Chaos Computer Club

Stellungnahme zum Routerzwang

an die Bundesnetzagentur

5. November 2013

Einleitung

Mit einer Pflicht zur Verwendung eines bestimmten, vom Hersteller konfigurierten und damit nicht änderbaren Routers würden die Nutzer in Verhaltensmuster aus Zeiten vor der Liberalisierung des Kommunikationsmarktes zurückgeworfen. Bis zur Liberalisierung des Telekommunikationsmarktes im Jahre 1989 befand sich der Netzabschlußpunkt jedes Teilnehmeranschlusses im Endgerät der Deutschen Post. Dies bedeutete, daß alle vom Teilnehmer betriebenen Endgeräte in den Hoheitsbereich der Deutschen Post fielen und vom Benutzer nicht verändert werden durften. Entsprechend verblieb das Telefon stets im Besitz der Deutschen Post, andere Geräte waren nicht zugelassen.

Da die Post ein großes Interesse an der Einheitlichkeit ihrer Infrastruktur hatte, mangels Wettbewerb aber keine Notwendigkeit bestand, das Netz dem aktuellen Stand der Technik anzupassen, befand sich das Netz zum Zeitpunkt der Liberalisierung auf dem technologischen Stand der späten 1960er Jahre. In den meisten Unternehmen und Haushalten befanden sich Endgeräte des Typs FeTAp 61(1), einem Modell, das seit seiner Einführung im Jahre 1963 nur wenige Änderungen erfahren hatte.

Mit der Liberalisierung wurde der Netzabschlußpunkt an die TAE-Dose verschoben. Dies ermöglichte den Anschlußteilnehmern nicht nur den Einsatz moderner Fernsprechapparate (beispielsweise schnurlose Telefone), sondern auch den Betrieb preisgünstiger Modems, die den Einsatz von Datenfernübertragung für eine breite Bevölkerungsgruppe zugänglich machte. Die Wurzeln des großen Erfolgs der Internettechnologie sind auch hier zu suchen.

Die freie Wahl des Endgerätes gibt jedem Anschlußteilnehmer die Möglichkeit, den Zugang zum Internet seinen Wünschen gemäß zu gestalten. Privatanwendern erlaubt dies, sich aus einem breiten Angebot frei zu entscheiden und das jeweils zu den eigenen Bedürfnissen angepaßte Angebot zu wählen.

Für Unternehmen spielt dazu oft die Abstimmung von unternehmensinternen Standards eine Rolle. Unternehmen, die unterschiedliche Standorte vernetzen wollen, sind in vielen Fällen von der Interoperabilität der eingesetzten Hardware abhängig, daher soll an unterschiedlichen Standorten jeweils die gleiche Hardware zum Einsatz kommen. Die freie Wahl der Endgeräte spielt daher auch für Unternehmen eine große Rolle.

Da Standortvernetzung zunehmend auch für kleinere Unternehmen von Bedeutung ist, die aus wirtschaftlichen Gründen einen ADSL-Anschluß verwenden, wie ihn auch Privatpersonen einsetzen, würden sie durch den zwangsweisen Einsatz eines bestimmten Routers eingeschänkt und gegenüber größeren Mitbewerbern benachteiligt.

Netzneutralität

Die Kontrolle der Endgeräte durch den Zugangsanbieter kann auch genutzt werden, um Verletzungen der Netzneutralität gleich in die Endgeräte einzubauen. So könnten beispielsweise Peer-To-Peer-Dienste oder Telefonieangebote direkt am Router gesperrt werden oder Inhaltsangebote von Mitbewerbern gegenüber den Angeboten des Zugangsanbieters verlangsamt werden. Besonders im Zusammenspiel mit der geplanten „Geschwindigkeitsdrossel“, wie nicht nur der Telekom-Konzern sie noch immer plant, sind sehr feinkörnige Einflußnahmen auf das Benutzerverhalten möglich.

Sicherheit

Da die meisten Zugangsanbieter aus Kostengründen die Routerhardware eines einzelnen Herstellers verwenden, würden vereinheitlichte Zwangsrouter ein deutlich größeres Sicherheitsrisiko darstellen als bisher. Bislang gibt es eine sehr große Vielfalt an unterschiedlichen Geräten mit den unterschiedlichsten Patch-Zuständen. Für potentielle Angreifer erschwert dies den Zugang, da für jeden einzelnen Anschluß eine Sicherheitslücke gesucht werden muß beziehungsweise mit einem bekannten Exploit eine geringe Reichweite zu erwarten ist.

Wenn die Mehrzahl der Anschlußinhaber dieselbe Hardware mit derselben Softwareversion verwenden, sind Angriffe auf Netzinfrastrukturen im großen Stil möglich: Ein einzelner Angriff kann ganz einfach gleichzeitig gegen Millionen Endgeräte angewendet werden. Daß solche Angriffe bereits automatisiert Anwendung finden, zeigen die Snowden-Enthüllungen, aus denen hervorgeht, daß der US-amerikanische Geheimdienst NSA mit „FoxAcid“ systematisch Schwachstellen in Routern ausnutzt, um Datenverkehr umzuleiten. Der Schaden, der durch einen erfolgreichen Angriff entstehen kann, ist also nicht nur erheblich, sondern durchaus bereits heute real.

Darüberhinaus wird dieser Angriffstyp auch für weitere Entitäten wirtschaftlich, da die einzusetzenden Mittel deutlich kleiner wären und der zu erwartende Nutzen gleichzeitig sehr viel größer als bisher.

Zudem führt die Fremdkontrolle des Routers zu rechtlichen Problemen: Bisherige Rechtspraxis ist, daß der Anschlußinhaber etwa bei Urheberrechtsverletzungen haftet, wenn der eigentliche Verletzer nicht zu ermitteln ist.

Hat aber der Anschlußinhaber keine Möglichkeit mehr, selbst für die Sicherheit seines Netzes zu sorgen, müßte konsequenterweise in diesem Fall der Zugangsanbieter als Betreiber des Endgerätes haften. Das jedoch sieht die derzeitige Rechtslage nicht vor. So könnte am Ende der Anschlußinhaber die Haftung für ein technisches System übernehmen, auf dessen Funktion er keinerlei Einfluß hat.

Grundsätzlich ist festzustellen: Wenn der Nutzer den Strom für das Gerät bezahlt, sollte er selbstverständlich auch bestimmen, was darauf läuft.

Fragen der Bundesnetzagentur:

Wie bewerten Sie in diesem Zusammenhang, daß bis heute bei xDSL von manchen Netzbetreibern als Netzzugangsschnittstelle der direkte Anschluß an die Kupferdoppelader an der TAE beschrieben wird?

Wir betrachten diese Vorgehensweise als Idealfall für den Anwender von Netzwerkdiensten. Der direkte Zugang ermöglicht dem Anschlußinhaber die größtmögliche Freiheit bei der Nutzung seines Netzwerkzugangs. Da die xDSL-Protokolle anerkannte Standards erfüllen, ist der Betrieb von Leitungsabschlußgeräten beliebiger Bauart möglich, die den Standard erfüllen. Damit erhält der Anschlußinhaber die Möglichkeit, Hardware einzusetzen, die seinen individuellen Bedürfnissen entspricht. Auch ein Austausch der Hardware ist zu jedem Zeitpunkt problemlos möglich. Der direkte Zugang zu den niedrigen Ebenen des xDSL ermöglicht auch den Einsatz offener Hard- und Software, die vom Benutzer an dessen Bedürfnisse angepaßt werden kann.

Welche Bestandteile eines Leitungsabschlußgeräts im Sinne der Modelle B1 bis B3 müssen zwingend integriert sein, um eine fehler- und störungsfreie Interaktion mit weiteren Netzelementen zu ermöglichen? Auf welche OSI-Layer erstrecken sich die Funktionen?

Alle Leitungsabschlußgeräte müssen den Anschluß verschiedener Geräte zulassen (PCs/Notebooks, Spielkonsolen, Mobilgeräte). Hierbei sind grundsätzlich offene Standards zu verwenden, damit der Anschluß von Geräten diskriminierungsfrei möglich ist. Bei heutigen Geräten kommen dafür in der Regel Schnittstellen der Norm IEEE802.3 (Ethernet) und IEEE802.11 (Wireles-LAN) zum Einsatz. Viele Geräte verfügen darüberhinaus noch über weitere Schnittstellen, etwa USB.

Für den störungsfreien Betrieb und die Interaktion von Abschlußgeräten und anderen Netzwerkkomponenten sollten nur offene, nicht-proprietäre Standards eingesetzt werden, da nur die Offenheit aller Schnittstellen die Kompatibilität und Interoperabilität garantieren kann.

Dabei müssen alle Standards auch deshalb frei und offen gehalten werden, um allen Marktteilnehmern einen gleichberechtigten Zugang zu den verwendeten Technologien zu ermöglichen. Lizenzpflichtige, unfreie Industriestandards sind daher abzulehnen.

Welche technischen Vor- und Nachteile sehen Sie insgesamt bei Anwendung a) des Modells A?

Vorteile:

- Das Modell bietet dem Anschlußinhaber die größte Wahlfreiheit. Er kann diejenigen Leitungsabschlußgeräte verwenden, die seinen Bedürfnissen am besten entsprechen.
- Die Verwendung offener Standards und die freie Gerätewahl erleichtern den Kunden den Anbieterwechsel, was wiederum den Wettbewerb zwischen den Zugangsanbietern befördert.
- Die freie Auswahl an Geräten öffnet den Markt für Endgeräte für einen fairen Wettbewerb, was positiv auf Innovationen wirkt.
- Eine diversifizierte Landschaft an Endgeräten erhöht die Sicherheit der verwendeten Netze, da das Ausnutzen von Schwachstellen in einer monokulturellen Landschaft wesentlich vereinfacht wird: Ein einzelner Fehler kann von Angreifern verwendet werden, um eine Vielzahl von Endnutzern anzugreifen. Da die verwendete Hardware in so einem Szenario leicht zu identifizieren ist, kann ein einziger Fehler erhebliche Schäden verursachen.
- Die Nutzung und der Aufbau freier und offener Netzwerkstrukturen wird gefördert, da die entsprechenden Technologien vom Anschlußinhaber einfach verwendet werden können.

Nachteile:

- Der Supportaufwand auf Seiten der Provider kann gegenüber den Modellen B2 und B3 leicht erhöht sein, und das im Support arbeitende Personal muß besser ausgebildet sein. Das schadet jedoch ohnehin nicht.

b) des Modells B1?

Vorteile:

- Die Wahlfreiheit des Endgerätes für den Anschlußinhaber nach dem Modem bleibt erhalten.
- Die Verwendung offener Standards und die freie Gerätewahl bleiben weitgehend erhalten, da nur die Grundfunktionen vom Modem vorgegeben werden.
- Die Diversität der Endgeräte und die daraus resultierende verbesserte Sicherheit bleiben erhalten, da Angriffe sich normalerweise gegen höhere Abstraktionsschichten des Netzwerkprotokolls richten.
- Durch die freie Wahl der Nutzung von Geräten bleiben auch die Möglichkeiten der Implementierung freier Netzwerkstrukturen erhalten.

Nachteile:

- Der Support-Aufwand wird nicht reduziert, da die meisten Konfigurationsoptionen die höheren Schichten der Netzwerkprotokolle betreffen und naturgemäß hier die meisten Probleme und Fragen auftreten.
- Wenn Modemhersteller sich nicht an gängige Standards halten, kann es zu Problemen mit der Kompatibilität der Endgeräte kommen.
- Da bei einem Providerwechsel das Modem ausgetauscht werden muß, eine Weiterverwendung des zu dem Zeitpunkt meist veralteten Modems für den ursprünglichen Provider in der Regel wirtschaftlich uninteressant ist, entsteht mehr Elektronik-Abfall.

c) des Modells B2 d) des Modells B3

Vorteile:

- Der Support-Aufwand für den Provider ist möglicherweise geringer, weil die Geräte einheitlich sind, vorkonfiguriert ausgeliefert werden und meistens „Out-Of-The-Box“ in Betrieb genommen werden können.

Nachteile:

- Der Kunde hat keine Wahlfreiheit über die verwendeten Endgeräte. Damit wird auch die Nutzbarkeit verfügbarer Dienste eingeschränkt, weil der Kunde nur nutzen kann, was das Engerät unterstützt. So ist beispielsweise eine Nutzung von IPv6-Diensten über einen sog. Tunnelbroker nicht möglich, wenn das gelieferte Gerät das entsprechende Protokoll nicht weiterleitet. Für Kunden, deren Provider selbst noch kein IPv6 anbieten, ist dies eine deutliche Einschränkung.
- Der Wettbewerb für Routerendgeräte wird künstlich eingeschränkt.
- Die Verwendung freier und offener Standards wird behindert, da nur die Protokolle verwendet werden können, die bereits implementiert sind.
- Der Endanwender ist von Wartungsintervallen der Zugangsanbieter abhängig. Fehler und Sicherheitslücken können erst behoben werden, wenn der Zugangsanbieter dies durchführt. Im Zusammenspiel mit der entstehenden Monokultur führt dies zu erheblichen Sicherheitsproblemen.
- Da bei einem Providerwechsel das Endgerät in der Regel nicht weiterverwendet werden kann, entsteht auch hier unnötig Abfall, der die Umwelt belastet.

Bitte differenzieren Sie dabei zwischen unterschiedlichen Zugangstechnologien (insbesondere xDSL, HFC, FttB/H sowie stationär genutzte Funklösungen).

Eine Differenzierung zwischen den unterschiedlichen Zugangstechnologien ist für die genannten Vor- und Nachteile nicht von Bedeutung. Für alle Zugangstechnologien steht Nutzern eine breite Auswahl verschiedener Endgeräte zur Verfügung. Entscheidendes Kritierum ist daher nicht die Art der Zugangstechnologie, sondern der Ort des Netzwerkendpunktes (vor oder hinter dem Endgerät).

Welche wettbewerblichen (wirtschaftlichen) und eventuelle weitere Vor- und Nachteile sehen Sie mit Blick auf die vorgestellten Modelle? a) des Modells A?

Das Modell A bietet dem Endkunden die größte Wahlfreiheit. Aus wettbewerblicher Sicht befördert dies die Vielfalt der am Markt verfügbaren Geräte. Die Nutzung offener Standards fördert dazu die Innovation neuer Technologien, da Anbieter vielfältige neue Funktionen entwickeln können.

Die sich aus dem Wettbewerb ergebende Diversifizierung der Gerätelandschaft erhöht darüberhinaus auch die Sicherheit von Netzwerken, da es Angreifern erschwert wird, in fremde Netze einzudringen und beispielsweise Unternehmen vertrauliche Daten zu stehlen.

b) des Modells B1?

Es gelten hier dieselben Kriterien wie bei Modell A, jedoch wird der Markt für Modem- oder Kombigeräte stark eingeschränkt, was dazu führen könnte, daß der Markt sich auf einige wenige Anbieter verdichtet.

c) des Modells B2? d) des Modells B3?

Beide Modelle führen zu einer Verdichtung des Marktes, in dem ein gesunder Wettbewerb kaum möglich ist. Die Zugangsanbieter kaufen in der Regel große Bestände an Geräten bei einigen wenigen Herstellern. Da hierbei meist vor allem auf den Einkaufspreis geachtet wird, leidet darunter die Qualität der Geräte. Hersteller die etwas „vom Kuchen abbekommen“ wollen, müssen billige, leicht zu konfigurierende Geräte liefern. Sicherheit und technische Innovation stehen dabei in der Regel im Hintergrund.

Anbieter, die nicht bei einem der großen Zugangsanbieter unterkommen, könnten in wirtschaftliche Not geraten, da der Markt für Endgeräte praktisch zusammenbricht, wenn Kunden keine alternativen Geräte mehr einsetzen können.

Ein weiterer Nachteil ist die Entstehung von Monokulturen, in denen eine große Anzahl von Anwendern den gleichen Typ Endgerät benutzt. Angreifer könnten diese Strukturen übernehmen und zum Aufbau von Botnetzen nutzen, die ihrerseits für kriminelle Aktivitäten verwendet werden können. Daß dies nicht nur eine theoretische Option ist, hat sich in der Vergangenheit gezeigt.

Hinzu kommt, daß Zugangsanbieter aus Kostengründen auf eine regelmäßige Aktualisierung von Hard- und Software oftmals verzichten.

Ist es Endkunden uneingeschränkt möglich, handelsübliche DSL-Router, Breitband-Router oder Telefonie-Endgeräte (IP-Telefon, SIP-Applikation, PBX) an den oben beschriebenen Modell-Schnittstellen (A, B1 bis B3) anzuschließen und diese in ihrem vollen Funktionsumfang zu nutzen? Sofern Sie technische Probleme bei der Nutzung von Endgeräten an einem solchen Leitungsabschlußgerät identifizieren, führen Sie bitte den Grund der technischen Probleme aus.

Je nach eingesetzter Modellschnittstelle hängt es stark davon ab, welche Ziele der Zugangsanbieter verfolgt. Besonders die Modelle B2 und B3 ermöglichen eine sehr feine Steuerung der Einflußmöglichkeiten durch den Provider. So kann ein Provider, der beispielsweise daran interessiert ist, eigene Inhalts-Dienste zu verkaufen, den Zugriff auf Produkte von Mitbewerbern künstlich erschweren oder unterbinden, so wie dies im Mobilfunkbereich bereits üblich ist (technische Unterbindung etwa von VoIP-Diensten).

Ein besonders restriktiver Provider könnte sogar die Anzahl oder den Typ der im privaten Netz verwendeten Geräte beschränken und so für eine künstliche Verknappung sorgen. So haben Zugangsprovider ein Interesse, daß der Kunde möglichst wenige Geräte gleichzeitig nutzt, um den Verbrauch an Bandbreite gering zu halten.

Eine restriktive Anwendung der Modelle B2 und B3 könnte auch zu rechtlichen Problemen führen. Die derzeitige Rechtsprechung sieht eine Störerhaftung durch den Anschlußinhaber vor, etwa bei Urheberrechtsverletzungen. Diese greift beispielsweise, wenn der Anschluß nicht „marktüblich“ gesichert war, etwa durch ein starkes WLAN-Kennwort (BGH I ZR 121/08, 12. Mai 2010).

Obliegt die Kontrolle über die Konfiguration des WLAN-Routers dem Provider, so hat der Anschlußinhaber gerade keine Kontrolle mehr über die Sicherheit seines Anschlusses. Die aktuelle Rechtsprechung ließe sich so kaum aufrechterhalten. Es darf jedoch bezweifelt werden, daß die Zugangsanbieter eine Haftungsübernahme in solchen Fällen klaglos akzeptieren werden.

Wie bewerten Sie insgesamt die Implementierungschancen für die Modelle B 1 bis B 3, insbesondere mit Blick auf die mögliche Akzeptanz bei Endnutzern/Teilnehmern?

Da die Zugangsanbieter sich im Moment mit Nachdruck für die Implementierung dieser Modelle einsetzen, steht von deren Seite einer erfolgreichen Einführung wenig entgegen. Die Akzeptanz der Endkunden wird in der derzeitigen Lage davon abhängen, wie einfach die Installation ihres Zugangs vorzunehmen ist. Die Nachteile von Zwangsroutern sind vor allem mittel- und langfristig und treten für den Endanwender erst zu Tage, wenn bereits eine Vertragsbindung besteht. Hinzu kommt, daß besonders in ländlichen Regionen die Auswahlmöglichkeiten sehr beschränkt sind, so daß Kunden sich ihren Zugangsanbieter gar nicht aussuchen können, weil in ihrer Region keine Mitbewerber vorhanden sind.

Sehen Sie Gefahren im Hinblick auf den Schutz privater Daten und im Hinblick auf die Einschränkung der Funktionsherrschaft des Endnutzers über seine private Infrastruktur?

Technisch gesehen ist der Router nicht der eigentliche Netzabschlußpunkt im Sinne eines Endgerätes, sondern fungiert als Verbindung zwischen dem öffentlichen Netz und dem privaten Netz dahinter. An dieser Stelle entscheidet der Teilnehmer, welche Daten sein privates Netz verlassen oder hineingelangen und welche Daten aus seinem privaten Netz im öffentlichen Netz sichtbar sind.

Als Torwächter zwischen den beiden Netzen ist der Router daher für die Hoheit des Teilnehmers über sein privates Netz ein essentieller Baustein.

Zwangsweise vorgeschriebene Endgeräte, die obendrein vom Netzwerkzugangsanbieter kontrolliert und gewartet werden, berauben den Nutzer dieser Hoheit. Letztlich kann der Nutzer eines privaten Netzes dann nicht mehr ausschließen, daß Dritte sich Zugang zum eigenen Netz verschaffen. Vor dem Hintergrund der Enthüllungen in der sog. NSA-Affäre ist das Vertrauen der Bürger ohnehin schon nachhaltig erschüttert. Es wäre fatal, wenn sich diese Unsicherheit bis in die eigenen vier Wände ausdehnen würde. Der fernkontrollierte Router ist geeignet, genau diesen Unsicherheiten und Ängsten weitere Nahrung zu geben.

Hinzu kommt, daß ein fernkontrollierter Router den Zugangsanbietern weitere Möglichkeiten gibt, auf das Nutzerverhalten Einfluß zu nehmen. Möglich wäre es beispielsweise, über die MAC-Adressen einzelne Geräte zu identifizieren und etwa eine Anmeldung der Geräte beim Anbieter vorzuschreiben. Hiermit würde sich der Zugangsanbieter letztlich auch die Hoheit über die Infrastruktur des Netzes hinter dem Router aneignen, was in der Regel zum Nachteil des Kunden wäre.

In seinem Urteil vom 28. Februar 2008 zur sog. Online-Durchsuchung hat das Bundesverfassungsgericht die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als Grundrecht formuliert.

Dieses Grundrecht leitete das höchste deutsche Gericht direkt aus dem Recht zur freien Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG) sowie der allgemeinen Menschenwürde (Art. 1 GG) ab. Das Urteil betont, daß Menschen insbesondere die heimischen Systeme, wie Personal Computer oder Smartphones, in zunehmendem Maße verwenden, um dort ihre privaten und intimen Gedanken abzulegen, gleichsam in einer Art erweitertem Gedächtnis. Diese Informationen können von Kontaktdaten über private Fotos und Tagebucheinträge bis zu Erwachsenenunterhaltung alles beinhalten, was Menschen in ihrem privaten Umfeld zu tun pflegen. Das Bundesverfassungsgericht hat anerkannt, daß die auf diesen privaten Geräten abgelegten Daten die Privat- und sogar die Intimsphäre betreffen, ähnlich wie auch ein klassisches Tagebuch zum Kernbereich der privaten Lebensgestaltung gezählt wird.

Zur Wahrung dieses Grundrechts bedarf es allerdings nicht nur rechtlicher Rahmenbedingungen, sondern vor allem auch der Gerätehoheit, die beim Benutzer der Systeme liegt. Wird der Router von Dritten kontrolliert, kann die Hoheit des Nutzers über sein privates Netzwerk nicht mehr gewährleistet werden.

Nehmen Boxen Verkehrs-/Dienstdifferenzierungen vor? Wenn ja, in welcher Form?

Diese Frage läßt sich aus unserer Sicht nicht eindeutig beantworten, da die Provider an dieser Stelle keinen Einblick in die Funktionsweise ihrer Geräte geben. Tests zeigen jedoch, daß es naheliegt, daß die meisten Provider eine Priorisierung des eigenen VoIP-Traffics vornehmen. Dies mag aus technischer Sicht auch sinnvoll sein, damit störungsfreie Telefonverbindungen gewährleistet sind. Jedoch besteht bei den meisten Boxen keine Möglichkeit, den VoIP-Verkehr anderer Anbieter ebenfalls zu priorisieren. Es kann ebenfalls nicht ausgeschlossen werden, daß auch andere Dienste, wie etwa Peer-To-Peer-Netzwerke, nachrangig behandelt werden.

Wirken sich Einstellungen der Boxen, die Managed Services betreffen, auf den Internetzugangsdienst aus? Wenn ja, in welcher Form kann sichergestellt werden, daß hier keine Beeinflussung vorkommt?

Die Zugangsanbieter haben ein Interesse daran, daß ihre eigenen Dienste in guter Qualität erreichbar sind, daher werden Managed Services priorisiert werden. In dem Maße, in dem die Zugangsanbietern auch zu Inhalte-Anbietern werden, sinkt gleichzeitig deren Interesse, die Dienste von Mitbewerbern in hoher Qualität durchzuleiten. Als Beispiel seinen hier IPTV-Dienste genannt, die inzwischen von vielen großen Providern angeboten werden. Diese Dienste

werden in der Regel priorisiert, während der Benutzer keine Möglichkeit hat, den Dienst eines Mitbewerbers in gleicher Qualität in Anspruch zu nehmen, da die Konfigurationsmöglichkeit hierzu am Endgerät fehlt.

Der Einsatz eigener Endgeräte erlaubt dem Anschlußinhaber eine deutlich größere Flexibiltät, da er die geeignete Hardware wählen kann, welche das von ihm bevorzugte Produkt am besten unterstützt.

Schränken Boxen die Möglichkeiten von dahinter geschalteten Endgeräten (z. B. Router) ein, den Internetzugangsdienst vollumfänglich nutzen zu können? Wenn ja, in welcher Form, mit welchen Informationen kann sichergestellt werden, daß hier keine Beeinflussung vorkommt und auch an einem hinter ein Box geschaltetes Endgerät (z. B. ein Router) ein uneingeschränkter Internetzugangsdienst genutzt werden kann?

Ja, viele Boxen schränken die Möglichkeiten bereits deutlich ein. So sind beispielsweise Portfreigaben- oder Weiterleitungen nicht möglich. Viele Geräte unterstützen Tunnelprotokolle nicht, so daß die Verwendung von VPN-Diensten eingeschränkt ist. Gerade sehr einfache Boxen implementieren Funktionen des IPv6-Stacks nicht vollständig (fehlende DHCP6-Prefix-Delegation, Firewalling etc.) Auch die zwangsweise Priorisierung bzw. Drosselung von Protokollen schränkt die Nutzungmöglichkeiten ein.

Letzlich kann jede vorkonfigurierte Box nur einen Teil der im Internet verfügbaren Funktionen abbilden, daher ist ein diskriminierungsfreier, uneingeschränkter Internetzugang am besten dadurch zu realisieren, daß der Netzabschlußpunkt an der TAE-Dose liegt und der Teilnehmer die für seinen Anwendungszweck geeignete Hardware selbst installiert.

Behindern vorkonfigurierte Boxen, daß Diensteanbieter (sowohl Telekommunikationsdienste als auch OTT-Dienste, wie z. B. DynDNS-Dienste) ihre Dienste diskriminierungsfrei anbieten können?

Ja. Vorkonfigurierte Boxen bieten meist – falls überhaupt – nur einen DynDNS-Dienstanbieter an. Kleinere Anbieter werden von den Boxen in der Regel nicht unterstützt. Das Gleiche gilt für VPN-, Cloud-, OTT- und zahlreiche andere Dienste.

Da es sich bei vorkonfigurierten Boxen zumeist um sog. Black-Boxes handelt, hat der Nutzer der Geräte keine Handhabe herauszufinden, welche Dienste bevorzugt werden und welche benachteiligt sind. Ein Ändern dieser Prioritäten ist wiederum nicht möglich.

Welche technischen Eigenschaften und Qualitätsparameter muß eine Box erfüllen, damit andere Diensteanbieter (sowohl Telekommunikationsdienste als auch OTT-Dienste, wie z. B. DynDNS-Dienste) ihre Dienste auf jedem angeschlossenen Endgerät anbieten können?

Eine Box kann nur dann uneingeschränkten und diskriminierungsfreien Zugang bieten, wenn der Teilnehmer die volle Hoheit über die Box hat. Dazu ist ein voller Zugriff auf die installierte Software erforderlich, um alle Konfigurationen vornehmen zu können. Die Software der Box sollte frei und quelloffen sein, damit der Nutzer die Software seinen Bedürfnissen entsprechend anpassen oder ggf. sogar eine andere Software wählen kann.

Die Box muß anpaßbar sein, so daß beispielsweise das Einspielen von Sicherheits-Updates und neuen Funktionen leicht vorgenommen werden kann.

Außerdem muß der Benutzer die Parameter des durchgeleiteten Verkehrs einsehen können, etwa um zu überprüfen, ob bestimmte Dienste priorisiert oder diskriminiert werden.

Da alle Kunden unterschiedliche Bedürfnisse haben, ist es zu bevorzugen, dem Benutzer den Zugang direkt an der TAE-Dose zu gewähren. Für Kunden, die eine Betreuung wünschen, kann jeder Zugangsanbieter entsprechend vorkonfigurierte Boxen anbieten. Dieses Modell würde zusätzlich den Wettbewerb stärken, da der Kunde nicht gezwungen ist, diese Dienstleistung bei dem Zugangsanbieter selbst einzukaufen, sondern diese von einem Dritten erwerben könnte.