Stellungnahme

zum Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG) (Stand: Referentenentwurf vom 11.03.2015)

Unitymedia mit Hauptsitz in Köln ist der führende Kabelnetzbetreiber in Deutschland und eine Tochter von Liberty Global, dem größten internationalen Kabelunternehmen mit Niederlassungen in 14 Ländern. Unitymedia erreicht mit seinem Glasfaser-Koax-Netz 12,6 Millionen Haushalte mit Breitbandkabeldiensten. Neben klassischen Kabel-TV-Dienstleistungen bietet Unitymedia seinen Kunden auch die Versorgung mit Telefonie sowie Highspeed- Internet mit Bandbreiten bis 200 MBit/s und ist so zum wichtigen Infrastrukturwettbewerber im Telekommunikations- und Breitbandmarkt geworden. Ende 2014 hatte Unitymedia 7,1 Mio. Kunden, die 6,6 Mio. TV-Abonnements und 2,9 Mio. Internet- sowie 2,7 Mio. Telefonie-Abonnements bezogen haben. Weitere Informationen zu Unitymedia finden Sie unter www.unitymedia.de/unternehmen.

Am 11.03.2015 hat das BMWi einen Referentenentwurf zur Änderung des Telemediengesetzes veröffentlicht. Dieser hat das Ziel, die im Koalitionsvertrag vereinbarte Förderung öffentlicher WLAN-Netze voranzutreiben und für die Anbieter solcher öffentlicher WLAN-Zugänge Rechtssicherheit zu schaffen. Darüber hinaus sollen neue Regeln für Host-Provider zum Schutz von Urhebern und Inhalte-Anbietern eingeführt werden. In unserer Stellungnahme werden wir uns jedoch auf den ersten Punkt konzentrieren.

Wir begrüßen das Ziel, mit dem Gesetzesentwurf einen Ausgleich zwischen den Interessen der Rechteinhaber und Sicherheitsinteressen auf der einen Seite und der Verbreitung von öffentlich zugänglichem WLAN auf der anderen Seite zu schaffen. Die dabei zu treffende Abwägung ist deshalb besonders schwierig, da es sich auf beiden Seiten um legitime und berechtigte Interessen handelt. Gleichwohl wurde in dem nun vorgelegten Referentenentwurf eine tragbare Balance zwischen diesen widerstreitenden Interessenslagen gefunden, mit der auch wir als Anbieter öffentlich zugänglicher WLAN-Netze gut arrangieren können.

Auch hinsichtlich des Ziels der Nutzersicherheit geht der nun vorgelegte Referentenentwurf in die richtige Richtung. Wir begrüßen, dass durch die geforderte Verschlüsselung im Rahmen eines offenen WLAN-Angebots auch Sicherheitsbedenken und -interessen der Nutzer Rechnung getragen wird, auch wenn wir an dieser Stelle noch Anpassungsbedarf sehen. Im Ergebnis sollten Anwender die Wahl haben, neben einer unverschlüsselten Verbindung auch auf einen verschlüssel-

ten Zugang zum Internet zurückgreifen zu können. Solange dies gegeben ist und zumindest auch die Möglichkeit zur verschlüsselten Nutzung des WLAN-Angebots besteht, darf das zusätzliche alternative Angebot einer unverschlüsselten Verbindung nicht dazu führen, dass das durch das TMG gewährleistete Haftungsprivileg des geschäftsmäßigen WLAN-Anbieters eingeschränkt wird. So sieht auch unser Modell für öffentlich zugängliches WLAN – wie wir es auch gerade in der Stuttgarter Innenstadt gemeinsam mit Stuttgart Marketing aufbauen – vor, dass zunächst allen Nutzern ein (mit eingeschränkter Funktionalität) versehener unverschlüsselter Zugang zur Verfügung steht. Mittels einer SMS können sich unsere Nutzer aber auch auf einfachstem Weg registrieren und erhalten dann – ebenfalls per SMS – einen Zugangscode, mit dem sie sich über eine verschlüsselte Verbindung unbegrenzt mit dem Internet verbinden können.

Gleichwohl darf das Erfordernis der Verschlüsselung nicht dazu führen, dass Haftungsprivilegierungen systemfremd generell an Sicherheitsaspekte gekoppelt werden. Hinsichtlich des Begriffs der „Verschlüsselung“ sehen wir zudem Klarstellungsbedarf, da unklar bleibt, ob eine Verschlüsselung des Datenverkehrs (also der vom Nutzer kommunizierten Inhalte) oder einer Verschlüsselung der Luftschnittstelle gemeint ist.

Zusammengefasst besteht aus Sicht von Unitymedia daher noch folgender Änderungsbedarf:

1. Gesetzliche Klarstellung, was genau unter Verschlüsselung zu verstehen ist, beispielsweise Verschlüsselung der Luftschnittstelle
2. Eine Anpassung von § 8 Abs. 4 n.F. TMG dahingehend, die es Diensteanbietern ermöglicht, dass ihre Nutzer neben einem verschlüsselten Zugang alternativ auch einen unverschlüsselten Zugang auswählen können, ohne dass hierdurch das Haftungsprivileg entfällt

Im Einzelnen:

1. **Gesetzliche Klarstellung in § 8 Abs. 4 n.F. TMG, was genau unter Verschlüsselung zu verstehen ist, beispielsweise Verschlüsselung der Luftschnittstelle**

   Es ist unklar, was genau in § 8 Abs. 4 n.F. TMG mit einem „anerkannten Verschlüsselungsverfahren“ gemeint ist. Hier besteht die Gefahr, dass der Referentenentwurf zu erheblicher Rechtsunsicherheiten führt, wenn keine Klarstellung erfolgt. Es wäre beispielsweise keines-

falls sinnvoll und praktikabel, den gesamten Internetverkehr Ende-zu-Ende zu verschlüsseln, zumal dies auch aus (urheber-)rechtlichen Gesichtspunkten bedenklich wäre. Auch im „normalen“, leitungsgebundenen Internet erfolgt eine Übertragung in der Regel unverschlüsselt, sofern es sich nicht um eine vom Inhalteanbieter initiierte „https“- oder anderweitig gesicherte Verbindung handelt. Daher verstehen wir unter Verschlüsselung die Verschlüsselung der Luftschnittstelle, also des per Funk übertragenen Datenstroms zwischen dem (mobilen) Endgerät des Nutzers auf der einen und dem Access-Point des WLAN-Anbieters auf der anderen Seite. Dies ist ausreichend, um die Daten des Nutzers zu schützen und zu verhindern, dass sich ein Dritter in die Funkübertragung zwischen Nutzer und Access-Point einhacken kann.

2. Anpassung von § 8 Abs. 4 n.F. TMG dahingehend, die es Diensteanbietern ermöglicht, dass ihre Nutzer neben einem verschlüsselten Zugang alternativ auch einen unverschlüsselten Zugang auswählen zu können, ohne dass hierdurch das Haftungsprivileg entfällt

Um das von der Bundesregierung verfolgte Ziel der in urbanen Gebieten möglichst flächendeckenden Verbreitung von Internetzugangspunkten über WLAN zu fördern, ist es zentral, dass die Angebote möglichst einfach zu nutzen sind, damit sie am Ende auch angenommen werden. Tatsächlich führt aber eine Verschlüsselung je nach Art des genutzten Endgeräts und des darauf installierten Betriebssystems sowie der eingesetzten Verschlüsselungsmethode zu einem erheblichen Einrichtungsaufwand für den Nutzer. Insbesondere im Bereich einiger weit verbreiteter Desktop-Betriebssysteme – die bekanntlich auch auf Laptops genutzt werden – kann sich die Einrichtung des Zugangs zu einem verschlüsselten WLAN-Netz extrem kompliziert gestalten. Aus diesem Grund könnte das unbedingte Erfordernis der Verschlüsselung die tatsächliche spontane Nutzung erschweren und so die Verbreitung öffentlicher WLAN-Netze bremsen.

Gleichwohl halten wir den Ansatz für richtig, Nutzern durch die Möglichkeit der Verschlüsselung einen besseren Schutz auch ihrer sensiblen Daten bei der Nutzung eines Internetzugangs über ein öffentliches WLAN-Netz anzubieten. Aus dieser Überzeugung heraus verfolgt Unitymedia – anders als andere Anbieter – bei dem gerade im Aufbau befindlichen WLAN-Projekt zur Vernetzung der Stuttgarter Innenstadt genau diesen Ansatz und bietet den Nutzern auch die Möglichkeit eines verschlüsselten Internetzugangs an. Nichts desto

trotz ist Unitymedia der Auffassung, dass der Schutz der Daten auch in der eigenen Verantwortung des Nutzers liegt. Daher sollte diesem – ohne dass daraus Nachteile für den Anbieter folgen – eine Wahlmöglichkeit zwischen der Nutzung einer unverschlüsselten oder verschlüsselten Verbindung zur Verfügung stehen dürfen. Durch eine entsprechende Regelung könnte sowohl Sicherheitsinteressen als auch den Interessen an einer schnellen und umfassenden Verbreitung öffentlicher WLAN-Netze Rechnung getragen werden.