Deutscher Bundestag
18. Wahlperiode
Ausschuss für Wirtschaft und Energie

Ausschussdrucksache 18(9)651neu
15. Dezember 2015

Sitzung des Ausschuss für Wirtschaft und Energie:
Öffentliche Anhörung am Mittwoch, 16. Dezember 2015, 11.00 Uhr

Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes
Hier: Änderung des § 8 TMG

Stellungnahme von Dr. Dirk Häger
Fachbereichsleiter Operative Netzabwehr, BSI

1. Ausgangslage und Herausforderungen

Der mobile Zugriff auf das Internet ist heute für viele Bürger eine Selbstverständlichkeit, und wird in den nächsten Jahren in Häufigkeit und erforderlicher Bandbreite weiter ansteigen. Zwar decken die Betreiber der Mobilfunknetze einen Großteil dieser Anforderungen ab, aber einerseits sind die über die Mobilfunknetze übertragenen Datenmengen vergleichsweise teuer, und andererseits ist der erzielbare Datendurchsatz in vielen Situationen, insbesondere innerhalb größerer Gebäude, nicht ausreichend.

Viele Geschäftsleute bieten deshalb ihren Kunden als zusätzlichen Service einen WLAN-basierten Zugang zum Internet an. Ähnliches ist im privaten Umfeld zu beobachten: die Weitergabe von WLAN-Zugangspasswörtern an Freunde, Verwandte und Bekannte zwecks Internetzugang ist mittlerweile Alltag.

Viele Firmen realisieren den Internetzugang für ihre Kunden nicht selbst, sondern beauftragen einen kommerziellen Dienstleister. Dieser Dienstleister übernimmt als Internetzugangsanbieter in der Regel sowohl die Installation als auch den Betrieb, und ist nach derzeitiger Rechtsprechung als Zugangsanbieter allenfalls in Ausnahmefällen von der sogenannten Störerhaftung betroffen. Üblicherweise lehnt die Rechtsprechung eine Inanspruchnahme der kommerziellen Zugangsprovider nach den Grundsätzen der Störerhaftung ab.

Nicht so eindeutig stellt sich zur Zeit die Situation mit der Störerhaftung dar, wenn eine Firma selbst den Internetzugang zur Verfügung stellt, oder dies im privaten Umfeld geschieht. Auch hier für eine Begrenzung des Haftungsrisiko zu sorgen, ist Ziel der Gesetzesände-

rung. Diese Gleichstellung mit den kommerziellen Dienstleistern ist an Auflagen gebunden. Die Bewertung, ob die Auflagen zur Zielerreichung geeignet und welche Maßnahmen zur Umsetzung der Auflagen geeignet und angemessen sind, ist Gegenstand dieses Gutachten.

2. IT-Sicherheit von WLAN-Netzen

Das BSI hat mit der TR-03103 eine detaillierte Richtlinie veröffentlicht, wie ein sicheres WLAN betrieben werden sollte, und auch im IT-Grundschutz gibt es umfangreiche Empfehlungen für einen sicheren Betrieb. Vorrangiges Schutzziel dieser Empfehlungen ist jedoch, unbefugte Dritte aus den internen Netzen heraus zu halten und damit die Vertraulichkeit und Integrität der Daten zu schützen sowie die Verfügbarkeit des Dienstes sicher zu stellen. Im Vergleich zu kabelgebundenen Netzen kommt bei Funknetzen vor allem das Risiko hinzu, dass ein Angreifer aus der (Funk-)Distanz heraus, d.h. ohne physischen Kontakt zu geschützten IT-Systemen oder Datenkabeln, agieren kann. Für den sicheren Betrieb eines solchen WLAN ist die verschlüsselte Übertragung der Funksignale unabdingbar.

Darüber hinaus gelten die Standardsicherheitsmaßnahmen für Datennetzwerke. Exemplarisch seien hier einige aufgezählt:

- Schutz des Netzwerkes gegen Angriffe aus dem Internet
- Regelmäßige Einspielen von Sicherheitsupdates
- Regelmäßige Audits der Netzwerkkomponenten

Wirksame Verschlüsselung vorausgesetzt, kann ein Angriff von außen nur über das Internet (Cyberangriff) oder durch physischen Zugang (z.B. durch Einbruch) – nicht jedoch auf der internen WLAN-Übertragungsstrecke – durchgeführt werden.

3. IT-Sicherheit bei WLAN-Internetzugangsanbietern

Die Bundesnetzagentur erstellt nach § 109 TKG einen Katalog von Sicherheitsanforderungen für den Betrieb von Telekommunikationssystemen. Grundsätzlich, wenn auch in stark reduziertem Umfang, muss dieser auch für WLAN-Internetzugänge gelten. Mindestens müssen der Schutz eventuell vorhandener personenbezogener Daten und der Schutz des

Fernmeldegeheimnisses sicher gestellt werden.Von einem WLAN-Betreiber ist also zu verlangen, dass er seine Infrastruktur absichert. Die zugrunde liegende Pflicht zur Umsetzung von Sicherheitsanforderungen ergibt sich, falls der WLAN-Betreiber insgesamt einem Diensteanbieter nach § 8 Abs. 1 TMG gleichgestellt wird, aus § 13 Abs. 7 TMG. Sofern er als Betreiber eines – zugegeben kleinen – öffentlichen Telekommunikationsnetzes im Sinne des TKG angesehen werden sollte, folgt es aus § 109 TKG.

4. Verhinderung unberechtigter Nutzung

Der neue § 8 Abs. 4 TMG-E fordert Maßnahmen seitens der WLAN-Betreiber. Nach meinem Verständnis handelt es sich dabei um folgende zwei zusammenhängende Pflichten:

- Die WLAN-Anbieter sollen nur solche Nutzer in ihr WLAN lassen, die erklärt haben, keine Rechtsverletzung zu begehen.
- Auf Basis dieser Erklärung soll eine zweite Pflicht der WLAN-Anbieter darin bestehen, technisch sicher zu stellen, dass nur eben diesen Nutzern Zugang gewährt wird.

Die Gesetzesformulierung „Sicherungsmaßnahmen gegen den unberechtigten Zugriff“ sollte also nicht als IT-Sicherheitsmaßnahmen im Sinne obigen Abschnitts „3. IT-Sicherheit eines WLAN-Internetzugangsanbieters“ interpretiert werden, sondern als Maßnahme zur Durchsetzung einer Einverständniserklärung des Nutzers.[1]

Als technische Maßnahme zur Durchsetzung dieser Forderung kommen vor allem zwei Lösungen in Betracht:

1. Zurverfügungstellung eines mit einem starken Passwort WPA2-verschlüsselten Gastzuganges. Jeder Nutzer muss das Zugangspasswort geeignet erfragen und den Nutzungsbedingungen zustimmen. Dies ist vor allem eine Lösung für kleine, dauerhafte Nutzergruppen. Viele der in Deutschland eingesetzten WLAN-Router bieten dies seit Jahren als Funktion an, so dass diese Maßnahme für viele WLAN-Betreiber ohne besondere Mehraufwände realisierbar wäre.
2. Zurverfügungstellung eines unverschlüsselten WLAN-Zugangs, bei dem die Nutzer auf einer verpflichtenden Begrüßungsseite ihr Einverständnis mit den Nutzungsbe-

1 Die in der Gesetzesbegründung angegebene Aussage, dass dies auch im Interesse des Betreibers läge, weil so auch seine Daten und die der Nutzer gegen Zugriff gesichert würden, kann nicht nachvollzogen werden, da der Betreiber diese Sicherungspflichten bereits nach § 13 Abs. 7 TMG bzw. § 109 TKG hat.

dingungen abgeben müssen. Dies kann gegebenenfalls mit weiteren Funktionen, wie z.B. dem Nachweis der Bezahlung, verknüpft sein. Dieses Verfahren ist für große Gruppen geeignet und entspricht dem heutigen Stand der Technik in vielen kommerziell betriebenen WLAN-Netzen; es ist aber auch mit Open Source Mitteln umsetzbar.

Achtung: Beide Verfahren schützen nicht davor, dass ein WLAN-Nutzer einen anderen ausspioniert. Zum Schutz der Vertraulichkeit der Kommunikation kann der WLAN-Betreiber nur seine eigene Infrastruktur geeignet schützen. Für die Übertragungsstrecke zwischen dem WLAN-Router und dem Endgerät gibt es keine geeignete Lösung, die seitens des Betreibers angeboten werden könnte, um die Nutzer vor gegenseitigem Lauschen zu schützen. Auch eine WLAN-Verschlüsselung hilft hier nicht, da alle Nutzer das Verschlüsselungskennwort kennen. Vielmehr müssen die Nutzer darauf achten, ihre sensiblen Informationen unabhängig vom WLAN selber zu verschlüsseln. Dadurch, dass immer mehr insbesondere große Dienste auf Anwendungsebene verschlüsseln (z.B. Webmail, aber natürlich auch Online-Banking und selbst Suchmaschinen), wird das Missbrauchspotential aber stetig, wenn auch sehr langsam, geringer.

Bei beiden Verfahren sind Umgehungsmöglichkeiten vorhanden. Im ersten Verfahren könnte ein Nutzer das Passwort an einen Dritten weitergeben. Da eine räumliche Nähe zum WLAN-Router notwendig ist, wäre eine häufige Ausnutzung zwar möglich, aber mit einem gewissen Entdeckungsrisiko verbunden.

Im zweiten Verfahren könnte ein unberechtigter Dritter die Verbindung abhören, und sich dann technisch als derjenige ausgeben, der sein Einverständnis erklärt hat. Die Eintrittswahrscheinlichkeit hierfür ist jedoch gering. Warum sollte jemand sich den Aufwand auferlegen, illegal Funkverkehr abzuhören, nur um eine Einverständniserklärung zu umgehen? Es wäre für ihn einfacher, die Einverständniserklärung abzugeben und sich danach nicht an sie zu halten.

Insofern sind beide Verfahren meines Erachtens geeignet, die im Gesetz geforderten „angemessen Sicherungsmaßnahmen“ zu erfüllen.

5. Missbrauchspotential

Selbstverständlich sind bei der Nutzung von WLAN-Zugängen illegale Handlungen im Internet möglich. Es wäre aber nur in seltenen Fällen vorstellbar, dass Täter den

WLAN-Zugang eines Bekannten regelmäßig für illegale Aktivitäten verwenden. Ihr Identifizierungsrisiko wäre hier ungleich höher, als wenn sie im Internet einen der vielen Anonymisierungsdienste verwenden würden.
Ähnliches gilt für die Verwendung öffentlicher WLAN-Netze. Hier ist mindestens durch den Ortsbezug immerhin ein Identifikationsansatz gegeben. Auch hier wäre die Verwendung von Anonymisierungsdiensten für Täter die geeignetere Verschleierungsmaßnahme.

Auch der Austausch urheberrechtlich geschützten Materials wäre über WLAN-Zugänge möglich. Aber seit dem Aufkommen immer mehr legaler Streaming-Dienste für Musik wie beispielsweise Spotify nimmt der missbräuchliche Download von MP3-Dateien seit Jahren stark ab. Ähnliches, wenn auch weniger stark, gilt für den Download aktueller Kinofilme. Da Filme jedoch ein sehr viel größeres Datenvolumen haben und damit bis zu mehreren Stunden zum Herunterladen notwendig sind, scheint auch dieses Missbrauchsrisiko eher gering zu sein.

Ein Missbrauchspotential durch die breite zur Verfügungstellung von WLAN-Internetzugängen ist vorhanden. Die Gesamtgefährdungslage wird dadurch jedoch nur unwesentlich erhöht.

6. Fazit

Das Gesetz ist, wenn die „angemessenen Sicherungsmaßnahmen“ den aufgezeigten Umfang nicht überschreiten, geeignet, das im Koalitionsvertrag gesetzte Ziel der Rechtssicherheit für WLAN-Betreiber zu schaffen.