
STELLUNGNAHME

BUNDESNETZAGENTUR - SCHNITTSTELLEN AN NETZABSCHLUSSPUNKTEN (398/2013)



Free Software Foundation Europe e.V.
Schönhauser Allee 6/7
10119 Berlin
Deutschland

T: +49-30-27595290

Zur technologieneutralen Umsetzbarkeit der entwickelten Modelle

Frage 1. Ist es aus Ihrer Sicht möglich, die Modelle A und B nicht nur über xDSL- Technologien, sondern auch über die folgenden Übertragungstechnologien zu realisieren

a) Breitbandkabel (z.B. HFC)

b) Glasfaser (z.B. FttB/H) oder

c) stationär genutzte Funklösungen (auch unter Berücksichtigung des ETSI Guide 201 730-1?

*Bitte machen Sie jeweils nähere Ausführungen zu signifikanten Unterschieden, die ggf. einer Übertragung entgegenstehen, sowie Besonderheiten in den verschiedenen OSI-Schichten.

Keine Antwort.

Frage 2. 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 bewerten diese Verhaltensweise als lobens- und wünschenswert. Die xDSL-Schnittstellen sind als Standards definiert und es findet sich somit eine Vielzahl an Geräten von zahlreichen Anbietern, die an die TAE-Dose angeschlossen werden können. Der DSL-Kunde hat somit Zugriff auf die niederen technologischen Abstraktionsebenen und folglich die Wahl zwischen einfachen Modems und funktionsreichen Kombigeräten (etwa Router mit VoIP-Funktionen). Sollten sich die Anforderungen an die eigene Infrastruktur ändern, steht es dem Endanwender jederzeit offen, andere Hardware einzusetzen und diese seinen Bedürfnissen entsprechend zu konfigurieren. Die TAE-Dose als Netzzugangsschnittstelle ist daher als endbenutzerfreundlich zu beurteilen.

Frage 3. 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? Bitte differenzieren Sie dabei zwischen unterschiedlichen Zugangstechnologien (insbesondere xDSL, HFC, FttB/H sowie stationär genutzte Funklösungen).

Jedes Leitungsabschlussgerät muss die Anbindung weiterer Geräte (etwa PCs, Notebooks, Telefone etc.) des Anwenders über gängige (d.h. weit verbreitete und akzeptierte) und offen definierte Schnittstellen gewährleisten und darf nicht nur kompatibel zu eigenen oder favorisierten Geräten, Protokollen oder Formaten sein. Bisher kommen dabei Ethernet für kabelgebundene Verbindungen und W-LAN nach IEEE802.11 zum Einsatz. Jedoch müssen nicht nur die bisherigen Standards integriert sein, sondern die Leitungsabschlussgeräte müssen auf sämtlichen verwendeten Layern möglichst für die

jeweils aktuellen Spezifikationen geeignet sein, die sich weltweit als Standards durchgesetzt haben (beispielsweise ISO, IETF, IEEE, 3GPP etc.). Nur solche Standards sind durch vielfachen Einsatz und Gegenprüfungen gehärtet und bewährt und daher proprietären, also nicht-offenen Standards, vorzuziehen. Eine fehler- und störungsfreie Interaktion mit anderen Netzelementen ist also nur durch langfristige Nutzung von offenen Spezifikationen möglich, da nur diese es gestatten, herstellerübergreifend Geräte einzusetzen.

Die Hersteller von Leitungsabschlussgeräten sollten daher ihre verwendeten Protokolle und Spezifikationen offen legen, damit auch in Zukunft alle Geräte und Nutzer von technologischen Weiterentwicklungen profitieren können.

Frage 4. Welche technischen Vor- und Nachteile sehen Sie insgesamt bei Anwendung a)des Modells A?

Vorteile des Modells A:

- Es bietet dem Endanwender die umfassendste Wahlfreiheit, da er hierbei in der Lage ist, ein Gerät zu wählen, welches exakt seinen Anforderungen entspricht
- Es wird ein offener Wettbewerb unter den Herstellern gefördert
- Dieser Wettbewerb ermöglicht dadurch stetige technologische Weiterentwicklungen und Verbesserungen. Die Wettbewerbsfähigkeit steigt durch kurze Reaktionszeiten auf Markt- und Technologieanforderungen
- Offene Protokolle und Spezifikationen sowie die Wahlfreiheit des Kunden fördern die Kompatibilität mit anderen Geräten und den einfachen Wechsel zu anderen Providern, was wiederum dem Wettbewerb zugute kommt
- Kombination von Geräten und Angeboten verschiedener Hersteller und Serviceprovider wird ermöglicht und verbessert
- Der Kunde kann durch die freie Auswahl an Produkten und Dienstleistungen Kosten sparen, auch durch Wiederverwendung von älteren Geräten und Stromersparnisse

Nachteile:

- Höherer Hotline-Aufwand auf Providerseite durch bessere Schulung

b)des Modells B1?

Vorteile:

- Wahlfreiheit des Endanwenders für die Geräte nach dem Modemgerät
- Wettbewerb für diese Geräte ist möglich
- Technische Weiterentwicklungen für frei auswählbare Geräte können herstellerunabhängig implementiert werden
- Die Kombination von Geräten nach dem Modem ist möglich, solange die Bedingungen aus Antwort 3 gegeben sind

Nachteile:

- Der Wettbewerb für Modem- und Kombigeräte wird eingeschränkt
- Die Verwendungen von Boxen und Geräten nach dem Modemgerät könnte eingeschränkt sein, wenn sich Hersteller nicht an gängige Standards halten oder aktuelle Technologien nicht in ihren Geräten implementieren
- Der Hotline-Aufwand im Vergleich zu Modell A wird nicht spürbar weniger, sondern könnte sich durch die Verwendung minimalistischer, billiger Modemgeräte vor der Hardware des Anwenders sogar erhöhen
- Der Endanwender hat nicht die Möglichkeit, das Modemgerät auszutauschen, sollte es nicht mit der eigenen Hardware funktionieren

c)des Modells B2?

d)des Modells B3?

Vorteile:

- „Alles aus einer Hand“, wenn alle benötigten Dienste vom Provider angeboten und unterstützt werden

Nachteile:

- Eingeschränkte Wahlfreiheit des Endkunden
- Künstliche Abschaffung des gesunden Wettbewerbs
- Behinderung technologischer Weiterentwicklungen durch fehlenden Wettbewerb und Aufbau von geschlossenen Systemen
- Entstehung von Sicherheitsproblemen durch Monokulturen, fehlende langfristige Pflege von Produkten und die fehlende Möglichkeit, selbst Patches oder sicherere Firmware aufzuspielen
- Kompatibilitätsprobleme mit Geräten, Protokollen und Diensten, welche der Provider nicht unterstützt (Telefone, Onlinespiele, Tunnel- und Netzwerkprotokolle, Firewalls etc.)
- Unnötige Umweltbelastung durch unbenutzte Funktionen in der gelieferten Box und Nichtverwendbarkeit von bereits bestehenden Geräten

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

Die eingesetzten Übertragungstechnologien sind in der Bewertung der Modelle A und B1 bis B3 nicht ausschlaggebend, sondern ausschließlich die örtliche Definition der Netzzugangsschnittstelle. Dadurch entscheidet sich, was dem Benutzer technisch ermöglicht bzw. erschwert wird und ob er ökonomisch bedacht aus einer freien Auswahl von Geräten am Markt auswählen kann.

Bei xDSL-Technologien besteht für den Endanwender eine große Auswahl an Kombigeräten diverser Marken, welche den Kunden unabhängig von der Zugangstechnologie verschiedene Funktionskombinationen anbieten.

Zu den wettbewerblichen und weiteren Implikationen

Frage 5. Welche wettbewerblichen (wirtschaftlichen) und eventuelle weitere Vor- und Nachteile sehen Sie mit Blick auf die vorgestellten Modelle?

a)des Modells A?

b)des Modells B1?

c)des Modells B2?

d)des Modells B3?

Bei Anwendung der Modelle A und bedingt B1 wird Herstellern unterschiedlicher Geräte ein gesunder Wettbewerb ermöglicht, da transparente Standards verwendet werden und alle Kunden die Freiheit besitzen, von ihnen favorisierte Apparate einzusetzen. Geräte mit oder ohne Modemfunktionen (Modell A) und Router ohne integriertes Modem (Modell A und B1) werden dabei mehr Nachfrage erhalten. Die durch Anwendung der Modelle A und B1 entstehenden positiven wirtschaftlichen Auswirkungen sind auch für die zahlreichen Hersteller mit Sitz in Deutschland nicht von der Hand zu weisen.

Ein weiterer Vorteil der Modelle A und B1 ist der Abbau der sich derzeit etablierenden Monokultur an Geräten. Solche Monokulturen erhöhen signifikant die Wahrscheinlichkeit, dass durch fehlerhafte oder unsichere Geräte Botnetze aufgebaut werden oder im großen Stil relevante Daten von Individuen und Firmen abgehört oder zweckentfremdet werden. Diese Gefahren sind nicht theoretischer Natur, sondern können immer wieder in der Realität beobachtet werden. Sollten diese Monokulturen bestimmter Hersteller durch die Anwendung der Modelle B2 oder B3 weiter gefördert werden, verursachen die Angriffe auf die Infrastruktur von Privatleuten, Unternehmen und Providern in Deutschland und weltweit noch mehr wirtschaftlichen Schaden als dies schon heute durch Sicherheitslücken der Fall ist.

In der Vergangenheit hat sich gezeigt, dass vom Provider vorgeschriebene Geräte schwächer ausgestattet sind, langsamer weiterentwickelt werden, mehr Sicherheitslücken aufweisen und seltener Sicherheitsupdates erhalten. Da liegt darin begründet, dass diese Geräte im Rahmen von Projektgeschäften gekauft werden, die keinen langfristigen

Support vorsehen. Einen offenen Wettbewerb gibt es dabei nicht, der Provider zieht in der Regel das billigste Gerät vor, ohne auf technische Spezifikationen, Sicherheitsausstattung, langfristige Pflege oder Kombinationsmöglichkeiten zu achten.

Auch in wettbewerbsrechtlicher Hinsicht sind alle restriktiveren Alternativen als Modell A als kritisch einzustufen. Neue Markteinsteiger werden in diesem wirtschaftlich relevanten Markt vertrieben oder können sich erst gar nicht etablieren. Dadurch ergeben sich erhebliche Folgefragen in rechtlicher Hinsicht, da die Gefahr mittelbar-faktischer Diskriminierung nicht von der Hand gewiesen werden kann.

Kurzfristige Nachteile vorgeschriebener und nicht austauschbarer Geräte:
Kundenbehinderung.

Mittelfristige Nachteile:

Die technologischen Weiterentwicklungen werden erheblich gebremst und die Sicherheit vor Angriffen aus dem Internet wird durch finanzielle Interessen der Provider gemindert.

Langfristige Nachteile:

Es können sich geschlossene Systeme entwickeln, in die nicht einmal der Provider komplette Einsicht hat, sondern nur der Hersteller des Betreibergeräts. Die Preise für Geräte werden daher nicht sinken, sondern steigen, da durch verhinderten Wettbewerb keine konkurrierenden Hersteller mehr vorhanden sind und deren Geräte nicht mehr mit dem geschlossenen System kompatibel sind.

Zur Endnutzerfreundlichkeit und Akzeptanz der entwickelten Modelle

Frage 6. 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

Die Möglichkeiten für Endkunden, beliebige Endgeräte zu nutzen, hängt stark von der Firmenpolitik der Provider ab und nicht von den technischen Gegebenheiten.

DSL-Modems, - Router und vergleichbare Endgeräte gibt es im freien Handel zu kaufen. Da diese Schnittstellen offen gelegt werden müssen, können alternative Hersteller Geräte anbieten, welche den jeweiligen Bedürfnissen der Kunden entsprechen. Diese lassen sich jedoch nur dann nutzen, wenn der Provider volle Transparenz über Zugangsdaten und technische Spezifikationen gewährt. Ist dies nicht der Fall, ist ein direkter Einfluss auf alle weiteren Geräte hinter dem Modem oder Router die Folge. Durch den Zwang, bestimmte vom Provider akzeptierten Geräte zu nutzen, können andere Dienste beeinträchtigt oder

nicht nutzbar sein und der Endkunde hat keine Möglichkeit, diesen Sachverhalt zu ändern oder gar technisch nachzuvollziehen.

Diese Problematik wurde auch von Stiftung Warentest herausgehoben:

„Mit Ausnahme von 1&1, Congstar, Telekom und Vodafone zwingen die Anbieter ihren Kunden einen ihrer Router auf. Dem mangelt es oft an Funktionen wie der Kontrolle des Datenverbrauchs oder an WLAN-Reichweite. Einen besseren Router schließen Kunden auf eigenes Risiko an. [...] Im Störfall zielt sich der Support dann gern mit dem Hinweis: „Sie setzen nicht unsere Technik ein.““ (Ausgabe 9/2013, S. 54)

Beispiel:

Bei Kabelmodems kann nur das vom Provider gelieferte Modem genutzt werden, da dieses am Headend registriert werden muss. Ist das Modem defekt, kann es nicht einfach durch ein anderes Modem ersetzt werden, selbst wenn es vom gleichen Hersteller oder Provider stammt. Kabelmodems sind daher kaum zu kaufen, da es nicht möglich ist, diese dann auch zu nutzen. Das kann nicht im Sinne des Wettbewerbs sein und lässt sich auch nicht plausibel mit technischen, sondern ausschließlich mit politischen oder wirtschaftlichen Interessen der Provider begründen.

Erschwerend kommt hinzu, dass sich der Endkunde schon oft bei Bestellung des Anschlusses für ein Gerät entscheiden muss und dieses anschließend nicht mehr tauschen kann, auch wenn sich seine Anforderungen vielleicht in Zukunft ändern werden. Es ist für ihn also unmöglich, aus dieser künstlich geschaffenen Provider- und Herstellerabhängigkeit auszubrechen, solange er gezwungen wird, bestimmte Geräte zu nutzen und keine vollkommene Wahlfreiheit hat, wie es in Modell A und teilweise Modell B1 der Fall ist.

Beispiel:

Negative Auswirkungen einer Provider- und Herstellerabhängigkeit sind abermals nicht nur theoretischer Natur, sondern lassen sich schon heute in produktiven Umgebungen nachvollziehen.

Ein eigener Router lässt sich zwar bei Einsatz des Protokolls IPv4 mit Hilfe eines zweiten NAT hinter dem vom Provider vorgeschriebenen Geräts betreiben, dies gilt jedoch nicht für die sich immer stärker etablierende Version 6 des IP-Protokolls, welches schon auf mittelfristige Sicht Version 4 ablösen wird. Bei IPv6 ist vorgesehen, dass jedes Gerät über eine eigene, einzigartige IPv6-Adresse verfügt. Will der Endkunde hinter dem Providergerät einen eigenen Router betreiben, sind Folgetechnologien nötig, um dem Kundenrouter das vom Provider delegierte IPv6-Subnetz durchzureichen.

Daher muss das Gerät des Providers zumindest die IPv6 Prefix Delegation beherrschen, da andernfalls kein IPv6 in brauchbarer Weise an nachgeschalteten Routern und Endgeräten des Kunden genutzt werden können. Unseren Tests zufolge bieten beispielsweise die von Kabel

Deutschland gelieferten Hiltron- und Compal-Geräte diese Funktionalität nicht.

Auch in einem anderen Zusammenhang ist eine Provider- und Herstellerabhängigkeit im Hinblick auf IPv6 problematisch. Einige Endgeräte lassen sich besser mit DHCPv6, andere besser mit SLAAC betreiben - oder mit einer Kombination von beiden Vergabeprotokollen. Bei von Providern vorgegeben Geräten sind dabei häufig keine Einstellungsmöglichkeiten vorhanden und viele Routermodelle unterstützen ausschließlich SLAAC. Somit lassen sich nicht alle Endgeräte problemlos betreiben, denn bietet der Provider kein geeignetes Gerät an oder verhindert den Anschluss eines solchen, ist es nicht möglich, alle Endgeräte am Internetanschluss zu nutzen. Auch das lässt sich technisch nicht begründen: Würden Provider ihren Endkunden völlige Transparenz gewähren und den Anschluss eigener Geräte ermöglichen, könnten diese alternative Apparate betreiben. In weiteren Tests haben wir herausgefunden, dass es insbesondere bei der neuen IPv6-Technologie viele Probleme und Fehler in Routern verschiedener Hersteller geben kann, sodass der Einsatz jedes Routers in Paarung mit verschiedensten Endgeräten nicht immer reibungslos funktioniert und nur durch den Austausch des Routers die Funktionalität wieder hergestellt werden kann.

Anhand dieser Beispiele zeigt sich, dass zukunftsweisende Technologien durch vom Provider vorgeschriebene und nicht austauschbare Geräte aktiv aufgehalten werden und die Kompatibilität geschmälert wird. Selbst wenn die oben genannten Fehler behoben werden sollten, ist es nur eine Frage der Zeit und der Menge an Tests, bis die nächsten unnötigen Restriktionen auftreten, solange der Nutzer nicht die freie Wahl hat, welche Geräte er verwenden kann. Jeder künstliche Eingriff, etwa die Geheimhaltung von Einwahldaten aller Art und dass Kunden keine eigenen Geräte an die TAE- oder Kabeldose anschließen können, erzeugt technische Einschränkungen und Folgeprobleme.

Frage 7. Wie wird sichergestellt, dass Endkunden bei allen beschriebenen Modellen gleichermaßen über die Kompatibilität zwischen der Netzzugangsschnittstelle und Endgeräten (einschließlich WLAN-Router) im Sinne des § 43a TKG klar und umfassend informiert sind?

Keine Antwort.

Frage 8. 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 viele Provider momentan auf die Umsetzung der Modelle B1 bis B3 drängen, ist der Einsatz solcher durchaus vorstellbar. Bekommt der Endkunde vom Hersteller ein fixes Gerät für alle Aufgaben, ist dies möglicherweise kurzfristig im Sinne der Anwender, da es eine einfachere Installation ermöglicht. Auch die Möglichkeit, für alle Dienste, etwa

Internet, Telefon und unter Umständen auch Fernsehen, nur eine Rechnung zu erhalten, kommt vielen Endkunden gelegen. Die Akzeptanz der Kunden dürfte also im momentanen Stand durchaus hoch sein.

Auf mittel- und langfristige Sicht jedoch entstehen dem Anwender durch verminderten Wettbewerb und den Aufbau geschlossener Systeme mehr Nachteile als Vorteile. Die Abhängigkeit von Providern, Herstellern und deren erlaubten Geräte wird auch in anderen Sparten den technischen Fortschritt einschränken und enorme Folgeprobleme verursachen. Es sollte daher nicht das durchgesetzt werden, was technisch machbar ist, sondern das, was den Wettbewerb fördert und dadurch langfristig Weiterentwicklung, Unabhängigkeit und Produktauswahl ermöglicht.

Frage 9. Sehen Sie Gefahren im Hinblick auf den Schutz privater Daten und im Hinblick auf die Einschränkung der Funktionsherrschaft des Endnutzers über seine private Infrastruktur?

Sobald der Nutzer keine volle Verfügungsgewalt auf alle technischen Geräte hinter der TAE-Dose oder dem Kabelanschluss besitzt, besteht eine ernstzunehmende Gefahr für den Schutz seiner persönlichen Daten...

- da er somit nicht selbst für die Sicherheit seines Netzwerkes garantieren kann. Das ist vor allem angesichts der Störerhaftung im Sachen- und Verwaltungsrecht höchst problematisch, da dann der Endnutzer für durch Sicherheitslücken verursachten Schaden aufkommen muss, er aber nie die Möglichkeit hatte, ein anderes, sichereres Gerät zu verwenden
- da er damit zusammenhängend auch selbst keine Sicherheitslecks schließen kann, etwa durch das Aufspielen eines Updates oder einer anderen Firmware. Er legt somit die gesamte Integrität seines Netzwerks in das Wohlwollen eines Providers und hat keine Möglichkeit, angemessen selbst für seine Sicherheit zu sorgen. Dies ist insofern besonders heikel, da die Box hinter der TAE-Dose oder des Kabelanschlusses die wichtigste Instanz zwischen der eigenen Infrastruktur und der Außenwelt ist. Jeglicher Datenverkehr verläuft über dieses Gerät, daher ist es auch als selbstverständlich zu erachten, dass der Nutzer volle Verfügungsgewalt über dieses und nachfolgende Geräte hat. Jedes unsichere Gerät hebelt die nachfolgende interne Sicherheitsarchitektur aus.
- da er selbst für triviale technische Probleme wie etwa die Einstellung des WLANs, die Begutachtung von Fehlerlogdateien und die Konfiguration von DNS-Servern vom Provider abhängig ist, da ihm grundlegende Mündigkeiten genommen werden. Besteht ein Problem in seinem Netzwerk, kann er es nur lösen, wenn der Provider Support leistet - er kann somit weder voll auf alle Geräte nach der TAE-Dose/des Kabelanschlusses zugreifen, noch inkompatible Geräte austauschen.
- da er nicht zum Hersteller seines Vertrauens greifen kann, wenn er beispielsweise dem Hersteller des Provider-Gerätes nicht vertraut oder angesichts ungelöster Probleme, Inkompatibilitäten oder Sicherheitslücken das Provider-Gerät nicht in

Frage kommt. Möchte oder muss der Endkunde etwa von zu Hause an sensiblen Daten arbeiten, ist es verständlich, dass er volle Transparenz und Verfügungsgewalt über seine IT-Infrastruktur inne hat.

- da der Endnutzer somit annehmen muss, dass der Provider nicht in seinem Sinne handelt, muss er auch damit rechnen, dass dieser seine Infrastruktur nur unzureichend vor dem Zugriff Dritter schützt. Wenn sich etwa der Provider das Recht einräumt, dem Kunden das Gerät vorzuschreiben und auf dieses auch noch jederzeit aus der Ferne zugreifen kann, kann davon ausgegangen werden, dass dies auch Dritten möglich ist - kein System ist absolut sicher.

Neben den Einschränkungen beim Schutz persönlicher Daten gibt es auch technische Einschränkungen, die sich unmittelbar durch einen Routerzwang ergeben und zumeist technisch nicht begründbar sind:

- Bei vielen Modellen ist die Freigabe von Ports nicht möglich oder eingeschränkt möglich. Diese Ports muss schon im ersten Gerät nach der TAE-Dose oder des Kabelanschlusses frei geschaltet sein. Einige Beispiele:
 - Onlinespiele erfordern häufig die Freischaltung eines Ports im Router, damit die Kommunikation mit anderen Spielern oder den Spieleservern erfolgen kann.
 - VoIP-Telefone und SIP-Dienste benötigen oftmals freigeschaltene Ports
 - Der Zugriff vom oder zum Heimnetzwerk über verschiedene Daten- oder Tunnelprotokolle (beispielsweise FTP, SSH, PPTP etc.) erfordert in den meisten Fällen freigegebene Ports. Die Verwendung solcher Praktiken ist auch im privaten Bereich gang und gäbe, Nutzer dürfen daher auch nicht gezwungen sein, sich deswegen einen Businesszugang zu bestellen. Für den Provider entstehen dadurch keine besonderen Zusatzlasten und die technische Umsetzung ist vielfach implementiert.
- Sichere Tunnelprotokolle wie OpenVPN, SSH oder IPsec/L2TP sind oftmals eine Grundvoraussetzung, wenn ein Endnutzer von zu Hause aus für eine Firma arbeiten muss. Diese Technologien müssen zwingend unterstützt sein und da meist sensible Daten über diese Leitungen laufen, hat der Kunde ein berechtigtes Interesse daran, selbst aktiv für die Sicherheit seiner Infrastruktur tätig zu werden und sich nicht auf intransparente Provider verlassen zu müssen.
- Der Endkunde könnte bei der Einschränkung der vollen Funktionsherrschaft gezwungen sein, nur bestimmte Telefone mit bestimmten Techniken oder von bestimmten Herstellern zu verwenden, welche eventuell nicht mit seinen sonstigen Endgeräten kombinierbar sind oder seinen Vorstellungen zur Strahlungsarmut nicht entsprechen. Resultat dieser Praktik wären unnötige Ausgaben und Umweltbelastungen. Ein Beispiel dafür ist die Einschränkung beim Kabelprovider Unitymedia mit dem Motorola/Cisco-Modem, welcher nur Analogtelefone unterstützt.
- Nicht nur Telefone können Inkompatibilitäten mit vom Provider vorgeschriebenen

- Boxen aufweisen, sondern jegliche anderen Endgeräte: WLAN-Empfänger, Hausautomationen (Heizungen, Kühlschränke, Einbruchsicherungen etc.), Fernsehgeräte, Netzwerkspeicher und so weiter
- Abgesehen von den enormen rechtlichen und technischen negativen Auswirkungen der Provider- und Herstellerabhängigkeit ist auch die unvermeidliche Wettbewerbsverzerrung zu beachten. Werden alternative Hersteller von den Providern nicht unterstützt oder geduldet, geht ihnen der gesamte Markt verloren.

Zur Netzneutralität

Frage 10. Nehmen Boxen Verkehrs/Dienst differenzierungen vor? Wenn ja, in welcher Form?

Wir können die Frage leider nicht mit voller Gewissheit beantworten, weil uns schon heute von Providern und Geräteherstellern die nötige Transparenz verwehrt wird, um die letzten Zweifel an unseren Vermutungen auszuräumen. Wir gehen jedoch stark davon aus, dass zumindest die Boxen der Telekom und sämtlicher Kabelprovider eigene VoIP-Services bevorzugen. Will man eine Alternative nutzen, wird dieser Traffic nur nach dem Best-Effort-Prinzip behandelt. Telefonate werden so also zu Lastzeiten stark beeinträchtigt. Die fehlenden Konfigurationsmöglichkeiten in allen Boxen verhindern etwa die manuelle Priorisierung eines solchen Datenverkehrs und schrecken Endkunden davor ab, andere Dienste als die vom Provider favorisierten zu nutzen. Möglicherweise besteht eine solche Priorisierung bereits bei Verbräuchen durch die Boxen direkt, auch bei anderen Diensten wie etwa Onlinespeichern, Videostreaming oder großen Datenübertragungen. Mangels Kontrolle über das Gerät lässt sich dieser Verdacht auch nicht beurteilen, da die Geräte insoweit intransparent konfiguriert werden. Angesichts der häufig zu beobachtenden Unregelmäßigkeiten mit VoIP-Diensten und Downloads ist jedoch davon auszugehen, dass eine Verkehrs- und Dienst differenzierung bereits Praxis ist, entweder beim Provider oder direkt bei der vom Provider gelieferten Box. Sollte dem Endkunden die volle Verfügungsgewalt über die Auswahl und Konfiguration der Geräte nach der TAE-Dose oder des Kabelanschlusses genommen werden, steht einer weiteren Verletzung des diskriminierungsfreien Internetverkehrs nichts mehr im Wege.

Frage 11. 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 in Frage 10 beschriebenen Differenzierungen sind nicht durch den Nutzer konfigurierbar. Möchte man etwa einen alternativen VoIP-Anbieter nutzen, kann es bei gleichzeitigen Up- oder Downloads zu einem spürbaren Qualitätsverlust des Dienstes kommen. Die Telekommunikationsanbieter versuchen selbstverständlich, ihren eigenen Diensten eine hohe Qualität einzuräumen, bieten dem Nutzer dies aber nicht bei alternativen Diensten an. Dass dies dem Endkunden bewusst vorenthalten wird, liegt auf der Hand.

Nur wenn der Anwender die volle Auswahl- und Funktionsherrschaft über alle Geräte

nach der TAE-Dose oder des Kabelanschlusses hat, kann eine Beeinflussung der Dienste auf Kundenseite ausgeschlossen werden. Für den Schutz von Markteinsteigern und die damit verbundene Wettbewerbsgleichheit und Marktoffenheit können ausschließlich politische Schritte helfen.

Frage 12. 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?

Viele Boxen schränken schon heute die Möglichkeiten von nachgeschalteten Endgeräten ein, unsere Antworten für Frage 9 beschreiben dabei schon einige exemplarische Problematiken.

- Portfreigaben können nicht möglich oder eingeschränkt sein, etwa wenn das erste Gerät dies nicht unterstützt.
- Tunnelprotokolle sind häufig nicht zugelassen oder unterstützt
- Die Priorisierung oder Drosselung bestimmter Datenpakete schränkt die vom Nutzer gewollten Möglichkeiten ein
- Fehlende Unterstützung von DHCP Prefix Delegation, was Probleme bei der Nutzung von IPv6 verursacht

Die meisten auf dem Markt erhältlichen Boxen, Modems und Router unterstützen diese Techniken, die Beschneidung ist rein firmenpolitischer Herkunft. Die Notwendigkeit von Portfreigaben zwingt etwa Endkunden dazu, einen Businesszugang zu erwerben, da es vom Anbieter nicht gewünscht wird oder dieser aus trivialen Techniken zusätzlichen Profit schlagen will.

Möchte der Kunde also einen uneingeschränkten Internetzugangsdienst nutzen, muss er in der Lage sein,

- jedes von ihm erwünschte Gerät ab der TAE-Dose oder des Kabelanschlusses zu nutzen und
- auf jedes dieser Geräte vollumfänglich zuzugreifen

Hat er auch nur eine dieser beiden Freiheiten nicht, ist er gezwungen, die Geräte des Providers zu nutzen oder hat keine Funktionsherrschaft über sein eigenes Heimnetzwerk. Damit er jedes von ihm gewünschte Gerät verwenden kann, benötigt er also zwingend alle seine Zugangsdaten des Providers, etwa für die Verbindung mit dem Internet oder dem VoIP-Dienst.

Frage 13. Behindern vorkonfigurierte Boxen, dass Diensteanbieter (sowohl Telekommunikationsdienste als auch OTT-Dienste, wie z.B. DynDNS-Dienste) ihre Dienste diskriminierungsfrei anbieten können?

Ja, vorkonfigurierte Boxen widersprechen der Diskriminierungsfreiheit von Diensteanbietern. So werden in vielen Fällen etwa kleinere DynDNS-Anbieter nicht von den Provider-Boxen unterstützt, sondern gar keine, nur einer oder wenige bekannte. Auch alternative VoIP-Dienste können durch fehlende Konfigurationsmöglichkeiten diskriminiert werden, da der Provider nur seine eigenen Dienste unterstützt oder priorisiert. Dies ist unter anderem problematisch, wenn der Endkunde von zu Hause arbeitet und den VoIP-Anbieter seiner Firma einbinden muss. Das Gleiche ist der Fall mit VPN-, Onlinespeicher-, SaaS- oder Streaming-Diensten.

Des Weiteren kann der Nutzer im Vorfeld nicht kontrollieren, ob bestimmte OTT-Dienste möglicherweise benachteiligt werden. Dies geht einher mit Allgemeinen Geschäftsbedingungen von Providern, welche etwa Volumenlimits einführen, aber nur providereigene Dienste davon ausnehmen. Von Diskriminierungsfreiheit kann dabei nicht mehr die Rede sein.

Frage 14. 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 erst dann diskriminierungsfrei, sicher und kompatibel mit anderen Diensteanbietern sein, wenn sie dem Anwender vollen Zugriff auf die Software bietet, um sie den Bedürfnissen anzupassen und für aktuelle und zukünftige Technologien individuell erweiterbar ist. Sie muss dem Endkunden gewähren, selbst Sicherheitsupdates oder Zusatzdienste, etwa über Plugins, einzuspielen oder eine alternative Software auf dem Gerät zu installieren, welche Probleme ausmerzt oder gewünschte Funktionen ermöglicht. Des Weiteren muss sie dem Endkunden die Möglichkeit geben, Verbindungsdaten einzusehen, anhand derer eingesehen werden kann, welche Anschlussgeschwindigkeit der Provider liefert und ob diese dem Vertrag entspricht.

Um all diese Voraussetzungen für die optimale Kompatibilität garantieren zu können, muss eine Box dem Anwender vier Freiheiten einräumen: Die Freiheit, die Boxsoftware für jeden Zweck zu verwenden, die Freiheit, die Funktionsweise zu analysieren und anhand des Quelltextes zu verändern, sowie die Freiheiten, die Software des Gerätes anderen zur Verfügung zu stellen und auch eigene Verbesserungen öffentlich zu machen. Nur mit dieser Transparenz haben Anwender die Möglichkeit, ihre bestehende Infrastruktur zu nutzen oder ohne künstliche Beschränkungen mit Produkten aus einem freien Markt zu erweitern.

Um jedoch sicherzustellen, dass der Kunde alle Diensteanbieter diskriminierungsfrei nutzen kann, muss er auch in der Lage sein, jedes Gerät nach der TAE-Dose oder dem Kabelanschluss auszutauschen. Nur dann hat er die Hoheit über seine IT-Infrastruktur und kann größtmögliche Kompatibilität mit allen Endgeräten gewährleisten. Um dies zu realisieren, darf der Provider keine Verbindungs- und Anmeldedaten vorenthalten und dem Kunden kein Gerät aufzwingen, ohne welches er seinen Internetzugang nicht vollumfänglich nutzen kann.

Um vollständige Diskriminierungsfreiheit anderer Diensteanbieter und Hersteller gewährleisten zu können, muss jedoch nicht nur die Anwenderseite gestärkt werden, sondern politisch für die allgemeine Gleichbehandlung aller Datenpakete gearbeitet werden. Andernfalls werden Provider immer die Möglichkeit haben, eigene Dienste zu favorisieren, dem Wettbewerb zu schaden, den Kunden zu entmündigen und damit zu gefährden.