an einem Internet Exchange Point (IXP) wie dem DE-CIX oder anderen regionalen und internationalen Internet-Austauschpunkten. Hier spricht man von einem Public Peering. Beim Public Peering können mehrere Peering-Vereinbarungen über nur eine physische Anbindung am Internet Exchange Point erstellt werden.

Die erwähnten 50 000 autonomen Systeme bilden über mehr als 500 000 Verbindungen gemeinsam das Internet. Für eine genauere Betrachtung der Verbundstruktur ist auch die Rolle der jeweiligen autonomen Systeme im Zusammenspiel des Internetverbunds bedeutsam.

Bei der im Folgenden dargestellten Klassifizierung in fünf Grundtypen ist zu beachten, dass ein autonomes System auch mehrere Rollen annehmen kann:

Global Tier One Provider (T1) sind die weltweit größten IP Carrier, zum Beispiel Verizon, AT&T, Sprint, Level 3 und Deutsche Telekom.

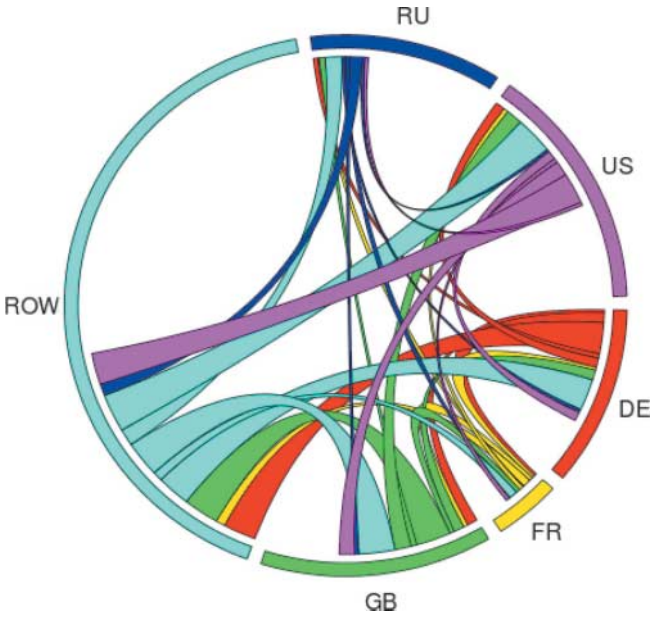
Transit Provider (TP) sind solche, die wenig bis keine direkten Internetkunden haben. Sie bieten Upstreams für Access Provider (AP), Content Provider (CP) und Business Customer AS (BS), betreiben zumeist Peerings mit anderen Transit Providern und haben einen Upstream zu den großen Global Tier One Providern. Transit Provider, die für Deutschland eine besondere Rolle spielen, sind die Deutsche Telekom und Lambdanet.

Access Provider (AP) oder sogenannte Eyeball ISPs sind autonome Systeme, die meist Haushalte und kleine Unternehmen ans Internet anschließen. Beispiele hierfür in Deutschland sind die Deutsche Telekom, Kabel Deutschland, Vodafone und Telefonica.

Content Provider (CP) stellen Webinhalte oder Streaming Services bereit, sei es durch das Hosten privater Webseiten oder durch das Betreiben eines stark frequentierten Onlineportals – etwa

X-TRACT

- Als Reaktion auf die NSA- und GCHQ-Aktivitäten hat unter anderem die Telekom gesetzliche Regelungen für ein nationales Routing vorgeschlagen.
- Ein regionales resp. nationales Routing verteuert das Internet, verhindert aber nicht grundsätzlich den unautorisierten Zugriff.
- Zielführender wäre eine weitreichende Verschlüsselung des IP-Verkehrs.



Dominanz der Big 5: Russland, die USA, Deutschland, Frankreich und Großbritannien generieren mehr Datenverkehr als alle anderen Staaten der Welt zusammen (Abb. 2).

Facebook, Microsoft, Google, eBay, Hetzner, STRATO und Host Europe.

Business Customer AS (BS) sind in der Regel große Unternehmen, die ein eigenes autonomes System betreiben. Hier geht es mehr um die ökonomische Bedeutung der Verbindungen als um das Volumen des Datentransfers. Typische Business Customer AS in Deutschland sind die Deutsche Bank, Lufthansa, Allianz, BASF, Siemens, DATEV, Volkswagen, Metro und RWE.

Eine zentrale Rolle spielen ferner die sogenannten Internet Exchange Points (IXP). Sie dienen als Austauschknoten für den Datenverkehr zwischen autonomen Systemen verschiedener Großräume. Sie sollen typischerweise die Abhängigkeit von Upstream-Providern reduzieren sowie Effizienz und Fehlertoleranz steigern. Größter deutscher Austauschpunkt ist der DE-CIX (Deutscher CIX/Commercial Internet Exchange) in Frankfurt am Main.

Systeme nach ihren Rollen

Staat/Rolle	AS	AP	BS	CP	TP
Argentinien	283	20	5	18	9
Australien	1070	89	941	92	57
Brasilien	1919	57	1877	76	57
China	259	87	197	65	32
Deutschland	**1484**	**127**	**1040**	**246**	**316**
Frankreich	909	72	654	135	175
Großbritannien	1626	97	1085	206	370
Indonesien	554	13	344	44	50
Indien	580	43	520	30	24
Italien	700	45	509	95	126
Japan	559	174	420	117	44
Kanada	938	145	868	118	34
Mexiko	181	53	167	12	8
Russische Föderation	4716	151	3286	192	726
Saudi-Arabien	102	11	69	3	12
Südafrika	162	35	145	14	12
Südkorea	685	110	632	36	27
Türkei	400	23	333	48	24
USA	15631	1733	14855	976	445
G20 gesamt	32758	3085	27947	2523	2548
Übrige Staaten	17646	1051	14043	1385	2302
Global gesamt	50404	4136	41990	3908	4850

AS: Autonome Systeme, AP: Access Provider, BS: Business Customer, CP: Content Provider, TP: Transit Provider

Unterschiedliche Kategorien

Ein Beispiel für die oben erwähnte Mehrfachrolle stellt die Deutsche Telekom dar, die gleichzeitig Tier 1, AC, CP und TP ist. Die meisten AS im Internet sind Business Customer.

Das am if(is), dem Institut für Internet-Sicherheit, von den Autoren mitentwickelte Internet-Kennzahlen-System (IKS) führt kontinuierliche Messungen der wichtigsten technischen Parameter des Internets durch [1]. Aus der Vielzahl von Messwerten werden spezifische Kennzahlen berechnet, die komplexe Zusammenhänge erkennbar machen und langfristige Entwicklungen aufzeigen. Allein im Bereich der Internet-Infrastruktur erhebt das if(is) jährlich gut 100 Millionen Kennwerte.

In der Tabelle „Regionale Kategorisierung“ ist die Verteilung 436 363 öffentlich sichtbarer Verbindungen zwischen den autonomen Systemen der jeweiligen Länder dargestellt. Ein AS wird dabei dem Land zugeordnet, in dem sich der größte Anteil der an das AS vergebenen IP-Adressen befindet.

Rund die Hälfte aller globalen Verbindungen entfällt auf die Mitgliedsstaaten der G20. Innerhalb dieser Gruppe entfallen wiederum rund 70 % der Verbindungen auf die Schwergewichte USA, Russland, Großbritannien, Deutschland und Frankreich. Diese fünf Staaten nehmen in Bezug auf die globale Vernetzung eine dominante Stellung ein. Die „Big 5“ des Internets kontrollieren die weltweite Infrastruktur des Datenverkehrs, an der Deutschland mit gegenwärtig knapp 1500 autonomen Systemen aktiv beteiligt ist.

Um die Auswirkungen eines verbindlichen Inlandsroutings abschätzen zu können, wurden die Verbindungen zwischen deutschen AS unter der Fragestellung analysiert, welche davon vermutlich gegenwärtig die Daten über ausländische autonome Systeme schicken. Die nachfolgende Abbildung zeigt den (geschätzten) Anteil der Verbindungen zwischen deutschen AS, bei denen Datenpakete nicht vollständig über inländische autonome Systeme transportiert werden.

Bei einer Routing-Simulation wurde die Shortest-Path-Strategie angewandt und eine Gleichverteilung der Nutzung aller direkten Verbindungen angenommen. In der Simulation wurden die aktuelle Quality of Service (Bandbreite, Verzögerung, Jitter, Verlustrate), Verfügbarkeit, Kosten und physikalische Lokalisation von Verbindungen nicht berücksichtigt. Eine gute Anbindung ist vorhanden, wenn ein oder mehrere Pfade mit möglichst kurzer Länge – idealerweise eine Direkt- und mehrere kurze Backup-Verbindungen – zwischen einzelnen autonomen Systemen vorhanden sind. Im Durchschnitt verläuft demnach jede fünfte Route zwischen zwei deutschen AS über mindestens ein ausländisches autonomes System – kein Shortest Path ohne ausländische autonome Systeme –, mindestens aber jede achte Verbindung, da keine direkte Verbindung zu anderen deutschen autonomen Systemen besteht.

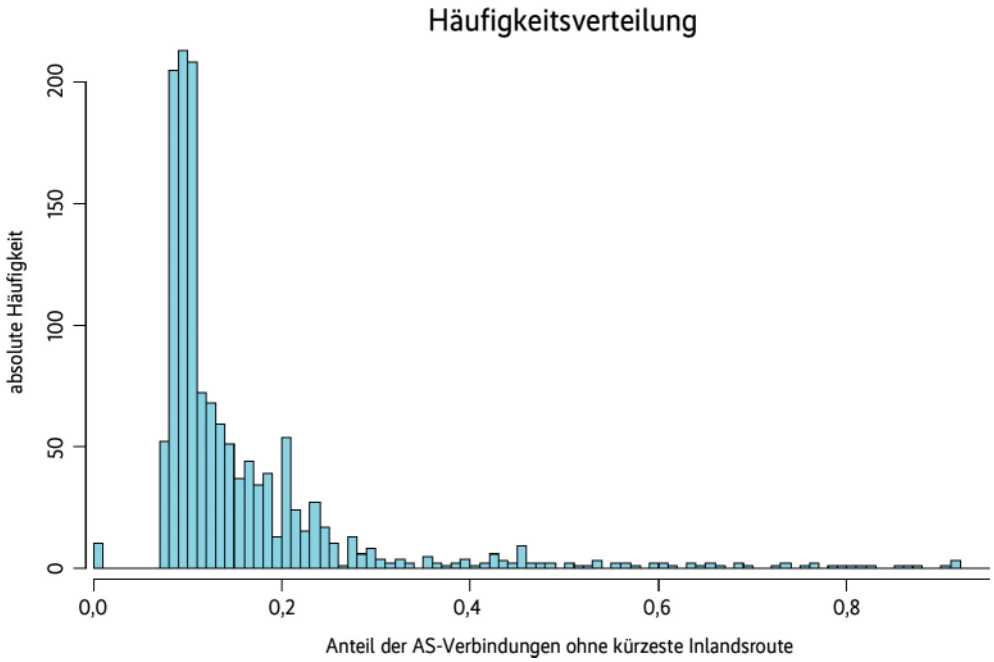
Auch wenn hierbei eine Reihe axiomatischer Grundannahmen bezüglich des Datentransports zu treffen sind, lassen sich doch zumindest qualitative Erkenntnisse ableiten. Vor allem die genannte Abweichung zwischen dem mittleren und dem häufigsten Wert, also die Differenz zwi-

schen Mittelwert und Modus, lässt eine deutlich asymmetrische Verteilung erkennen. Infolge dieser Asymmetrie ergeben sich im Falle eines verbindlichen Transportweges divergierende Konsequenzen für einzelne autonome Systeme.

Ungleichheit durch Schengen-Routing

Im Ergebnis wären AS-Betreiber also unterschiedlich stark betroffen, wenn sie beim Routing der Daten auf neue gesetzliche Vorgaben verpflichtet würden. Die Frage, ob damit Wettbewerbsbeschränkungen geschaffen werden, die zumindest nationalem und europäischem Recht standhalten müssten, soll hier außen vor bleiben.

Da die Organisation des Datenverkehrs bisher primär unter technisch-ökonomischen Gesichtspunkten geregelt ist,



Der Kurvenverlauf lässt ein Maximum bei 0,12 erkennen, gleichbedeutend mit dem Modus der Verteilung. Demnach sind typischerweise in 12 % der Fälle autonome Systeme außerhalb Deutschlands in den Datentransport involviert, obwohl Ausgangs- und Endpunkt der Kommunikation im Inland liegen. Im Durchschnittsfall – repräsentiert durch den arithmetischen Mittelwert – ist dies sogar bei 22 % der Verbindungen gegeben, hier erkennbar an der Fläche zwischen den Achsenabschnitten 0.1 und 0.25 auf der Horizontalen (Abb. 3).

Regionale Kategorisierung der Verbindungen zwischen autonomen Systemen

von \ nach	AR	AU	BR	CA	CN	DE	EU	FR	GB	ID	IN
AR	**492**		1	1							1
AU		**3403**		5	5	78	1	19	98	7	25
BR	4	4	**3197**	11	1	13		8	12		5
CA	1	19	3	**1520**	19	126	1	114	340	19	15
CN		6		7	**1007**	21	3	1	26	2	4
DE		80	12	136	24	**18253**	72	1003	3515	5	32
EU		1		1	3	72	**9**	136	122	1	2
FR		19	3	107	1	1026	119	**8128**	1539	2	5
GB		111	7	338	28	3542	122	1463	**24139**	42	134
ID		5		7		2	1	1	33	**3433**	2
IN	2	25	2	5	4	18	2	3	45	2	**1678**
IT		6		24	3	388	42	195	531		3
JP		110	1	18	25	13	3	31	107	11	11
KR		6	1	1	10	45	1	11	112	1	2
MX	1		1	2		1		1	15	1	
RU		40	7	85	20	1621	8	380	1981	12	29
SA				4		7			13		1
TR				5		39	2	2	29		
US	105	264	419	791	107	3286	72	1575	5475	122	128
ZA		2		6		50	3	24	293	1	2
G20 gesamt:	**605**	**4101**	**3654**	**3074**	**1257**	**28601**	**461**	**13095**	**38425**	**3661**	**2079**
Übrige Staaten:	24	560	57	634	300	10807	268	2986	11680	520	198
Global gesamt:	**629**	**4661**	**3711**	**3708**	**1557**	**39408**	**729**	**16081**	**50105**	**4181**	**2277**

Ländercodes nach ISO-3166: AR=Argentinien, AU=Australien, BR=Brasilien, CA=Kanada, CN=VR China, DE=Deutschland, EU=Europäische Union, FR=Frankreich, GB=Vereinigtes Königreich, ID=Indonesien, IN=Indien. IT=Italien, JP=Japan, KR=Südkorea, MX=Mexiko, RU=Russische Föderation. SA=Saudi-Arabien, TR=Türkei, US=USA, ZA=Südafrika

führt ein solcher Eingriff in die wirtschaftliche Handlungsfreiheit der Provider möglicherweise zu höheren Kosten, die dann mit hoher Wahrscheinlichkeit in Form von Preissteigerungen auf die Nutzergemeinde abgewälzt würden. Zu rechnen wäre auch mit schlechterer Service-Qualität wegen künstlich geminderter Ausfallsicherheit, da die Verbindungen zu ausländischen Systemen nicht als Backup-Leitungen für innerdeutsche Kommunikation dienen können.

Eine Verteuerung der Internetnutzung würde nicht nur den Standort Deutschland belasten, sie impliziert auch unerwünschte soziale Folgen. Ohne entsprechende Kompensation wären einkommensschwache Bevölkerungsteile besonders betroffen, bei denen eine vermehrte Internetnutzung eigentlich besonders erstrebenswert ist, wie diverse Studien belegen.

Aber auch eine Ausgleichsabgabe – in welcher Form auch immer – würde letztlich die Allgemeinheit belasten. Sofern die Sicherheit des Datenverkehrs als öffentliches Gut und staatliche Gestaltungsaufgaben betrachtet wird, wäre der hierfür zu betreibende Aufwand prinzipiell kein Hindernis. Allerdings ist dann die Frage legitim, ob die aufzuwendenden Mittel zweckdienlich eingesetzt sind, ob man also mit den zusätzlichen Ausgaben einen objektiven Sicherheitsgewinn erzielt.

Regionales Routing erfüllt diese Bedingung per se nicht, der Zugriff auf ungeschützte Daten ist nach wie vor mit denselben Mechanismen wie heute möglich. Statt von einem technologisch höheren Sicherheitsniveau zu profitieren, muss die Nutzergemeinde nur anderen Akteuren vertrauen, was eine objektive Bewertung verhindert.

Facebook & Co. kaum greifbar

Aus technischer Sicht kommt hinzu, dass durch Cloud Computing, Social Media, Suchmaschinen, E-Mail-Provider und so weiter umfangreicher Content auf Servern außerhalb Europas gehostet ist, der auch in Deutschland intensiv genutzt wird. Diese Transportwege lassen sich naturgemäß nicht durch Routing-Änderungen abkapseln.

Unklar bleibt auch, wie die Abgrenzung zwischen inländischen und ausländischen autonomen Systemen im Rahmen einer verbindlichen Regelung zum Datenrouting überhaupt zielkonform definiert werden kann. Im Ergebnis soll der Datenzugriff durch unautorisierte (ausländische) Dritte verhindert werden. In Anbetracht multinationaler Konzerne auf Anbieterseite reicht es hierfür aber nicht aus, allein auf den Standort der Infrastruktur abzustellen, wie wir aus der Snowden-Aufklärung erfahren haben. Erforderlich wäre eine internationale Policy zum Schutz der übertragenen Daten, die die konkurrierende Gesetzgebung verschiedener Staaten übergreifend regelt und somit den betroffenen Providern einheitliche Verfahrensgrundsätze auferlegt.

Einsatz von Verschlüsselung in Deutschland

Im Dezember 2013 liefen über das unverschlüsselte Webprotokoll HTTP (Port 80) 77 % der Datenpakete, über das Krypto-Pendant HTTPS via SSL/TLS (Port 443) 23 %. Da etwa 60 % des Datenvolumens beziehungsweise 50 % der Pakete Webkommunikation sind, ist, bezogen auf die gesamte Internet-Kommunikation, nur circa jedes siebte IP-Paket SSL-verschlüsselt.

IPSec kam gerade einmal bei 0,8 % aller IP-Pakete zum Einsatz, das heißt, nur jedes 125. IP-Paket im Internet wurde IPSec-verschlüsselt.

Und nur 4 % aller E-Mails, also jede 25. E-Mail, war verschlüsselt.

	IT	JP	KR	MX	RU	SA	TR	US	ZA	G20 gesamt:	Übrige Staaten:	Global gesamt:
								29		**524**	12	**536**
	4	54	6	1	20			248		**3974**	510	**4484**
		2	1	3	5			262		**3528**	111	**3639**
	23	14	6	3	52	6	4	628	2	**2915**	757	**3672**
	3	11	7		17			82	1	**1198**	288	**1486**
	367	21	51	3	1158	10	44	3093	54	**27933**	11054	**38987**
	42	3	1		10		1	72	3	**479**	286	**765**
	213	31	16	3	231	1	3	1429	28	**12904**	3183	**16087**
	593	114	121	19	1432	16	28	5104	193	**37546**	12096	**49642**
		8	1	1	1			60		**3555**	344	**3899**
	1	6	1	1	10	1		197	1	**2004**	196	**2200**
	5806	3		5	89		1	419	3	**7518**	1103	**8621**
	3	**2408**	19	1	8	1		379		**3149**	534	**3683**
		10	**3153**		9			55		**3417**	211	**3628**
	5	1		**298**	1			48		**375**	30	**405**
	166	19	22	8	**41534**	5	9	1215	52	**47213**	5688	**52901**
		1				**592**	1	26		**645**	37	**682**
	1				8	2	**2380**	47		**2515**	234	**2749**
	523	296	86	103	964	48	55	**32499**	88	**47006**	12923	**59929**
	6	2	2	1	23			74	**230**	**719**	239	**958**
	7756	**3004**	**3493**	**450**	**45572**	**682**	**2526**	**45966**	**655**	**209117**	49836	**258953**
	1101	410	220	37	3956	42	188	10681	175	**44844**		
	8857	**3414**	**3713**	**487**	**49528**	**724**	**2714**	**56647**	**830**	**253961**		**436363**

Die gesamte Zweckdienlichkeit einer solchen Lösung lässt sich also nur im Kontext der geltenden Rechtslage beurteilen, sodass die Problematik im Grunde nur von der technischen in die juristische Ebene verschoben wird. Allerdings könnten die führenden deutschen Internet Service Provider vor dem Hintergrund der aktuellen Diskussion auch zu dem Schluss kommen, dass eine verstärkte Kooperation der nationalen Anbieter im gemeinsamen Interesse liegt, etwa um der zunehmenden Dominanz US-amerikanischer Anbieter entgegenzuwirken und vorrangig lokale Austauschpunkte zu nutzen, wie es der DE-CIX vorgeschlagen hat.

Klar ist aber auch, dass Deutschland als Exportland und Wissensgesellschaft von der unbeschränkten Verfügbarkeit des Internets abhängig und selbiges qua natura nur als globales Medium denkbar ist. Besser wäre es daher, den Schutz der Privatsphäre und die Abwehr von Wirtschaftsspionage mit objektivierbaren, technologischen IT-Sicherheitsmaßnahmen zu unterstützen, die offen kommuniziert werden, und so dem breiten Vertrauensverlust auf Anwenderseite entgegenzuwirken, was für den langfristigen Erfolg von Cloud Services und anderen digitalen Diensten unabdingbar ist.

Aktive Verschlüsselung statt passive

Nachdem bekannt wurde, dass auch das großflächige Abhören von Mobilfunk und das Anzapfen von Glasfaserleitungen zum technischen Repertoire der NSA gehört, darf man bezweifeln, ob der physische Zugriff auf Kommunikationsmedien überhaupt zu verhindern ist. Die Verbindungen zwischen den autonomen Systemen gehen als Kabel (Kupfer oder Glasfaser) oder Funk durch Wälder und Felder sowie durch die großen Meere dieser Welt und sind dort abhörbar. Schutzkonzepte sollten daher eher auf den Inhalt der Kommunikation als auf die Transportweginfrastruktur abstellen.

Sofern es gelingt, den Informationsgehalt von Daten vor Dritten zu verbergen, wird die Fähigkeit zum Abhören und Mitschneiden nahezu wertlos. Das setzt voraus, Nutzdaten auf dem Weg von der Quelle zum Ziel durchgängig zu schützen, üblicherweise mittels Verschlüsselung durch starke Kryptografie. Dadurch wäre auch die Diskussion über eine nationale Router-Souverantität überflüssig, weil ja nur noch verschlüsselte Daten über die Router laufen.

Zwar kann SSL-verschlüsselter Traffic an den jeweili-

Anzahl autonomer Systeme

1	USA	15631
2	Russische Föderation	4716
3	Brasilien	1919
4	Ukraine	1874
5	Polen	1741
6	Großbritannien	1626
7	**Deutschland**	**1484**
8	Rumänien	1335
9	Australien	1070
10	Kanada	938
11	Frankreich	909
12	Italien	700
13	Südkorea	685
14	Niederlande	658
15	Indien	580
16	Schweiz	578
17	Japan	559
18	Indonesien	554
19	Bulgarien	552
20	Schweden	506
	Global gesamt	5040

gen Endpunkten (Server und Client) abgegriffen werden, die Inhalte sind aber (bei korrekter Implementation des Verfahren) während der Übertragung nicht im Klartext zu lesen. Um einen wirkungsvollen Schutz vor Traffic Snooping und MITM-Attacken (MITM: Man in the Middle) zu gewährleisten, sind allerdings profunde Fachkenntnisse erforderlich, die man beim typischen Durchschnittsnutzer nicht voraussetzen kann. Für Laien ist das Zertifikatssystem oft unüberschaubar, und Warnmeldungen, etwa bezüglich Zertifikatsänderungen, sind mitunter nur schwer zu deuten.

Komplexe SSL/TLS-Verschlüsselung

Auch ist die „Trustworthiness“ von Certificate Authorities (CA) ein noch ungelöstes Problem. Besonders bei den vielen in den USA ansässigen CAs ist es schon lange nicht mehr undenkbar, dass ausländische Geheimdienste durch Gerichtsbeschlüsse oder gar nicht-autorisierte Zugriffe Zugang zu Zertifikaten erhalten, mit denen gefälschte Internetseiten vom Nutzer nicht als illegitim erkannt werden können.

Das Beispiel DigiNotar zeigt, dass dieses Problem auch innerhalb Europas eine wichtige Rolle spielt. Erinnert sei auch an den Missbrauch der CA von ANSSI (das französische Pendant zum deutschen BSI) für die Erstellung von Google-Zertifikaten für SSL Traffic Sniffing im internen Netz. Gefälschte Zertifikate können auch in MITM-Angriffen benutzt werden. Ein hohes Maß an Vertrauen in die Authentizität der Zertifikate ist der Grundstein bei flächendeckendem SSL-Einsatz, und dieses Vertrauen kann schon jetzt nicht erbracht werden.

Auch die zentralistisch gesteuerte Einführung einer solchen flächendeckenden Verschlüsselung ist problembehaftet, da angepasste Software bei Endkunden beziehungsweise Internetnutzern installiert werden müsste. Die Nutzung der verschiedenen Verschlüsselungsverfahren nimmt zu, ist aber noch nicht in wünschenswertem Umfang etabliert (siehe Kasten „Einsatz von Verschlüsselung in Deutschland“).

Fazit

Anstelle einer restriktiven Gesetzgebung sollten Internet-Provider durch verschiedene Anreize motiviert werden, aktive IT-Sicherheitstechnologien selbst zu implementieren oder ihre Kunden hierbei zu unterstützen. Denkbar wären etwa Steuervorteile, Beihilfen und Technologiesubventionen oder Förderungen im Rahmen der öffentlichen Beschaffung.

Damit könnten Eingriffe in die unternehmerische Handlungsfreiheit und negative Konsequenzen für den Standort Deutschland vermieden und durch eine langfristig orientierte, staatlich geförderte Innovationsstrategie ersetzt werden.

Technologische IT-Sicherheitsmaßnahmen helfen aber nicht nur heraus aus der Grauzone staatlicher Internetüberwachung, sie bieten auch Unterstützung im Kampf gegen den weltweit zunehmenden Cybercrime. Infolge der Komplexität einer technisch tragfähigen Gesamtlösung und der notwendigen Unterstützung durch geeignete Rechtsnormen wird deutlich, dass mit Blick auf die hier skizzierten Probleme gemeinsame Anstrengungen der Marktakteure, Internetnutzer, IT-Sicherheitsindustrie und politischen Entscheidungsträger notwendig sind, um eine konsensfähige und nachhaltige Sicherheitslösung zu erzielen.

In der europäischen Währungskrise hat Deutschland zunächst widerwillig eine Führungsrolle übernommen und – nach konsequentem Handeln – durchaus internationale Anerkennung erhalten. Es wäre zu begrüßen, wenn die politisch Verantwortlichen auch beim Thema Internet ihre passiv-duldende Grundhaltung aufgeben und künftig eine aktive Rolle als Repräsentanten der europäischen Gemeinschaft übernehmen.

Dabei sollte man transatlantische Meinungsverschiedenheiten nicht zur globalen Krise hochspielen. Die Geschichte diverser „Handelskriege“ zwischen der EU und den USA, etwa wegen der Preise von Stahl und Agrarprodukten, macht deutlich, dass solche Konflikte durchaus zur Normalität der politischen Streitkultur gehören und nicht zu dauerhaften Zerwürfnissen führen müssen.

Dafür spricht auch, dass in den USA der Widerstand gegen zügellose Geheimdienstaktivitäten wächst. In einem offenen Brief an Kongress und Präsident Obama fordern führende US-Unternehmen wie Google, Facebook, Apple und Microsoft eine Rückkehr zu Transparenz und rechtsstaatlichen Prinzipien bei der Internet-Überwachung. Auf einer gemeinsamen Website proklamieren sie fünf Prinzipien, zu denen staatliche Überwachungsprogramme global verpflichtet werden sollen. Im Kern geht es dabei um die Verhinderung anlassloser Massenüberwachung und eine demokratisch legitimierte Kontrolle geheimdienstlicher Aktivitäten durch unabhängige Instanzen.

Technische Eingriffe wie Routenänderungen können als reaktive Maßnahmen den Schutz der Vertrauenswürdigkeit im Internet bestenfalls operativ unterstützen – und auch nur, solange sie nicht durch Gegenmaßnahmen ausgehebelt oder umgangen werden, was in dem beschriebenen Szenario möglich und wahrscheinlich wäre.

Ein nachhaltiger Schutz der Daten von Staatsüberwachung im Internet kann nur auf international verbindlichen Normen beruhen, die gemeinsam ausgehandelt und wirksam durchgesetzt werden. (js)

Prof. Norbert Pohlmann

ist geschäftsführender Direktor des Instituts für Internet-Sicherheit und Professor für Verteilte Systeme und Informationssicherheit an der Westfälischen Hochschule Gelsenkirchen.

Illya Siromaschenko

ist wissenschaftlicher Mitarbeiter im Forschungsbereich Internet-Kennzahlen am Institut für Internet-Sicherheit der Westfälischen Hochschule Gelsenkirchen.

Michael Sparenberg

ist wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit der Westfälischen Hochschule Gelsenkirchen und Projektleiter für den Forschungsbereich Internet-Kennzahlen.

Literatur

[1] Ein Internet-Kennzahlensystem für Deutschland: Anforderungen und technische Maßnahmen; in: Proceedings der DACH Security Konferenz 2011 – Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven; Hrsg.: Peter Schartner, Jürgen Taeger; syssec Verlag, Klagenfurt 2011

[2] S. Feld, N. Pohlmann, M. Sparenberg, B. Wichmann; Analyzing G-20'Key autonomous Systems and their Intermeshing using AS-Analyzer; in: Proceedings of the ISSE 2012 – Securing Electronic Business Processes – Highlights of the Information Security Solutions Europe 2012 Conference, Eds.: N. Pohlmann, H. Reimer, W. Schneider; Springer Vieweg Verlag, Wiesbaden 2012

Alle Links: www.ix.de/ix1402112