Praxis

Die nächste Generation des Internets – auch eine Frage der Sicherheit

Wo liegen die Chancen und Risiken und was hat IPv6 damit zu tun?

SILVIA HAGEN

Zu einer wirkungsvollen Cybersecurity gehören eine ganze Reihe von wichtigen Elementen, die alle nur in ihrem ganzheitlichen Zusammenspiel ihre Wirkung entfalten können. In diesem Puzzle ist IPv6 nur ein Element. Trotzdem spielt es eine nicht unwichtige Rolle – dies auch, weil es mit der Frage der Sicherheit zusammenhängt. Dieser Artikel basiert auf einem Vortrag, den die Autorin im September 2022 gehalten hat.

Schlüsselbegriffe Cybersecurity; IPv6; Cyberangriffe; digitale Souveränität; SCION
Keywords cybersecurity; IPv6; cyber attacks; digital sovereignty; SCION

SILVIA HAGEN ist Expertin, Beraterin und Buchautorin im Bereich Internet Protokoll Version 6. Seit über 25 Jahren führt sie das erfolgreiche Unternehmen Sunny Connection AG. Zu ihren Kunden zählen Grossfirmen mit internationalen Netzwerken aus diversen Industriesektoren. Sie schrieb Fachbücher zum Thema TCP/IP und IPv6. Für den IT-Fachverlag O'Reilly verfasste sie das anerkannte Standardwerk «IPv6 Essentials». Seit 2001 ist sie in der Internet-Gemeinschaft aktiv und ist seither eine gefragte Referentin an internationalen Konferenzen und für Ausbildungsworkshops. 2010 gründete sie das schweizerische IPv6 Council, ein regionales Chapter des Internationalen IPv6 Forums. Im Rahmen ihrer Tätigkeit als Präsidentin des IPv6 Councils hat sie in Zürich in den Jahren 2013–2016 erfolgreiche IPv6 Konferenzen organisiert mit internationalen Koryphäen als Speakern.
E-Mail: silvia.hagen@sunny.ch

In diesem Artikel werde ich die verschiedenen Aspekte und ihr Zusammenspiel beschreiben. Dabei gehe ich davon aus, dass nicht jeder Leser ein IT-Profi sein muss, sondern versuche, das Ganze allgemein verständlich zu beschreiben. Der IT-Profi kann die technischen Beschreibungen der Grundlagen einfach überfliegen.

1 Was ist IPv6?

1.1 Die Rolle von IPv6

Um eine Grundlage fürs Verständnis zu legen, betrachten wir zunächst die Frage, «was ist denn IPv6» und was sind seine Eigenschaften? IP ist das Internet Protokoll und ein wichtiger Bestandteil der TCP/IP Protokollfamilie.

> IP ist zuständig für den Transport aller Daten im Internet, sozusagen die Datenstrasse.

In den frühen 1970er Jahren wurde IP Version 4 (IPv4) definiert und eingeführt. Dieses Protokoll hat bislang erfolgreich den Auf- und Ausbau des Internets ermöglicht. Seit sich das Internet in den 1990er Jahren zu verbreiten begann, wurde deutlich, dass der 32-bit Adressraum von IPv4 nicht für alle Zukunft ausreichen wird. So fing man bereits damals an, an einer Nachfolgeversion zu arbeiten, mit dem Hauptziel, den Adressraum zu erweitern. IPv6 hat einen 128-bit Adressraum. Was das bedeutet und wieviel das ist, darauf gehen wir im nächsten Absatz genauer ein.

«Seit sich das Internet in den 1990er Jahren zu verbreiten begann, wurde deutlich, dass der 32-bit Adressraum von IPv4 nicht für alle Zukunft ausreichen wird. So fing man bereits damals an, an einer Nachfolgeversion zu arbeiten, mit dem Hauptziel, den Adressraum zu erweitern.»

Um die Rolle von IP besser zu verstehen, ist eine Illustration hilfreich (Abbildung 1). Das Bild zeigt das DOD-Vierschichten-Modell, das die Architektur des Internets und von Netzwerkprotokollen beschreibt.

Die Beschreibung der vier Schichten von unten nach oben ergibt einen Einblick in die Zusammenhänge und Herausforderungen:

Hardware

Die unterste Schicht ist die Verbindung des Betriebssystems mit der Hardware. Hier sind die Netzwerktreiber zu finden und die Schicht beschreibt die Topologie. Die Netzwerkkarte wird über eine sogenannte MAC Adresse (Media Access Control) angesprochen.

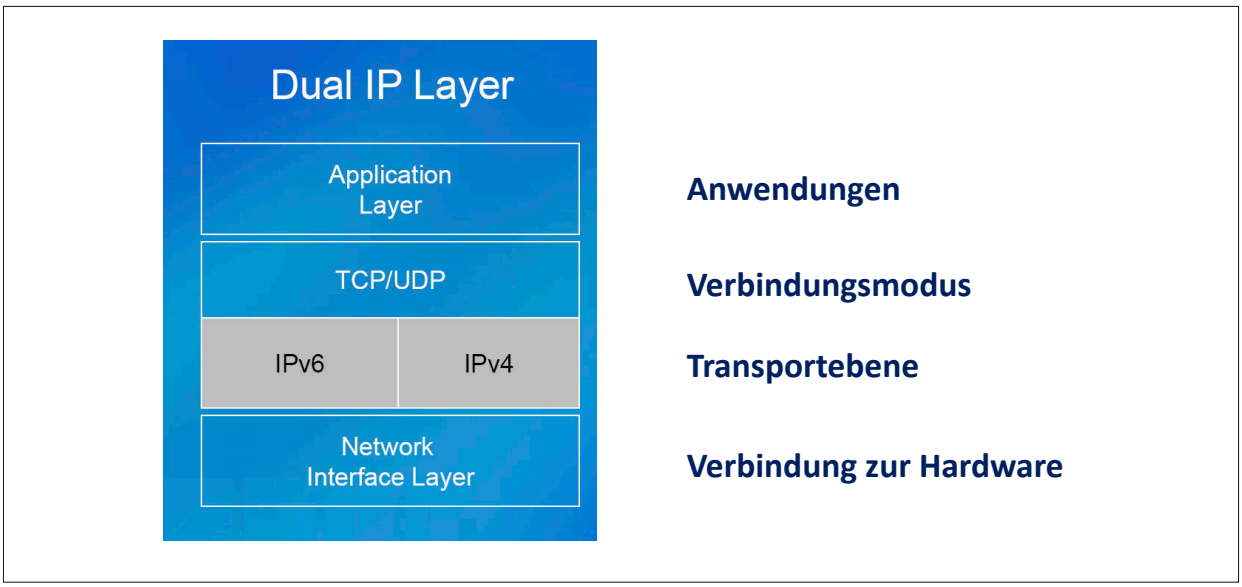


Abbildung1: Das DOD-Vierschichtenmodell. (Eigene Darstellung)

Transportebene

Auf der zweiten Ebene folgt das Transportprotokoll und damit sind wir beim Thema IPv4 und IPv6. Bis zur Einführung von IPv6 gab es nur IPv4 als Transportmöglichkeit. Das bedeutet, alles was wir im Internet getan haben (surfen, E-Mail) wurde über IPv4 transportiert.

Heute bestehen beide Möglichkeiten. Wir können nun Daten entweder über IPv4 oder über IPv6 transportieren. Die Komplexität bei der Einführung von IPv6 kommt daher, dass wir ganz unterschiedliche Szenarien parallel betreiben können oder müssen.

Es gibt Geräte (oder genauer gesagt Netzwerkkarten), die nur IPv4 sprechen, Netzwerkkarten die nur IPv6 sprechen und sogenannte dual-stack-Karten, die beides können. Eine sogenannte IPv4-only-Netzwerkkarte kann nicht direkt mit einer IPv6-only-Netzwerkkarte kommunizieren. Um das zu ermöglichen, braucht es Übersetzungsmechanismen. Eine dual-stack-Karte kann sich mit beiden Protokollen unterhalten. Das lässt sich gut mit einer Zweisprachigkeit vergleichen. Jemand der Deutsch und Französisch spricht, kann wählen, in welcher Sprache er sich unterhält, je nachdem was sein Gesprächspartner spricht. Jemand der nur Deutsch spricht, braucht einen Übersetzer, um sich mit jemand zu unterhalten, der nur Französisch spricht.

Verbindungsmodus

Auf der nächsten Ebene wird der Verbindungsmodus definiert. Hier sind die häufigsten Protokolle TCP (Transmission Control Protocol) und UDP (User Datagram Protocol).

TCP ist ein verbindungsorientiertes Protokoll. Hier bauen Sender und Empfänger explizit eine verbindliche Beziehung auf und bestätigen sich jeweils den Empfang der Datenpakete gegenseitig. Es gibt Mechanismen, um Datenverlust zu vermeiden. UDP ist ein verbindungsloses Protokoll. Das heisst, der Sender weiss nicht, ob seine Daten angekommen sind oder nicht. Es wird in Bereichen eingesetzt, in denen der Verlust von Daten nicht so kritisch ist. Als Bild könnte man TCP vergleichen mit einem eingeschriebenen Brief und UDP mit einer Postkarte.

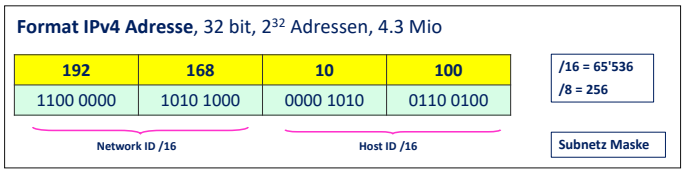


Abbildung 2: Das IPv4 Adressformat. (Eigene Darstellung)

Anwendungen

In der obersten Schicht laufen unsere Dienste und Applikationen. Sie sind der Grund, warum wir die ganzen Netzwerkinfrastrukturen aufbauen. Hier sind die Dienste, die es mir ermöglichen zu surfen, in einem Shop einzukaufen, E-Mails zu schreiben, Social Networks zu benützen und auf Daten irgendwelcher Art zuzugreifen.

Applikationen, die sich an dieses Modell halten, indem sie nur direkte Schnittstellen zu TCP oder UDP haben, die brauchen in der Regel keine oder nur minimale Anpassungen, um in einem IPv6 Netzwerk betrieben werden zu können.

1.2 IPv4 Adressformat

Bevor wir auf das IPv6 Adressformat eingehen, schauen wir uns als Vergleich zunächst das IPv4 Adressformat an.

In Abbildung 2 sehen wir das 32-bit Format der IPv4 Adresse. Diese wird im binären Format geschrieben, das heisst jedes Bit kann entweder 0 oder 1 sein. Darüber sieht man die dezimale Umsetzung der binären Adresse, wie sie wahrscheinlich viele der Leser und Leserinnen schon gesehen haben.

Mit 32 Bits kann man total rund 4.3 Mrd. Adressen bilden (2^{32}). Das ist die Grenze des IPv4 Adressraums. Sie ist auch eine theoretische Grenze, in der Praxis ist es nicht möglich, den Adressraum zu 100 % auszuschöpfen.

Der linke Teil der Adresse bezeichnet das Netzwerk, in dem sich eine Netzwerkkarte befindet (Network ID), der rechte Teil bezeichnet die einzelne Netzwerkkarte (Host ID). Innerhalb eines Netzwerkes muss eine Host ID einmalig sein. Die Stelle des Übergangs zwischen Netzwerk und Host ist bei IPv4 nicht fix, sie kann nach Bedarf verschoben werden. Wie lange die Netzwerk ID ist, bezeichnet man als Subnetz Maske.

Total verfügbare Adressen:	4.3 Mrd (theoretisch)
Aktuelle Weltbevölkerung:	7.9 Mrd
Globale Penetrationsrate:	69 % = 5.4 Mrd

Tabelle 1: Penetrationsrate.
(Quelle: https://internetworldstats.com/stats.htm)

Mit der Penetrationsrate bezeichnet man den Prozentsatz einer Bevölkerungsgruppe, der eine Internet Verbindung hat.

Die Gegenüberstellung oben zeigt klar, dass bei weitem nicht genügend IPv4 Adressen zur Verfügung stehen, um allen aktuellen Internetbenützern eine Adresse zuweisen zu können, geschweige denn noch Wachstum zu ermöglichen.

Zu beachten ist dabei vor allem, dass in diesen Zahlen Geräte wie Internet of Things Geräte (IoT) *nicht* berücksichtigt sind.

«Damit brechen wir jedoch mit einem Grundgesetz des ursprünglichen Internet Designs, nämlich die End-to-End Verbindung zwischen zwei Kommunikationspartnern.»

Im Kontext der Frage, was der Beitrag von IPv6 zu erhöhter Sicherheit ist, ist die Tatsache zu verstehen, dass die schon lange bestehende Adressknappheit mit IPv4 dazu geführt hat, dass wir komplizierte Mechanismen definiert haben und sehr breit einsetzen, die den Adressraum sozusagen künstlich erweitern. Das heisst, wir setzen sogenannte NAT-Gateways (Network Address Translation Gateways) ein, die es ermöglichen, viele User hinter einer öffentlichen IPv4 Adresse zu «verstecken». Damit brechen wir jedoch mit einem Grundgesetz des ursprünglichen Internet Designs, nämlich die End-to-End Verbindung zwischen zwei Kommunikationspartnern. Da diese NAT-Gateways die Adressen umschreiben, ist eine Verbindung nicht mehr direkt nachvollziehbar und stellt auch für verschiedene Dienste ein Problem dar. Der Adressmangel ist gross und besteht seit Langem, das bedeutet, dass an vielen Orten sogar mehrere Schichten von NAT eingesetzt werden.

Dadurch werden Netzwerke sehr komplex, die Kosten für Betrieb und Troubleshooting steigen damit enorm an. Vielen Firmen ist die Dimension dieser Kosten nicht so bewusst.

Die IoT-Anwendungen, die seit einiger Zeit wie Pilze aus dem Boden schiessen, erhöhen den Bedarf an IP Adressen exponentiell. Dieses Wachstum lässt sich nicht mehr mit IPv4 umsetzen, nicht mit allen Tricks. Höchste Zeit also für IPv6, den Adressraum exponentiell zu erweitern. Damit IoT-Geräte unkompliziert mit IPv6 adressiert werden und darüber kommunizieren können, setzt voraus, dass wir Schritt für Schritt in allen Infrastrukturen IPv6 einführen.

1.3 IPv6 Adressformat

Und so sieht das Format einer IPv6 Adresse aus (Abbildung 3):

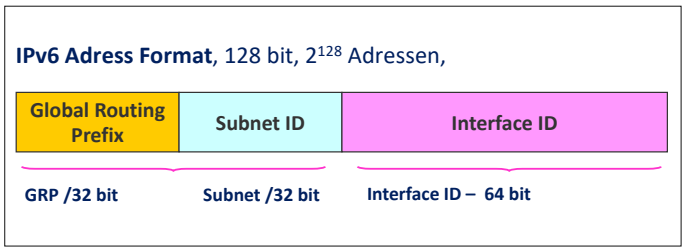


Abbildung 3: Das IPv6 Adressformat. (Eigene Darstellung)

Das *Global Routing Prefix* wird einem Land oder einer Organisation von der zuständigen Behörde zugewiesen (auf diese Organisationen kommen wir im Kapitel 3 zu sprechen). Es hat häufig eine Länge von 32 bit, was man dann ein /32 nennt (ausgesprochen: Slash 32). Die Länge kann aber auch variieren, so hat zum Beispiel die Schweiz ein /27 erhalten.

Da die Trennung zwischen Netzwerk ID und Interface ID immer bei 64 bit ist, hängt die Länge der Subnet ID von der Länge des Global Routing Präfix ab.

Die *Subnet ID* ist der Adressbereich, den ich für meine individuelle Adressierung frei verwenden kann. Wenn also eine Organisation ein /32 erhält, kann sie die nächsten 32 bit zur Gestaltung ihres internen Adress-

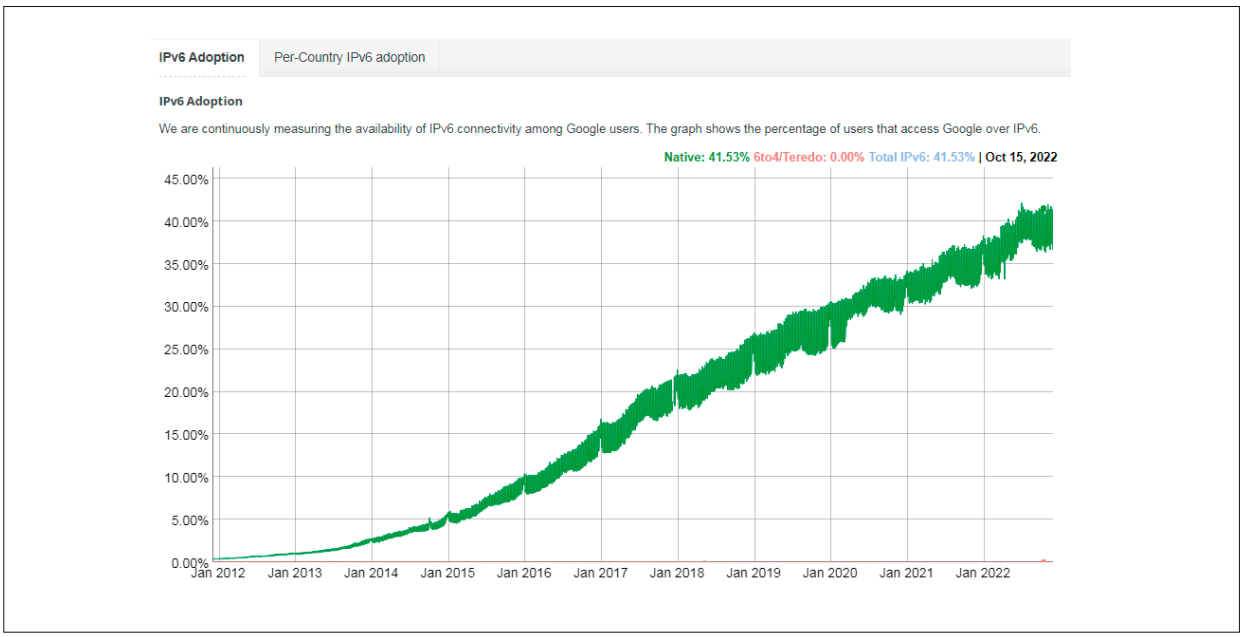


Abbildung 4: Google IPv6 Statistik per Oktober 2022. (Quelle: https://www.google.com/intl/en/ipv6/statistics.html)

plans verwenden. Der Schweiz, die ein /27 hat, stehen also für die Aufteilung in Netzwerke 37 bits zur Verfügung, die nun auf alle Bundesdienste, Kantone und Gemeinden in einem Adressierungsplan verteilt werden können. Das sind dann mehr als 137 Mrd. Netzwerke (2^{37}).

IPv6 Adressen werden hexadezimal dargestellt und mit Doppelpunkten getrennt. Das sieht dann zum Beispiel folgendermassen aus:

2001:0db8:0000:0000:0208:c705:30c5:5e7a

Wie viele Adressen stellt das denn nun zur Verfügung?

2^{128} sind 340 282 366 920 938 463 463 374 607 431 768 211 456 Adressen

Ist das viel? Wie lange reicht das? Wenn wir 20 Jahre oder mehr brauchen um es einzuführen und dann ist es mit IoT in 10 weiteren Jahren alle? Was dann?

2 Ein paar Statistiken

Um diese Fragen beantworten zu können, brauchen wir Vergleiche und einen Kontext. Darum lade ich die Leser und Leserinnen nun ein, auf eine kleine Reise durch die aktuelle Verbreitung von IPv6 in der Welt, die ich mit einer Annäherung an die Frage abschliesse, ob dieser Adressraum ausreichend ist für unsere exponentiell steigenden Ansprüche.

2.1 Das Wachstum des Internets

Die Zahlen in Tabelle 2 beziffern die Internet Bevölkerung und sind protokollunabhängig. Das heisst, sie schliessen Verbindungen zum Internet ein, egal ob jemand IPv4 oder IPv6 benützt.

2001	360 Mio	
2011	1.9 Mrd	Ende des IPv4 Adresspools
2022	5.5 Mrd	Faktor 15+ in 20 Jahren

Tabelle 2: Das Wachstum des Internets.
(Quelle: https://www.internetworldstats.com)

Wie bereits erwähnt, sind in diesen Zahlen keine Geräte enthalten. Im Jahre 2011 gingen bei IANA (Internet Assigned Numbers Association) die IPv4 Adressen aus. Das bedeutet, seither kann niemand mehr offiziell öffentliche IPv4 Adressen beziehen. Auf diese Organisationen und den Prozess geh ich im nächsten Kapitel noch etwas näher ein.

> Hier ist zu verstehen, dass damit IPv4 seit 2011 de facto «End of Life» ist.
>
> IPv4 wird nicht mehr von der IETF weiterentwickelt. Es werden nur noch Sicherheitsprobleme gelöst. Die Weiterentwicklung findet für IPv6 statt.

Abbildung 4 stellt die Zunahme von IPv6 Internetbenützern seit 2012 dar. Der 6. Juni 2012 war der Tag, an dem offiziell das IPv6 Internet lanciert wurde. Die 20 % Marke wurde 2017 erreicht und heute (Oktober 2022)

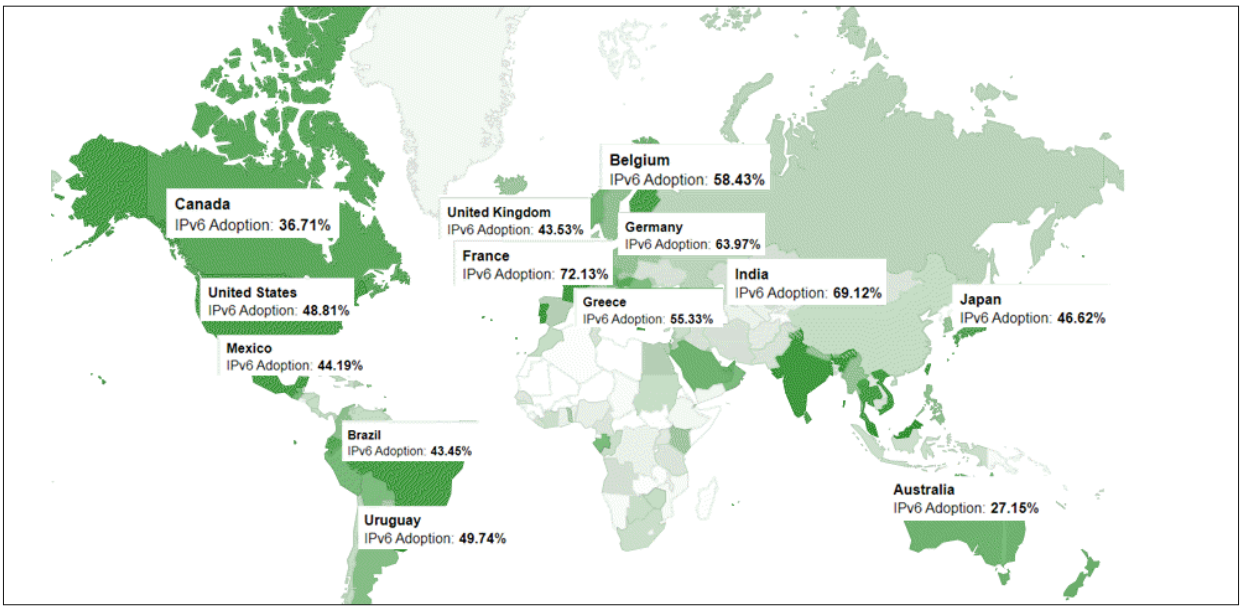


Abbildung 5: Google IPv6 Statistik per Oktober 2022 – Deployment pro Land.
(Quelle: https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption)

sind wir auf rund 42 %. Das bedeutet, dass ca. 2.3 Mrd. Internetbenützer sich heute mit IPv6 im Internet bewegen.

Über 30 % der Top-1000-Websites sind über IPv6 erreichbar. Es wäre für die globale Internetkommunikation (und für die Budgets der Provider) von Vorteil, wenn es mehr wären. Das ist eine Bitte an alle Betreiber von Webseiten, ihre Inhalte über IPv6 zugänglich zu machen, zu Gunsten der gesamten Internet Community.

Auf derselben Google-Statistikseite findet man auch die Verbreitung von IPv6 für jedes Land (Abbildung 5, Auszug mit einigen Beispielen). Schaut man sich auf der Seite etwas um, sieht man, dass in vielen Ländern die Verbreitung im Bereich von 40 % bis 60 % ist. Es gibt auch einige Länder mit einer Deployment Rate von über 70 %.

Es ist für alle Teilnehmenden im Internet von Vorteil, wenn möglichst viele Daten über IPv6 transportiert werden. Gründe dafür sind die enormen Kosten sowie die Komplexität von NAT beim Einsatz von IPv4. Darauf gehen wir im Kapitel 2.1 und 6.2.2 noch näher ein. Um das zu erreichen, müssen sowohl die Internetbenützer (User), als auch die Webseiten, die sie besuchen, dualstack sein, also sowohl IPv4 als auch IPv6 als Kommunikationsprotokoll unterstützen.

Sobald beide Kommunikationspartner IPv6 sprechen können, wird die IPv6-Strasse für den Transport bevorzugt. Das entlastet die komplexen und überlasteten IPv4 Strassen.

Dass möglichst viele User IPv6 benützen können liegt in der Verantwortung der Internetanbieter (ISPs) und der vielen Organisationen, die ihren Mitarbeitenden ebenfalls Internetzugänge über IPv6 zur Verfügung stellen sollten.

Dass möglichst viele Webseiten über IPv6 erreichbar sind, liegt in der Verantwortung der Webseitenbetreiber und ihrer gewählten Hostings und Content Delivery (CDN) Dienste.

2.2 Zurück zur Gretchenfrage

Wenn das IoT zu einem exponentiell wachsenden Bedarf an IP Adressen führt, wie lange reicht dann IPv6?

Erinnern wir uns nochmals an das Format einer IPv6 Adresse (Abbildung 6). In unserem Rechenbeispiel gehen wir von einem Global Routing Präfix von 32 bit aus. Dies bedeutet, dass ich für interne Subnetze weitere 32 bit zur Verfügung habe.

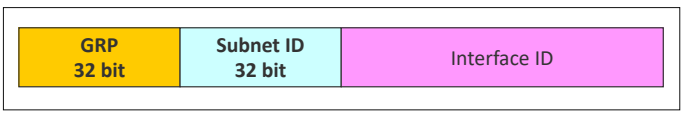


Abbildung 6: Format der IPv6 Adresse mit GRP 32 bit.
(Eigene Darstellung)

Wenn wir uns in Erinnerung rufen, dass eine IPv4 Adresse total 32 bit hat, so enthält demzufolge ein einziges /32 Subnetz deutlich mehr IPv6 Adressen als das gesamte IPv4 Internet.

Die Gretchenfrage ist damit aber noch nicht vollständig beantwortet. Schauen wir uns mal an, wie viele solcher /32 wir denn bis heute vergeben haben.

Hier eine Tabelle, die zeigt wie viele IPv6 /32 Blöcke per Juni 2022 vergeben wurden:

Registry	Zahl der /32	Prozentanteil
AFRINIC	9821	2.7%
APNIC	98 610	27.5%
ARIN	65 831	18.3%
LACNIC	16 069	4.5%
RIPE NCC	169 090	47%
Total	359 422	100%

Tabelle 3: IPv6 /32-Blöcke.
(Quelle: http://www.bgpexpert.com/addrspace-ipv6.php)

Jetzt kommen wir der Sache näher. Wir haben bis Juni 2022 total 359 422 /32 Netzwerke vergeben. Das sind also 359 422 mal mehr IPv6 Präfixe, als das IPv4 Internet Adressen hat. In dieser Zahl sind Adressen, die für IoT-Geräte beantragt wurden beinhaltet. Diese Adressen wurden zugewiesen, das heisst aber noch nicht, dass sie auch schon alle eingesetzt werden. Diese Überlegung spielt aber für die Gretchenfrage keine Rolle.

Wenn wir jetzt verstehen wollen, ob das viel ist, oder wieviel das ist, dann setzen wir es in Relation zur gesamthaft verfügbaren Zahl an IPv6 Adressen.

Als aktuell verfügbarer globaler und öffentlicher IPv6 Adressraum wurde das 2000::/3 definiert. Die Rechnung lautet also wie folgt:

Wieviel Prozent sind 359 422 /32 Blöcke von total 536 870 912 möglichen /32?

Es sind sage und schreibe 0.067%.

Wir können also getrost davon ausgehen, dass selbst bei exzessiver Nutzung von IoT-Diensten, dieser Adressraum nicht so schnell ausläuft. Und dann gilt für die kritischen Rechner zu beachten, dass wenn dieser Adressblock, das 2000::/3 erschöpft ist, noch weitere sieben /3 zur Verfügung stehen, die aktuell noch nicht zur Benutzung freigegeben sind.

2.3 Konsequenzen für die Gestaltung von IPv6 Adressplänen

Für mich sind das Zahlen in einer Grössenordnung, die ich mir nicht mehr wirklich vorstellen kann. Aber einen sehr wichtigen Hinweis möchte ich hier mitgeben, an alle, die IPv6 Adresspläne gestalten.

Ein Aspekt, der den Betrieb und die Sicherheit von IPv4 Netzwerken schwer und aufwändig macht, ist die Tatsache, dass wir den IPv4 Adressraum von 32 bit stets mit dem Adressmangel im Nacken zu optimieren versuchen. Das führt zu vielen Inkonsistenzen und fragmentierten Adressbereichen. Dieser Drang, mit IP Adressen sparsam umzugehen, sitzt uns jedoch in den Knochen. Seit Jahren ist das einer der wichtigsten Design Aspekte.

Diesen Automatismus müssen wir lernen zu «entlernen». Und ich kann aus meiner langjährigen Beratungserfahrung sagen, dass das viel schwieriger ist, als man denkt.

«Diesen Automatismus müssen wir lernen zu ‹entlernen›. Und ich kann aus meiner langjährigen Beratungserfahrung sagen, dass das viel schwieriger ist, als man denkt.»

Die wichtigste Regel lautet: Es macht keinen Sinn, einen IPv4 Adressplan auf IPv6 zu kopieren. Das geht zwar problemlos, es schränkt uns aber für alle Zukunft ein und erlaubt uns nicht, die Möglichkeiten des grossen Adressraums zu nutzen. Einer der ersten und wichtigsten Schritte beim Designen eines IPv6 Adressplanes ist es, alle Elemente in unserem vertrauten IPv4 Adressplan zu erkennen, die wir eingeführt haben, um Adressen zu sparen. Denn diese müssen wir alle entfernen für IPv6.

Die Grösse des IPv6 Adressraums verleitet gerne dazu, viele hierarchische Stufen oder Identifikationen wie Server IDs oder VLAN IDs in die Adresse einzubauen, weil es vermeintlich das Erkennen und das Troubleshooten erleichtert. In der Tat sollte man sich sehr sorgfältig überlegen, was für Elemente in der Adresse

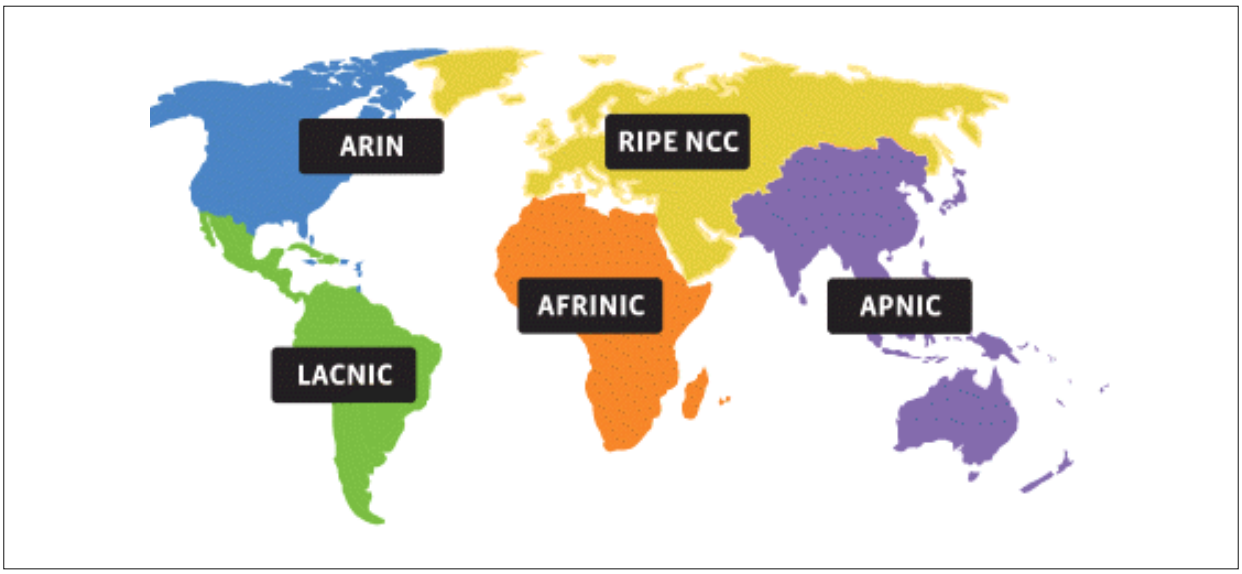


Abbildung 7: Die fünf regionalen RIRs. (Quelle: https://www.iana.org/numbers)

wirklich hilfreich sind für den Betrieb und die das Troubleshooting und die Security optimal unterstützen.

3 Organisationen und Standardisierungsprozess

3.1 Adressvergabe

Eine zentrale Organisation in der Koordination wichtiger Schlüsselfunktionen des Internets ist die die Internet Assigned Numbers Authority (IANA). Unter anderem ist sie zuständig für die globale Vergabe von IP Adressen. Seit der IPv4 Pool im Jahre 2011 auslief, koordiniert sie noch die Vergabe der IPv6 Adressen.

Es gibt fünf Regionale Internet Registries (RIRs). *AFRINIC* ist für die Afrika Region zuständig, *APNIC* für Asia/Pacific, *ARIN* für Canada, USA und einige karibische Inseln, *LACNIC* für Latein Amerika und einige karibische Inseln und *RIPE NCC* für Europa, den Middle East und Zentralasien (Abbildung 7).

Die IANA ist zuständig für die Zuweisung von Adressblöcken an die RIRs. Die RIRs wiederum sind zuständig für die Zuweisung von Adressblöcken in ihrer Region. Für uns in Europa ist RIPE NCC in Amsterdam zuständig. Weiterführende Informationen findet man auf https://www.ripe.net/.

Im Februar 2011 hat die IANA die letzten fünf Blöcke von IPv4 Adressen an die RIRs vergeben. Jede RIR hat noch einen Block erhalten.

Mittlerweile sind auch bei den RIRs die Vorräte an IPv4 Adressen aufgebraucht und auf diesem offiziellen Weg sind keine IPv4 Adressen mehr erhältlich.

3.2 Standardisierung Protokolle

Die Internet Engineering Taskforce (IETF) koordiniert den Prozess der Definition und Standardisierung aller Protokolle. Alle Informationen dazu findet man auf ihrer Website www.ietf.org.

Es gibt zu allen verschiedenen Themen IETF-Arbeitsgruppen, sogenannte WG's (Working Groups). Diese WG's sind offene Gruppen, die allen zugänglich sind. Jeder und jede kann sich in die jeweiligen Mailinglisten eintragen. Selbstverständlich sind die Hersteller gut vertreten, damit sie Einfluss auf die Protokollentwicklung nehmen können. Es wäre wünschenswert, wenn sich mehr Firmenvertreter aktiv am Prozess beteiligen würden, damit bei der Definition nicht nur die Sicht der ISPs und der Hersteller vertreten ist, sondern die Fragen auch vermehrt aus einer Anwenderperspektive diskutiert werden mit Leuten, die verstehen, was in der Unternehmenswelt die Anforderungen und Bedürfnisse sind und wo in der Umsetzung Schwierigkeiten oder Lücken bestehen.

Die Protokolle werden in diesen Arbeitsgruppen ausgearbeitet. Jemand hat eine Idee, schreibt einen ersten Draft (Entwurf). Wenn die Gemeinschaft denkt, dass das eine gute Idee ist, wird der Draft gemeinsam

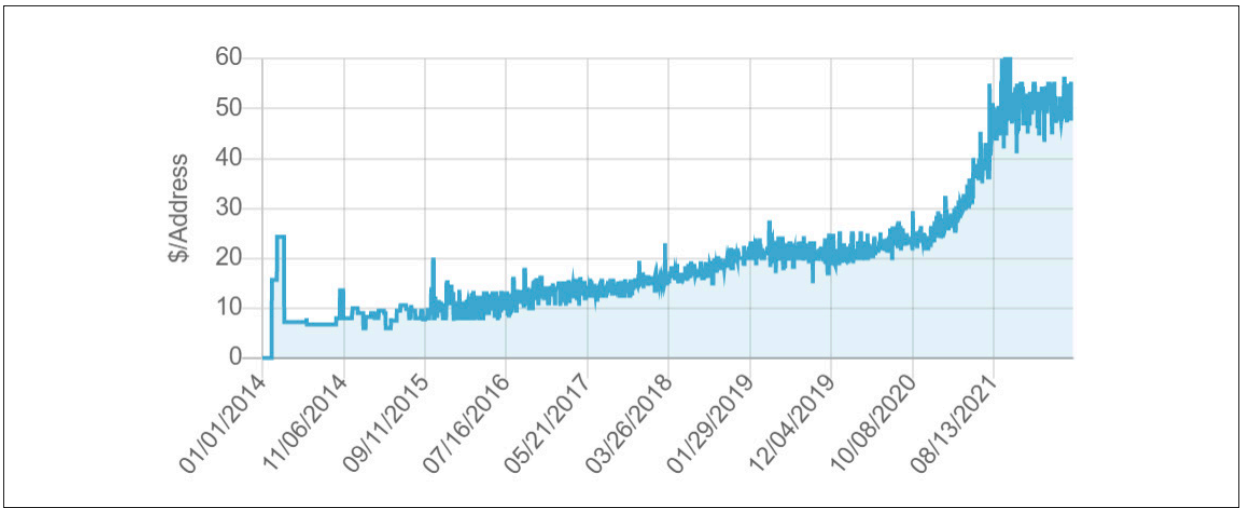


Abbildung 8: Preisentwicklung IPv4 Adressen seit 2014. (Quelle: https://www.ipxo.com/blog/ipv4-price-history/)

weiterentwickelt, bis man der Ansicht ist, er sei ausgereift für eine Publikation und die Umsetzung. Dann wird aus dem Draft ein sogenanntes RFC (Request for Comment). Diese RFCs sind dann für die Hersteller und Entwickler die Grundlage für ihre Implementation des Protokolls. Die RFCs werden fortlaufend nummeriert. Zum Zeitpunkt des Schreibens dieses Artikels (Oktober 2022) sind wir bei RFC 9321 angelangt. Mal schauen ob es eine Party gibt, wenn wir die 10›000er Grenze überschreiten.

3.3 RFCs bezüglich IP

Es gibt hunderte von RFCs die mit IP und TCP/IP zusammenhängen. Ich möchte hier einen kurzen Blick auf die RFCs, die das Grundprotokoll von IPv4 und IPv6 beschreiben werfen.

Das heutige IPv4-dominante Internet basiert auf RFC 791 aus dem Jahre 1981. IPv4 ist «End of Life» und wird nicht mehr weiterentwickelt. Es gibt nur noch Updates für kritische Probleme vor allem im Bereich Security. Der heutige aktuelle Stand für IPv6 ist RFC 8200, datiert Juli 2017. Dieses Protokoll wird weiterentwickelt.

4 Kosten und versteckte Kosten von IPv4

4.1 Einige ökonomische Gedanken zu Kosten für IP Adressen

Das führt zu einer weiteren interessanten Beobachtung: Wo erhält man heute IPv4 Adressen? Auf dem freien Markt. Es gibt viele internationale Adressbroker, die sich damit ihr Geld verdienen. Mittlerweile ist der durchschnittliche Preis einer einzigen IPv4 Adresse von ursprünglich rund 10 bis 12 USD gestiegen auf über 50 USD.

In Abbildung 8 ist die Preisentwicklung in USD seit 2014 zu sehen.

Ich weiss von einer international tätigen Organisation, die vor nicht allzulanger Zeit für einen /16 IPv4 Adressblock rund 1 Mio USD bezahlt hat. Da IPv4 auch im Betrieb, Unterhalt und im Troubleshooting deutlich höhere Kosten generiert, gehen Anbieter und ISPs allmählich dazu über, für IPv4 Dienste mehr Geld zu verlangen als für IPv6 Dienste.

So hat zum Beispiel Azure angekündigt, dass sie ab Juli 2022 für IPv4 Adressen und Präfixe mehr verlangen. Eine statische IPv4 Adresse kostet nun $ 31.50/Jahr während statische IPv6 Adressen gratis sind.

4.2 Versteckte Kosten für IPv4

Die eher schwerwiegenden Kosten für IPv4 Adressen liegen jedoch in einem nicht so transparenten Bereich. Dazu gehören:

- Komplexität der Netzwerke
- keine End-to-End Verbindungen
- hohe Risiken wegen unübersichtlicher Netzwerkarchitekturen
- Betriebsausfälle und aufwändiges Troubleshooting durch mehrfache NAT-Layers
- mangelhafte Übersicht über Datenflüsse und Nachverfolgbarkeit (Cybercrime)
- überlappende IP Adressbereiche

Ich stelle bei vielen Kunden immer wieder fest, dass die Gewohnheit einen blind machen kann für Hin-

dernisse. Die mangelnde Übersicht über die internen Netzwerke, die vielen Workarounds, die wir seit Jahren täglich benützen, die umständlichen Troubleshooting-Prozesse sind wir uns so gewohnt, dass wir sie gar nicht mehr hinterfragen und lethargisch einfach abarbeiten.

Kunden, die sich drauf einlassen und einmal etwas genauer analysieren, was dadurch für Aufwände und Kosten entstehen, sind meist höchst erstaunt. Und dann muss man sich ins Bewusstsein rufen, dass einfachere und übersichtlichere Netzwerke, die mit IPv6 gebaut wurden viele dieser Kosten hinfällig machen, dann wird die Rechnung attraktiv.

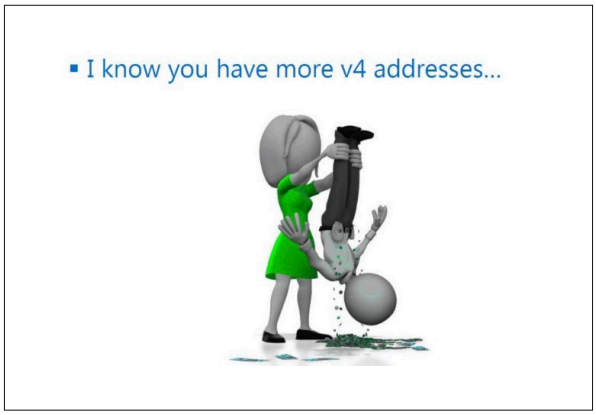
Und auch hier spielen normale menschliche Mechanismen häufig eine blockierende Rolle. IPv6 ist eben noch keine Gewohnheit und wir sind nicht vertraut damit. Das heisst, um den Weg zu einfacheren Netzwerken zu finden, müssen wir bereit sein, uns vorübergehend aus der Komfortzone herauszubewegen und uns damit vertraut zu machen. Das geht nur, wenn wir anfangen damit zu arbeiten und so praktische Erfahrungen sammeln.

Ein weiterer Hinderungsgrund kommt häufig aus der Geschäftsleitungsetage, wo man gerne einen kurzfristigen Return on Investment sieht. Wenn man mit einer Jahresperspektive oder gar, wie häufig der Fall, in Quartalen denkt, dann rechnet sich IPv6 nicht. Diese versteckten Kosten kann man erst sparen, wenn man sorgfältige Planungs- und Migrationsarbeit gemacht hat und immer mehr IPv4-Dienste und NAT-Gateways abbauen kann. Das ist ein längerer Prozess, dessen Nutzen man nur bei einer ganzheitlichen und mehrjährigen Perspektive sehen kann. Dafür zahlt er sich anschliessend exponentiell aus, weil damit jährlich hohe Beträge an Betriebs- und Supportkosten eingespart werden können.

5 Warum brauchen wir IPv6?

Nachfolgend eine kurze Zusammenfassung der wichtigsten Argumente und Kriterien.

- IPv6 ist das aktuelle Internet Protokoll (seit 2011) Das würde eigentlich bei einer sorgfältigen vorausschauenden Planung bereits ausreichen als Grund



es einzuführen. Es findet mit IPv4 kein Wachstum mehr statt.
- Der Betrieb von IPv4 wird zunehmend komplexer, umständlicher, teurer und risikobehafteter.
- Offensichtliche Hauptschauplätze bei IPv4: Mehrfach-NATs und Middleboxen; Adresskonflikte; overlapping address space; fragmentierte Netzwerke; überkomplexe Firewall Regeln.
- Investitionen in ein End-of-Life Protokoll (IPv4) sind aus betriebswirtschaftlicher Sicht nicht nachhaltig und IPv4 wird nicht weiterentwickelt.
- Der Betrieb von dual-stack Netzwerken ist unnötig aufwändig und stellt doppelte Sicherheitsrisiken dar. Es gilt wo immer möglich und sobald wie möglich auf IPv6-only zu migrieren.

«Der Betrieb von IPv4 wird zunehmend komplexer, umständlicher, teurer und risikobehafteter.»

- Das Internet of Things (IoT) wird einen exponentiellen Adressbedarf auslösen.

5.1 Wie kann IPv6 helfen?

- Ein gigantisch grosser Adressraum (2^{128}) *löst das End-zu-End Problem*. Es sind keine NATs mehr notwendig.
- Jedes Gerät kann eine oder mehrere *einzigartige (unique) Adressen* haben.
- IPv6 bietet einen *einheitlichen Subnetsize*. Dies vereinfacht Betrieb, Management und Troubleshooting (das bedeutet: Keine falschen Subnetzmasken und kein komplexes Resizing mehr).

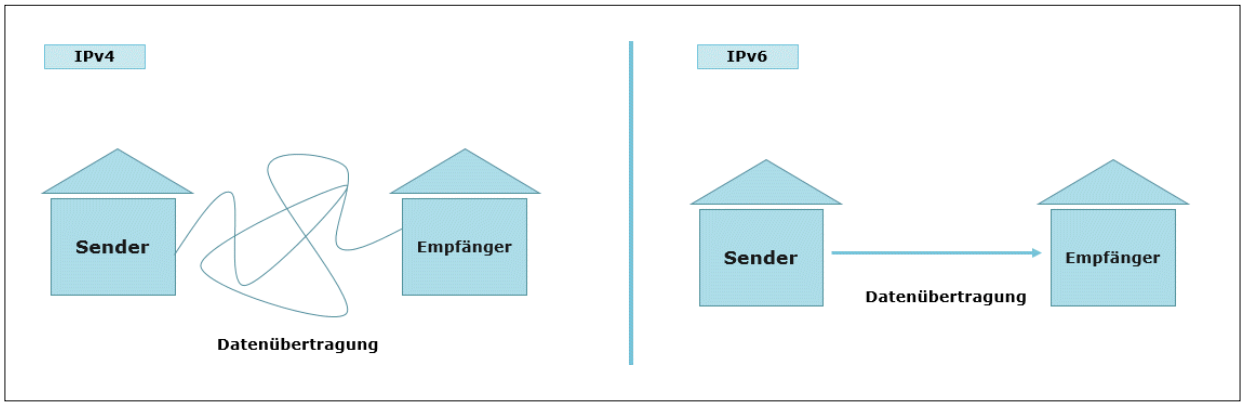


Abbildung 9: Komplexe NAT Architektur vs. End-to-End. (Eigene Darstellung)

- Es erlaubt eine *klare Struktur* des Adressbereichs mit dem Hauptfokus auf «Ease of Operation» und «Security».
- Aus Netzwerksicht ist es endlich wieder möglich, *einfachere und überschaubare Netzwerkarchitekturen* zu schaffen. Einfach im Sinne von Betrieb, Robustheit und Kosten.

> Überschaubare, klar strukturierte Netzwerkarchitekturen sind eine wichtige Grundlage für eine hohe Security und eine griffige Überwachung.

Abbildung 9 soll das stark vereinfacht visualisieren: Die linke Skizze stellt ein klassisches, heute weit verbreitetes internes IPv4 Netzwerk dar. Zwischen Sender und Empfänger herrscht aufgrund vieler NATs ein Spaghetti-Netzwerk. Die Datenflüsse sind schwer nachvollziehbar. Das Auditing ist erschwert. Der Überblick fehlt, was das Troubleshooting und vor allem auch eine schnelle Analyse bei Angriffen kompliziert und aufwendig macht.

Selbstverständlich ist IPv6 nicht der alleinige Heilsbringer, eröffnet aber die Möglichkeit einfachere Netzwerkarchitekturen zu schaffen. In einem IPv4 Netzwerk stets neue Layers von NAT und Firewalls einzubauen, erhöht die Angriffsoberfläche. Das Einführen von mehr End-zu-End Verbindungen und Übersichtlichkeit vermindert die Angriffsoberflächen.

Soviel zu den technischen Aspekten, die notwendig sind, um ein tieferes Verständnis für die Problematik zu entwickeln. Wie steht es nun aber bei der Umsetzung des IPv6 in der Schweiz?

6 Status IPv6 beim Bund und den Universitäten

6.1 Die Schweiz in der Vorreiterrolle?

In meiner Rolle als Präsidentin des Schweizerischen IPv6 Councils (eine regionale Gruppe des Internationalen IPv6 Forums), verfolge ich seit Jahren die Verbreitung von IPv6 in der Schweiz.

Im Jahre 2014 hat die ganze Welt auf die Schweiz geschaut. Genauer: die Internet-Welt. Wir waren das erste Land, das die 10 % Grenze bei der User Adoption durchbrochen hat. Dafür haben wir vom Internationalen IPv6 Forum den Jim Bound Award für World Leadership in IPv6 Deployment erhalten. Der Preis wurde uns am V6 World Congress von niemand Geringerem als von Bob Kahn (Internet Pionier) in Paris übergeben. Zu verdanken war das hauptsächlich Swisscom, die sich 2012 an dem World IPv6 Launch Day aktiv engagiert hat und seither ihren Kunden IPv6 Internet anbietet. Was haben wir draus gemacht?

6.2 Der Status in der Schweiz heute

Blicken wir nun mal auf die Statistiken. Ist die Schweiz heute ein Technologieleader? Nimmt der Bund und nehmen die Behörden eine Vorreiterrolle wahr? Sind wir ein Land mit einer modernen Infrastruktur, die sorgfältig betrieben und gut organisiert ist und wichtigen Aspekten wie Sicherheit, Aktualität, Wirtschaftlichkeit und Nachwuchsförderung die nötige Aufmerksamkeit zollt?

Im Dashboard des Swiss IPv6 Councils können wir uns einen Überblick verschaffen, über die IPv6 Verfügbarkeit von Bundeswebseiten. Das Dashboard wird mehrmals täglich aktualisiert.

6.2.1 IPv6 in der Bundesverwaltung und den Kantonen

Table 1: Several sites of the swiss federal government:

Name	Website Test	Mail Exchange Test	Nameserver Test
Bundesverwaltung (admin.ch)	FAIL	FAIL	OK
Bundesamt fuer Informatik und Telekommunikation (bit.admin.ch)	FAIL	FAIL	OK
ISB (www.isb.admin.ch)	FAIL	FAIL	OK
Bundeskanzlei (bk.admin.ch)	FAIL	FAIL	OK
Eidg. Departement für auswärtige Angelegenheiten (eda.admin.ch)	OK	FAIL	OK
Departement des Innern (edi.admin.ch)	FAIL	UNKNOWN	OK
Eidg. Justiz- und Polizeidepartement (ejpd.admin.ch)	FAIL	FAIL	OK
Verteidigung, Bevölkerungsschutz und Sport (vbs.admin.ch)	FAIL	OK	OK
Eidg. Finanzdepartement (efd.admin.ch)	FAIL	UNKNOWN	OK
Eidg. Departement für Wirtschaft, Bildung und Forschung (wbf.admin.ch)	FAIL	FAIL	OK
Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation (uvek.admin.ch)	FAIL	FAIL	OK
Bundesamt für Kommunikation (bakom.admin.ch)	FAIL	FAIL	OK
Staatskalender (staatskalender.admin.ch)	FAIL	UNKNOWN	OK
Gerichte der Schweiz. Eidgenossenschaft (eidgenoessischegerichte.ch)	FAIL	FAIL	FAIL
Bundesverwaltungsgericht (bvger.ch)	FAIL	UNKNOWN	OK
Bundesstrafgericht (bstger.ch)	FAIL	FAIL	OK
Bundespatentgericht (patentgericht.ch)	FAIL	FAIL	OK
Bundesverwaltungsgericht (bundesverwaltungsgericht.ch)	FAIL	FAIL	OK
Bundesanwaltschaft (bundesanwaltschaft.ch)	FAIL	FAIL	OK
Schweizer Behörden Online (ch.ch)	FAIL	FAIL	OK
Bundesversammlung (parlament.ch)	FAIL	FAIL	FAIL
eCH E-Government Standards (ech.ch)	FAIL	FAIL	FAIL
E-Government Schweiz (egovernment.ch)	FAIL	FAIL	OK
dotswiss Domain (dotswiss.ch)	OK	UNKNOWN	OK
Eidg. Institut für Geistiges Eigentum (ieg.ch)	OK	OK	FAIL
Bundesamt für Gesundheit (BAG) (bag.admin.ch)	FAIL	FAIL	OK
Bundesamt für Landestopografie (swisstopo.admin.ch)	FAIL	FAIL	OK
Eidg. Institut für Metrologie (METAS) (metas.ch)	FAIL	FAIL	OK
Bundesamt für Sozialversicherungen (BSV) (bsv.admin.ch)	FAIL	FAIL	OK
Bundesamt für Statistik (bfs.admin.ch)	FAIL	FAIL	OK
Eidg. Steuerverwaltung (ESTV) (estv.admin.ch)	FAIL	FAIL	OK
Staatssekretariat für Wirtschaft (SECO) (seco.admin.ch)	FAIL	FAIL	OK

Abbildung 10: IPv6 in der Schweizer Bundesverwaltung. Die erste Spalte zeigt an, welche Webseiten über IPv6 erreichbar sind (grün) und welche nicht (rot). Die zweite Spalte zeigt an, ob Email über IPv6 läuft. Ohne dass man die kleingedruckten Details lesen muss, zeigt sich ein klares Bild: Nur gerade mal drei Bereiche stellen eine positive Ausnahme dar. Das EDA, Dotswiss und das Institut für Geistiges Eigentum. (Quelle: Swiss IPv6 Council, http://dashboard.swissipv6coun-cil.ch/ipv6dashboard/government/)

Scrollt man auf derselben Seite weiter nach unten zeigt sich, wie es bei den Kantonen aussieht:

Table 2: Sites of the swiss cantons:

Name	Website Test	Mail Exchange Test	Nameserver Test
Kanton Aargau (ag.ch)	FAIL	FAIL	FAIL
Kanton Appenzell Ausserrhoden (ar.ch)	OK	FAIL	OK
Kanton Appenzell Innerrhoden (ai.ch)	FAIL	FAIL	FAIL
Kanton Basel-Landschaft (baselland.ch)	OK	UNKNOWN	OK
Kanton Basel-Stadt (bs.ch)	FAIL	FAIL	FAIL
Kanton Bern (be.ch)	FAIL	OK	OK
Etat de Fribourg (fr.ch)	FAIL	FAIL	FAIL
Genêve (geneve.ch)	FAIL	FAIL	FAIL
Kanton Genf (ge.ch)	OK	FAIL	OK
Kanton Glarus (gl.ch)	FAIL	FAIL	FAIL
Kanton Graubünden (gr.ch)	FAIL	FAIL	FAIL
Canton du Jura (jura.ch)	FAIL	FAIL	FAIL
Kanton Luzern (lu.ch)	FAIL	FAIL	OK
Canton de Neuchâtel (ne.ch)	FAIL	FAIL	OK
Kanton Nidwalden (nw.ch)	FAIL	FAIL	FAIL
Kanton Obwalden (ow.ch)	FAIL	FAIL	FAIL
Kanton Schaffhausen (sh.ch)	FAIL	FAIL	OK
Kanton Schwyz (sz.ch)	FAIL	FAIL	FAIL
Kanton Solothurn (so.ch)	FAIL	FAIL	FAIL
Kanton St. Gallen (sg.ch)	FAIL	FAIL	OK
Cantone Ticino (ti.ch)	FAIL	FAIL	FAIL
Kanton Thurgau (tg.ch)	FAIL	FAIL	FAIL
Kanton Uri (ur.ch)	FAIL	FAIL	OK
Canton de Vaud (vd.ch)	FAIL	FAIL	FAIL
Canton du Valais (vs.ch)	FAIL	FAIL	FAIL
Kanton Zug (zug.ch)	FAIL	FAIL	OK
Kanton Zürich (zh.ch)	OK	FAIL	FAIL

Abbildung 11: IPv6 in den Kantonen. Mit Ausnahme von Appenzell Ausserhoden, Baselland, Genf und Zürich scheint kein Bewusstsein fürs aktuelle Internetprotokoll vorhanden zu sein. (Quelle: Swiss IPv6 Council, http://dashboard.swissipv6coun-cil.ch/ipv6dashboard/government/)

Sogar die Webseite des BIT unterstützt kein IPv6. Die Verbindung auf www.bit.admin.ch läuft über IPv4.

Ich hoffte, dass wenigstens Bereiche, die mit eGovernment zu tun haben etwas fortschrittlicher unterwegs sind, was zu einer herben Enttäuschung führte (Abbildung 12).

Abbildung 12: digitale Verwaltung Schweiz

Das erweckt nicht den Eindruck, dass wir es hier in der Schweiz mit moderner Infrastruktur und technologischer Leadership zu tun haben. Hochmoderne Apps für ein Netzwerk mit einem ausgedienten Transportprotokoll zu entwickeln, ist wie auf ein marodes Fundament ein Haus bauen wollen.

«Das erweckt nicht den Eindruck, dass wir es hier in der Schweiz mit moderner Infrastruktur und technologischer Leadership zu tun haben.»

6.2.2 Warum spielt das eine Rolle?

Man könnte jetzt ketzerisch sagen, «das spielt doch keine Rolle, jeder Internet Teilnehmer hat doch noch IPv4 und kann diese Webseite besuchen». Das stimmt erstens nicht, da es Provider gibt, die schon so lange knapp sind an IPv4 Adressen, dass sie ihren Endnutzern IPv6-only Verbindungen anbieten müssen (und dann IPv4 über komplizierte Workarounds wie Translation zur Verfügung stellen müssen). Und zweitens hat die Verfügbarkeit von IPv6 einen nicht zu übersehenden Effekt auf die Kosten für ISPs, wie ich an folgendem Beispiel von Swisscom zeigen möchte.

Die Zahlen stammen von 2017, aber es ist das anschaulichste und nachvollziehbarste Beispiel, das von Swisscom ausgewertet wurde. Dies hat Swisscom an unserer damaligen internationalen IPv6 Konferenz in Zürich präsentiert.

100 % der Fixnet Kunden sind dual-stacked (IPv4 und IPv6)

Mehr als 35 % des Gesamttraffics ist IPv6

Die IPv4-CGNAT Infrastruktur (das ist der komplizierte IPv4-Workaround Teil) wird dank IPv6 von 9 Gb/s der Netzwerklast entlastet.

IPv6 Transport	CHF 1650.00	
CG-NAT IPv4	CHF 8000.00	(ohne Kosten für aufwendiges Logging)

Tabelle 4: Betriebskosten für 1 Gb/s Durchsatz.
(Quelle: Swisscom, 2017)

Das heisst, für Daten, die über IPv6 transportiert werden können, kostet der Betrieb rund viermal weniger, als der Transport über IPv4. Das bedeutet, um es mal aus einer Schweizer Perspektive anzuschauen, mit jeder Schweizer Website, die dual-stack, also mit IPv6 Unterstützung erreichbar ist, kann der Verkehr von User zu Website und zurück über IPv6 laufen. Das bedeutet für jeden Provider auf der Strecke deutlich weniger Kosten. Somit hilft jeder, der seine Webseite dual-stack macht mit, dass für alle das Internet schlanker und kostengünstiger wird. Ein Provider, der kein IPv6 anbietet, kann dann leider nicht profitieren, aber das ist seine Wahl. Unsere Bundesbehörden scheinen das noch nicht erkannt zu haben.

Das ist möglich, weil IPv6 automatisch das bevorzugte Protokoll ist. Das bedeutet, sobald sowohl Sender als auch Empfänger dual-stack sind, wird IPv6 für die Kommunikation gewählt. Somit schwenkt der Verkehr automatisch auf IPv6 über, wo auch immer es aktiviert wird. Das geschieht sowohl im Internet, als auch in den internen Netzwerken. So ist ein gradueller Übergang möglich. Mit jedem aufgeschalteten Service bewegt sich ein Teil des Verkehrs weg von der IPv4 Schiene auf die IPv6 Schiene.

6.2.3 Die Schweiz auf der internationalen Rangliste

Auf der Webseite von APNIC gibt es eine Rangliste von Ländern mit IPv6 Verbreitung (Abbildung 13). Die Top 10 Länder sind folgende:

CC	Country	IPv6 Capable	IPv6 Preferred
IN	India, Southern Asia, Asia	79.78%	79.42%
BL	Saint Barthelemy, Caribbean, Americas	77.27%	75.31%
BE	Belgium, Western Europe, Europe	66.04%	65.37%
MY	Malaysia, South-Eastern Asia, Asia	61.86%	60.79%
SA	Saudi Arabia, Western Asia, Asia	61.33%	60.04%
DE	Germany, Western Europe, Europe	59.89%	59.26%
FR	France, Western Europe, Europe	55.60%	55.14%
MS	Montserrat, Caribbean, Americas	54.32%	52.90%
UY	Uruguay, South America, Americas	54.17%	54.02%
LK	Sri Lanka, Southern Asia, Asia	53.39%	52.79%

Abbildung 13: Die Top 10 Länder bezüglich IPv6 Verbreitung. (Quelle: https://stats.labs.apnic.net/ipv6/)

Warum ist die Schweiz nicht unter den Top 10? Wir kommen an 30. Stelle, nach Portugal.

6.2.4 IPv6 in der Ausbildung

Wenn es um Vorreiterrolle, Technologie-Leadership und Wirtschaftlichkeit geht, spielt Aus- und Weiterbildung sowie Nachwuchsförderung eine wesentliche Rolle. Die Jungen sind unsere Zukunft. Die Wirtschaft braucht, um konkurrenzfähig zu sein, aktuelle Informatik und moderne Systeme. Also sollte ein Augenmerk auch darauf gelegt werden, in der Ausbildung dafür zu sorgen, dass die diesbezüglich wichtigen Kompetenzen vermittelt werden.

Wenn wir uns die Statistik der Webseiten für einige Schweizer Universitäten anschauen, ergibt sich ein ähnliches Bild wie bei der Verwaltung. Mit Ausnahme der Universität Bern, der ETH, dem EPFL und den Universitäten St. Gallen und Tessin sind alle Universitätswebseiten nur über IPv4 erreichbar.

Eine Webseite dual-stack zur Verfügung zu stellen, ist ein No-Brainer und in vielen Fällen recht einfach zu bewerkstelligen. Aus der Tatsache, dass dies hier nicht gemacht wird, schliesse ich, dass das Thema IPv6 auch in der Ausbildung nicht oder nur rudimentär behandelt wird. Wer Interesse hat, kann hier mal etwas nachforschen, ich lass mich gern eines Besseren belehren.

> Wir reden von moderner IT, von eGovernment, von Digitalisierung, von Clouddiensten, von E-ID und setzen nicht mal das aktuelle Internetprotokoll ein?

Schaut man sich in der vierjährigen Informatik Grundausbildung um, ergibt sich ein ähnliches Bild. Eine Nachfrage bei einigen kantonalen Ausbildungsstätten und bei ICT Berufsbildung Schweiz hat ergeben, dass das Thema IPv6 tatsächlich im Lehrplan nicht offiziell verankert ist und es den einzelnen Berufsschulen überlassen ist, ob sie es anbieten oder nicht. Entsprechende Lehrmittel scheint es keine zu geben. ICT Berufsbildung Schweiz sieht keinen Handlungsbedarf. Auch die Webseite von ICT Berufsbildung Schweiz ist IPv4-only.

Es gibt vom Verband ICT Berufsbildung einen Modulbaukasten, der Handlungsziele vorgibt. Handlungsziele definieren keine Technologien, sondern Kompetenzen. Eine Kompetenz in der Grundausbildung sollte zum Beispiel sein, wie man aktuelle sinnvolle Netzwerkarchitekturen entwickelt. Hier gehört IPv6 zwingend in die Betrachtung mit rein, weil das Fach sonst inhaltlich nicht zukunftsfähig ist. Insbesondere gilt es zu verstehen, wie man Netzwerkarchitekturen in der Übergangszeit gestalten kann.

Auch bei Themen wie Netzwerkmonitoring, Cloud Services und Datacenter, Security und Applikationsentwicklung sollte IPv6 thematisiert werden.

Wenn die Schulen das nicht von sich aus mit Priorität behandeln, wäre es sinnvoll, dies in den Zielen des Lehrplans vorzuschreiben. Ich glaube, man könnte erwarten, dass Abgänger der vierjährigen Informatik-Grundausbildung wissen, dass sich das Internet und unsere Netzwerke mitten in einer grösseren Transformation befinden und mit den Grundzügen beider Protokolle vertraut sind.

Gemäss Auskunft von ICT Berufsbildung Schweiz werden die Baukastenmodule u. a. aufgrund Befragungen von Betrieben definiert. In den Betrieben sieht man anscheinend keinen Bedarf für IPv6 Ausbildung. Möglicherweise haben sich die Firmenvertreter, die diese Meinung vertreten, noch nicht ganzheitlich mit dem Thema auseinandergesetzt. Ich wage auch zu bezweifeln, dass das repräsentativ ist. Ich kenne einige grosse

Betriebe in der Schweiz, die seit Jahren an IPv6 Projekten arbeiten. Häufig sind es auch unterschiedliche Organisationsbereiche innerhalb der Organisation und die interne Kommunikation ist nicht durchgängig. Ich habe in Grossbetrieben gearbeitet, wo an grossen IPv6 Initiativen gearbeitet wurde, während naheliegende Organisationsbereiche davon noch nie gehört hatten.

«Es gibt sehr viel Hektivismus und Aufwand aufgrund von Halbwissen und Unverständnis. Wer hat heute schon die Zeit, sich mit etwas fundiert auseinanderzusetzen und sich eine eigene Meinung zu bilden?»

Dieses in der Ausbildung zu ignorieren, trägt natürlich dazu bei, dass die Einführung harzig voranschreitet. Woher soll unser Nachwuchs kommen? Ich arbeite in Betrieben, die Applikationen im IoT-Bereich entwickeln. Sensorsysteme, Steuerungssystem. Betriebe, die erkannt haben, wo es hingeht und die planen, ihre nächste Generation an Produkten für IPv6 zu entwickeln. Die brauchen Nachwuchs, der weiss worum es geht, der das in seiner Ausbildung gelernt hat.

«Es wäre schön, wenn unsere Bundesbehörden und Verwaltungen ihre Vorbildfunktion ernster nehmen würden. Sie lassen sich vom Kostendruck genauso verführen, oberflächlich zu argumentieren.»

Nach der Analyse des Umsetzungsgrads und der Aufnahme des Themas in die Lehrpläne muss leider eine ernüchternde Bilanz für die Schweiz gezogen werden. Was müsste man nun aber tun, um die Situation zu verbessern?

7 Was gibt's zu tun?

7.1 Wo sind Stolpersteine?

Die Stolpersteine, warum die Einführung von IPv6 so harzt, haben aus meiner Sicht mit allgemeinen Entwicklungen und Tendenzen zu tun, die sich auch in anderen Bereichen zeigen und die ich mit zunehmender Besorgnis beobachte.

Der allgemeine Kostendruck führt dazu, dass vieles «Quick-and-Dirty» gemacht wird. Die Menschen heute haben keine Zeit mehr, sorgfältig zu planen und zu implementieren und laufend aufzuräumen.

Es gibt sehr viel Hektivismus und Aufwand aufgrund von Halbwissen und Unverständnis. Wer hat heute schon die Zeit, sich mit etwas fundiert auseinanderzusetzen und eine eigene Meinung zu bilden? Man verlässt sich gern auf Schlagzeilen und folgt unüberlegt angeblichen Trends. Thema: Wenn alle anderen es tun, kann es ja nicht so falsch sein.

Was bei dieser Rechnung häufig übersehen wird, ist die Tatsache, dass die Kosteneinsparung bei Planung und Einführung zu einem mehrfachen an Kosten in der Zukunft führen wird. Diese Kosten erscheinen jedoch meist in einem anderen Budget und interessieren darum nicht. Diese Haltung entbehrt jedoch einer wirtschaftlichen, unternehmerischen und nachhaltigen Gesamtsicht.

Es wäre schön, wenn unsere Bundesbehörden und Verwaltungen ihre Vorbildfunktion ernster nehmen würden. Sie lassen sich vom Kostendruck genauso verführen, oberflächlich zu argumentieren. Ihre IT-Infrastrukturen werden jedoch aus Steuergeldern bezahlt und ich würde mir wünschen, dass mehr ganzheitliches Verantwortungsbewusstsein und Sorgfalt im Umgang damit sichtbar würde. Zudem ist in diesem Fall ein Sicherheitsproblem damit verbunden (Stichwort: kritische Infrastruktur).

Es wäre auch sehr hilfreich, wenn der Bund seine Kaufkraft und Budgets ins Spiel bringen würde, um die Hersteller dazu zu bringen, ihren Implementationen mehr Sorgfalt und Durchgängigkeit angedeihen zu lassen. Da fehlt noch Einiges. Auf dem Papier existieren zwar solche Anforderungen, aber solange der Bund nicht pragmatisch umsetzt und dann aus der Praxis konkrete Anforderungen stellt, bringt uns das nicht weiter.

«Die mangelhafte Grundausbildung ist ein weiteres Symptom dieser Haltung, sich nicht wirklich mit einer Thematik zu befassen und sie angemessen und ganzheitlich zu berücksichtigen.»

Als ich bei meiner Umfrage mit einer Informatik-Berufsschule sprach und sie fragte, warum sie keinen IPv6 Unterricht anbieten, wurde u. a. gesagt, dass sie in ihren Schulungsnetzen nicht mal IPv6 aktivieren können, weil das Kantonsnetz, an dem sie hängen, das nicht anbietet.

Die mangelhafte Grundausbildung ist ein weiteres Symptom dieser Haltung, sich nicht wirklich mit einer Thematik zu befassen und sie angemessen und ganzheitlich zu berücksichtigen. Was wiederum zu einer weiteren Stagnation und unnötigen Komplexitäten, Kosten und letztendlich Lethargie führt.

7.2 Was gilt es zu tun?

- *Das Endziel müssen so weitgehend wie möglich «IPv6-only» Netzwerke und Dienste sein.*
- Modernisierung all unserer Netze und Dienste auf aktuellen Stand mit einer ganzheitlichen Perspektive (das betrifft nicht nur IPv6).
- Sicherstellung einer kompetenten, aktuellen und erfahrungsbasierten Ausbildung, vor allem in der Informatik-Grundausbildung und in allen IT-Fachrichtungen.
- Aufhören, viel Papier zu produzieren und in die Umsetzung gehen. Oder anders gesagt: Weniger Bürokratie und mehr Pragmatismus.
- Die Schweiz hat seit 2008 einen IPv6 Adressplan und seit 2015 eine IPv6 Adressallokation von RIPE. Warum sieht man heute noch nichts davon?

Es wäre auch wichtig, auf breiter Ebene Aufklärung und Fachwissen in die Diskussionen der Entscheidungsträger zu bringen.

Da wird IPv6 als nicht wichtig eingestuft, in Diskussionen, in denen man nicht darüber geredet hat, was man denn meint mit IPv6. Wann ist IPv6 eingeführt? Betrachtet man ein dual-stack Netz mit beiden Protokollen als Migration? Oder ist erst ein Netzwerk das IPv6-only läuft ein migriertes Netzwerk? Wenn ich ein IPv4 Paket in ein IPv6 Paket einpacke, sogenanntes Tunneling, ist das nun IPv6 eingeführt?

Wir sind beim Thema angelangt, sich Zeit zu nehmen, sich ernsthaft mit dem Thema zu befassen und sorgfältige, kompetente Diskussionen führen und Entscheidungen zu treffen. Die Gedanken, die man sich im Rahmen einer Gesamtsicht machen müsste, gehen aber noch weiter. Sie betreffen auch ethische Fragen.

7.3 Ethik und Integrität in der Wirtschaft und Digitalisierung

Ethik und Integrität in der Wirtschaft und insbesondere im Zusammenhang mit Digitalisierung und dem Internet sind aus meiner Sicht ein höchst stiefmütterlich behandeltes Thema. Auch dieser Aspekt gehört meines Erachtens in eine Gesamtbetrachtung. Ich sehe wenig ernsthafte Auseinandersetzung mit und wenig Verständnis für die Risiken der Digitalisierung und von Artificial Intelligence (AI). Die vorhergehende Kurzanalyse bezüglich mangelhafter Auseinandersetzung mit wichtigen Themen zeigt sich auch hier – mit möglicherweise verheerenden Konsequenzen.

«Ich sehe wenig ernsthafte Auseinandersetzung mit und wenig Verständnis für die Risiken der Digitalisierung und von Artificial Intelligence (AI).»

Es gibt mittlerweile einige wissenschaftliche Untersuchungen, die aufzeigen, dass wir unsere kulturellen Prägungen, Vorurteile, Glaubenssätze in unsere künstliche Intelligenz einbauen. Das können wir gar nicht verhindern. Es herrscht ein weit verbreiteter Irrglaube, dass mit künstlicher Intelligenz (KI) alles besser wird, denn es sei «neutral». Das führt leider dazu, dass wir keine Verantwortung dafür übernehmen. Der Algorithmus wird›s schon richten. Häufig werden Entscheidungen mit weitreichenden «unbekannten» Konsequenzen gefällt.

Wir setzen heute schon KI in vielen Bereichen ein. Bei der Gesichtserkennung, bei der Vorselektion von Bewerbungen, ja sogar bei Gerichtsverfahren und Pro-

zessbeurteilungen. Was wissen wir denn darüber, wie die Algorithmen wirklich funktionieren? Sie können nur so gut sein, wie die Daten mit denen sie gefüttert werden. Es mag schon nerven, wenn wir als Frauen im Internet ständig Werbung für Kinderkleider und Schwangerschaftsmode erhalten, während den Männern Automodelle angezeigt werden. Das ist vielleicht lästig, aber nicht tragisch. Nur, wie können wir erkennen oder verhindern, dass bei unserem neuen Bewerberselektionstool nicht Frauen oder ältere Menschen benachteiligt werden, oder bei Gerichtsverfahren Menschen aus anderen Ländern benachteiligt werden? Dass bei unserer Gesichtserkennungssoftware Gesichter von bestimmten Bevölkerungsgruppen oder mit anderer Hautfarbe eher eine höhere Anzahl Übereinstimmung mit Verbrecherfotos haben? Tausend Fragen. Ein unüberlegter Einsatz von KI Systemen in solchen kritischen Bereichen kann sehr gefährlich werden.

Das bedeutet, dass KI-Algorithmen also nicht automatisch vorurteilsfrei sind. Sie können unsere menschlichen Vorurteile spiegeln oder sogar verstärken. Und sie können bei schlechter Absicht auch manipulativ eingesetzt werden. Ich habe mich bisher mit diesem Thema noch nicht vertieft auseinandergesetzt und will darum hier keine neurologische Abhandlung über kognitive Verzerrungen in unserer Wahrnehmung und deren Spiegelung in KI Algorithmen schreiben. Das könnte für mich ein nächstes Forschungsgebiet werden, ich finde das sehr spannend.

Ich erwähne es hier in diesem Artikel, weil diese Fragestellungen unbedingt in eine gesamtheitliche Betrachtung bei der Einführung der Digitalisierung in unseren Behörden- und Verwaltungsnetzwerken gehören. Ich hoffe, dass die zuständigen Fachleute beim Bund sich die Zeit nehmen, das gründlich zu erforschen und zum Besten der Bevölkerung einzusetzen.

Es gibt eine Reihe von Artikeln, die sich als Einstiegslektüre eignen.[1]

Der Artikel auf Science.org ist von drei Wissenschaftlern von der Princeton University. Hier das Abstract, von mir auf Deutsch übersetzt. Es fasst die Grundproblematik gut zusammen:

«Maschinelles Lernen ist ein Mittel zur Gewinnung künstlicher Intelligenz durch die Entdeckung von Mustern in vorhandenen Daten. Hier zeigen wir, dass die Anwendung maschinellen Lernens auf gewöhnliche menschliche Sprache zu menschenähnlichen semantischen Verzerrungen führt. Wir haben ein Spektrum bekannter Verzerrungen, die mit dem Impliziten Assoziationstest gemessen wurden, mit einem weit verbreiteten, rein statistischen Modell für maschinelles Lernen reproduziert, das auf einem Standardtextkorpus aus dem World Wide Web trainiert wurde. (…) Unsere Ergebnisse zeigen, dass Textkorpora wiederherstellbare und genaue Abdrücke unserer historischen Voreingenommenheit enthalten, ob moralisch neutral wie bei Insekten oder Blumen, problematisch wie bei Rasse oder Geschlecht oder sogar einfach wahrheitsgemäss, indem sie die Status-quo-Verteilung von Geschlecht in Bezug auf Karrieren oder Vornamen widerspiegeln. Unsere Methoden sind vielversprechend, wenn es darum geht, Quellen für Vorurteile in der Kultur, einschliesslich der Technologie, zu identifizieren und zu korrigieren.»

7.4 Was bedeutet das alles für eine gesunde Entwicklung in der Schweiz?

Hier einige Impulse, welche Fragen in der Schweiz gestellt und sorgfältig diskutiert werden müssen, um unser Internet, unsere Sicherheit und unsere Wirtschaft möglichst sinnvoll weiterzuentwickeln.

«Hier einige Impulse, welche Fragen in der Schweiz gestellt und sorgfältig diskutiert werden müssen, um unser Internet, unsere Sicherheit und die ökonomische Entwicklung möglichst sinnvoll weiterzuentwickeln.»

Einer der wichtigen Aspekte ist aus meiner Sicht, dass wir in erster Linie unsere Autonomie im Fokus haben. Das hat vielschichtige Aspekte. Es fängt auch bei unserer Datensicherheit an. Wo legen wir unsere Daten ab? In wessen Hoheit sind sie? Wer kann darüber verfügen, sie benützen, sie weitergeben oder weiterverkaufen? Haben wir die Kontrolle darüber?

Ich habe einen Kollegen in der Schweiz, der eine Autogarage eines amerikanischen Autoherstellers besitzt. Er braucht als Partner einen Vertrag und Autorisierung, um auf einen zentralen Server in den USA zugreifen zu können. Wartungsarbeiten kann er nur mit

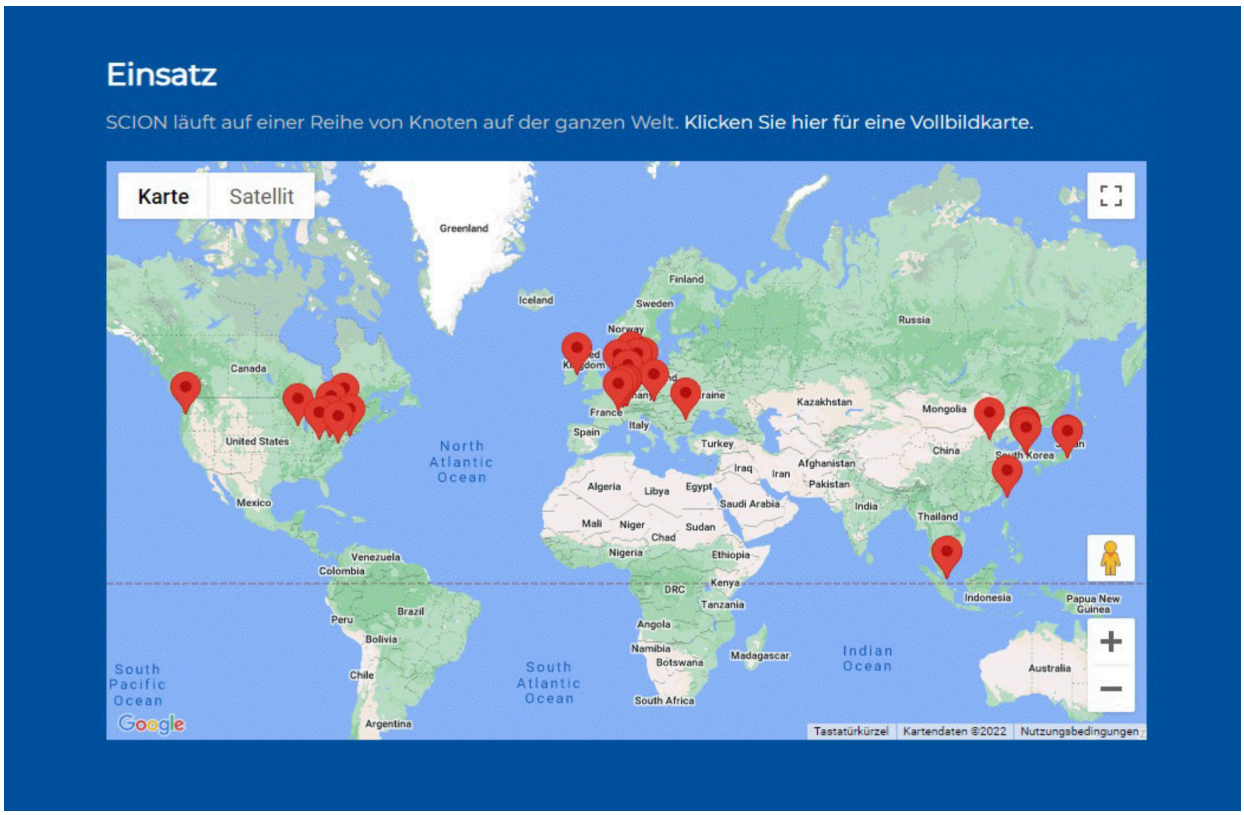


Abbildung 14: Das SCION Netzwerk. (Quelle: https://scion-architecture.net/)

einer laufenden online Verbindung zu diesem Server machen. Fällt diese Verbindung aus irgendeinem Grund aus, so kann er nicht arbeiten. Vielleicht ein relativ harmloses Beispiel, aber es zeigt, was ich meine.

Wenn Sie ein Rechenzentrum in Russland hatten, wurde das möglicherweise abgestellt. Was ist dabei mit ihren Daten geschehen? Was geschieht, wenn die Daten der Schweiz in ausländischem Besitz sind im Krisenfall? Was geschieht, wenn die Schweiz ihre Daten in eine Google AWS Cloud oder eine Microsoft Azure Cloud gibt? Verträge können uns nicht vor Datenklau schützen. Wenn es um sensible Daten wie die der Schweizer Armee oder Eidgenossenschaft geht, so gehören die nicht in unkontrollierbare Hände. Ein Staat muss im Informationszeitalter, wo Strom, Wasser, und die gesamte Infrastruktur ohne IT kaum noch sinnvoll gesteuert werden können, seine digitale Souveränität und Handlungsfähigkeit sicherstellen. Wenn wir entdecken, dass Missbrauch entstanden ist, ist es zu spät. Endlose, jahrelange juristische Prozesse retten uns dann nicht.

Militärische Angriffe werden immer mehr im Cyberspace geführt. Davor können uns die teuersten Kampfflugzeuge nicht schützen. Cyberangriffe auf Flugzeuge, Autos oder die kritische Infrastruktur wie beispielsweise Spitäler, Staudämme oder Kernkraftwerke sind gefährliche und realistische Szenarien. Nordkorea und Russland haben fitte Hackertruppen, die Chinesen bestimmt auch. Die Entdeckung von Stuxnet im Jahre 2010 war ein erstes bekanntes Beispiel einer Cyberattacke. Zielscheibe war das nukleare Programm des Irans. Stuxnet benützte zur Verbreitung Computer mit Microsoft Windows Betriebssystemen.[2] International grosses Aufsehen erregte auch der Angriff auf das Stromnetz der USA, durch Lahmlegung der Colonial Oelpipeline, die wichtigste Versorgungsleitung des Landes für Strom, Diesel und Kerosin. Oder der Versuch, Trinkwasser in einer Aufbereitungsanlage im US-Bundesstaat Florida per Hacker-Angriff chemisch zu manipulieren. Dies wurde zum Glück sofort entdeckt und konnte damit rückgängig gemacht werden. Auch in der Schweiz sind Angriffe auf die Trinkwasserversorgung bekannt.[3]

«Militärische Angriffe werden in Zukunft vermehrt im Cyberspace laufen. Davor können uns die teuersten Kampfflugzeuge nicht schützen.»

Ein wichtiger Aspekt, uns zu schützen ist es, die Möglichkeit zu haben oder zu schaffen, dass unsere Behörden eine direkte Kommunikationsmöglichkeit untereinander haben (und allenfalls auch mit Nachbarstaaten), die *nicht* übers Internet gehen. In der Schweiz bestehen solche Bestrebungen Dabei wird ein von der ETH entwickeltes System, SCION genannt eingesetzt (Abbildung 14).

SCION wurde von der ETH entwickelt und ist die erste reine Internetarchitektur, die entwickelt wurde, um Routensteuerung, Fehlerisolierung und explizite Vertrauensinformationen für die End-to-End-Kommunikation bereitzustellen.[4]

SCION wird heute schon von der Nationalbank eingesetzt für Inter-Bankenverkehr. Wie im November angekündigt wurde, testet auch das VBS das SCION -Netzwerk für die Cyberabwehr.[5]

7.5 Beispiele

Es gibt Sicherheitslücken oder sogar beabsichtigte Schwachstellen in Hardware und Software. Von Facebook ist bekannt, dass sie keine Router und Switches einkaufen. Sie bauen sie selber, weil sie weder den Amerikanern noch den Chinesen trauen. US-Geheimdienste sammeln Sicherheitslücken. Sie werden nicht bekanntgemacht, damit sie später für Angriffe verwendet werden können und der Schwarzmarkt für Kauf und Verkauf von Schwachstellen blüht.[6]

Wer sich damit näher befassen möchte, kann als Einstieg folgendes Dokument lesen:

SWP-Studie von Mathias Schulze, «Governance von o-Day-Schwachstellen in der deutschen CyberSicherheitspolitik»[7]

Einige Beispiele, die nachdenklich stimmen:

- *Uni Berlin – Active Directory wurde kompromittiert.* Brauchten 1.5 Jahre bis IT wieder einigermassen lief. Sie durften keine Experten beiziehen (Policy). Sie mussten ihre Lohnbuchhaltung händisch kontrollieren und brauchten drei Monate bis sie wieder Zugriff hatten.
- *Crypto AG Affäre Schweiz*
  Spionageelemente in Geräte eingebaut und Daten an CIA geliefert.[8]
- Cisco hat mit einem NSA-Auftrag ausspionierte Daten geliefert.
- Neuere Handys mit Android oder iOS sammeln laufend Daten. Viele Apps für Smartphones sammeln ungeniert Daten. Auch Microsoft Betriebssysteme sind sehr effizient im Daten abholen. Selbstverständlich nur zu unserer Sicherheit.

Aufgrund vieler solcher Beispiele kann man nicht ausschliessen, dass Daten, die in AWS Cloud von Google oder Azure Cloud von Microsoft abgelegt werden, auf relativ einfachem Weg von CIA und NSA abgerufen werden können. Diese haben dazu genügend Instrumente. Darum wäre es ratsam, in allen Bereichen wo es um staatliche Organe und kritische Infrastrukturen geht, von solchen Verträgen abzusehen und die Daten in einem Bereich abzulegen, in dem wir als Schweiz die volle Autonomie und Kontrolle haben.

Zusammenfassend möchte ich sagen, dass moderne Netze und Cybersicherheit eine sehr vielschichtige Struktur auf verschiedenen Stufen haben, angefangen bei Hardware bis zu Strategien und ethischen Aspekten. Keine der Ebenen kann allein für Sicherheit sorgen. Der beste Schutz ist es, auf allen Ebenen die angemessenen Massnahmen professionell zu ergreifen und betreiben – sich zu kümmern. So ergibt sich im Gesamt-Zusammenspiel der bestmögliche Schutz. ◆

Endnoten

1 Hier drei Beispiele: https://data-science-blog.com/blog/2018/12/27/kunstliche-intelligenz-und-vorurteil/; https://www.statworx.com/content-hub/blog/vorurteile-in-ki-abbauen/; https://www.science.org/doi/full/10.1126/science.aal4230.

2 https://en.wikipedia.org/wiki/Stuxnet

3 https://www.tagesanzeiger.ch/diese-hacker-attacke-sorgt-fuer-nervositaet-895024024835

4 Für Informationen: https://scion-architecture.net/.

5 https://www.ar.admin.ch/de/home.detail.news.html/ar-internet/news-2022/news-w-t/scion-netzwerk.html

6 Wer sich damit näher befassen möchte, kann als Einstieg folgendes Dokument lesen:

SWP-Studie von Mathias Schulze, «Governance von 0-Day-Schwachstellen in der deutschen CyberSicherheitspolitik».https://www.swp-berlin.org/publications/products/studien/2019S10_she.pdf

7 https://www.swp-berlin.org/publications/products/studien/2019S10_she.pdf

8 https://de.wikipedia.org/wiki/Crypto_AG

Literatur- und Linkverzeichnis

IPv6 Essentials, von Silvia Hagen, O'Reilly, English
https://www.amazon.de/-/en/Silvia-Hagen/dp/1449319211/

IPv6 – Grundlagen, Funktionalität und Integration, Silvia Hagen, Sunny Edition
https://www.amazon.de/-/en/Silvia-Hagen/dp/3952294233/

Diese 7 Apps lesen Ihre E-Mails mit:
Dieser Artikel zeigt auf wie viele Email Apps für Android alles mitlesen und zeigt, welche Firmen dahinterstehen und wie sie miteinander verbandelt sind.
https://mobilsicher.de/ratgeber/apps-gecheckt-diese-7-e-mail-apps-lesen-mit

App-Anbieter kommen DSGVO-Auskunftspflicht nur unzureichend nach:
Im Interview sprechen wir mit dem Wirtschaftsinformatiker Jacob Kröger darüber, wie App-Anbieter mit Anfragen zu gespeicherten personenbezogenen Daten umgehen. Ergebnisse einer mehrjährigen Undercover Studie.
https://www.weizenbaum-institut.de/news/app-anbieter-kommen-dsgvo-auskunftspflicht-unzureichend-nach/

Konzepte für Datensicherheit und Datenschutz in mobilen Anwendungen:
Von der Fakultät für Informatik, Elektrotechnik und Informationstechnik der Universität Stuttgart
https://elib.uni-stuttgart.de/bitstream/11682/9541/1/thesis_c_stach.pdf

Google IPv6 Statistik:
https://www.google.com/intl/en/ipv6/statistics.html

World IPv6 Launch Day, 6. Juni 2012 – historische Website:
https://www.worldipv6launch.org/

Cisco 6lab Statistik, globale Verbreitung von Websites die über IPv6 erreichbar sind:
https://6lab.cisco.com/stats/index.php?option=content

RIPE NCC – Internet Registry für Europa:
https://www.ripe.net/

Beschreibung des RFC Prozesses der IETF:
https://www.ietf.org/standards/rfcs/

Übersicht und Verlinkung aller RFCs:
https://www.rfc-editor.org/

Künstliche Intelligenz und Ethik:
https://data-science-blog.com/blog/2018/12/27/kunstliche-intelligenz-und-vorurteil/
https://www.statworx.com/content-hub/blog/vorurteile-in-ki-abbauen/
https://www.science.org/doi/full/10.1126/science.aal4230

SCION, von ETH entwickelt:
https://scion-architecture.net/

The Iran Firewall:
https://blog.thc.org/the-iran-firewall-a-preliminary-report

50 Ways to Leak your Data:
https://www.ftc.gov/system/files/documents/public_events/1415032/privacycon2019_serge_egelman.pdf

SWP Studie von Mathias Schulze, «Governance von 0-Day-Schwachstellen in der deutschen CyberSicherheitspolitik»
https://www.swp-berlin.org/publications/products/studien/2019S10_she.pdf