16. August 2016

Stellungnahme zum Begutachtungsentwurf des Funkanlagen-Marktüberwachungs-Gesetz (FMAG, 220 ME / XXV. GP)

Unterstützt von:

Aaron L. Kaplan
(Privatperson)

AKVorrat Arbeitskreis Vorratsdaten
info@akvorrat.at
ZVR: 140062668

INITIATIVE FÜR NETZFREIHEIT
info@netzfreiheit.org
ZVR: 675848645

C³W Chaos Computer Club Wien
buero@c3w.at
ZVR: 656204875

FUNKFEUER WIEN
vorstand@funkfeuer.at
ZVR: 814804682

Zusammenfassung

Das in Begutachtung stehende Gesetz setzt die Richtlinie 2014/53/EU (sog. „Funkrichtlinie“) in Österreich um. Es zielt auf die gesetzeskonforme Einhaltung der Funkstandards (z. B. 100mW EIRP Sendeleistung bei 2.4GHz-WLAN) ab. Wir begrüßen diese Initiative prinzipiell, da unkontrolliertes (“zu lautes”) Senden mit hoher Sendestärke für alle WLAN-Geräte im Umkreis nachteilig ist, als auch Effekte auf z.B. das Wetter-Radar haben kann. Allerdings ergeben sich durch die vorgeschlagene Umsetzung auch sicherheitsrelevante Nebeneffekte, auf die in dieser Stellungnahme in der Folge eingegangen wird. Wir möchten eine Beachtung der nachfolgenden Aspekte bei der gesetzlichen Regelung mit Nachdruck anstoßen.

Betroffene Bestimmungen

§ 3 Abs. 3 des vorliegenden Gesetzesentwurfs sieht vor:

> *„Der Bundesminister für Verkehr, Innovation und Technologie kann durch Verordnung Klassen oder Kategorien von Funkanlagen bestimmen und dabei festsetzen, welche Klasse oder Kategorie zusätzlich zu den in Abs. 1 und 2 genannten grundlegenden Anforderungen eine oder mehrere der folgenden grundlegenden Anforderungen erfüllen muss:*
> *(...)*
> *Z 4. sie haben weder schädliche Auswirkungen auf Kommunikationsnetze oder deren Betrieb noch bewirken sie eine solche Nutzung von Netzressourcen, durch welche eine längerfristige zweckgerechte Nutzung des Dienstes nicht mehr möglich wäre;*
> *Z 5. sie verfügen über Sicherheitsvorrichtungen, die sicherstellen, dass personenbezogene Daten und die Privatsphäre des Nutzers und des Teilnehmers geschützt werden;*
> *(...)*
> *Z 9. sie unterstützen bestimmte Funktionen, mit denen sichergestellt werden soll, dass nur solche Software geladen werden kann, für die die Konformität ihrer Kombination mit der Funkanlage nachgewiesen wurde.“*

Zur Ziffer 9 wird in den Erläuterungen präzisiert:

> *„Das in Z 9 genannte Gebot stammt aus der Richtlinie. Zweck der Regelung ist es, Änderungen an der Software, welche die technischen Funkparameter verändern, zu verhindern. In der Vergangenheit war es nicht unüblich, die Software der Geräte zu verändern um mit dieser geänderten Konfiguration Einfluss auf die Funkparameter*

wie automatische Frequzenzauswahl und Sendeleistung zu nehmen. Dies führte oft zu Störungen beim Betrieb anderer Geräte auch außerhalb des manipulierten Frequenzbereichs und hat nicht notwendigerweise die objektive Sendequalität des manipulierten Geräts verbessert. Derartige Veränderungen der Funkparameter sind auch nach der bisher geltenden Rechtslage unzulässig, durch die nun verlangte technische Sperre für solche Softwareupdates soll auch die verbotene Umprogrammierung verhindert werden.
Von diesem Gebot bleiben jene Softwareteile unberührt, welche nicht die funktechnischen Eigenschaften betreffen, etwa die Ausgestaltung der Bedienoberfläche. Solche Veränderungen bleiben zulässig. Da jedoch die Trennung zwischen jenen Softwareteilen, die zu sperren sind und jenen, die verändert werden dürfen, für die Betreiber offenbar zu viel Kosten erzeugen, wird von den Betreibern in der Praxis jedwedes Softwareupdate blockiert, ohne dass es dafür eine gesetzliche Pflicht gibt."

Detailerläuterungen

Zu den eingangs genannten Nebeneffekten zählt aus unserer Sicht auch der hier beschriebene pragmatische Weg im Interesse der BetreiberInnen (z.B. Provider). Die verlangte technische Sperre für Software-Updates, die die Konformität von Funkanlagen sicherstellen sollen, ist nicht zielführend. Erfahrungsgemäß ist anzunehmen, dass in der Praxis (Kostenersparnis, komplexe interne Prozesse beim Hersteller) Softwareupdates - inkl. das Schließen kritischer Sicherheitslücken - erschwert werden. Die Zertifizierung der Software erfordert darüber hinaus eine Absicherung des Updateprozesses, welche kommerzielle oder freie alternative Gerätesoftware (Firmware)[1] unmöglich macht und hierdurch die Abhängigkeit vom Gerätehersteller erzwingt.

Hier entsteht aus unserer Sicht ein Spannungsverhältnis zwischen § 3 Abs 3 Z 9 und den ebenfalls oben zitierten § 3 Abs 3 Ziffern 4 und 5. Softwareupdates sind notwendig, um sowohl das eigene System – und somit auch die eigene Privatsphäre – als auch das Netz als Ganzes zu schützen[2]. Sie sind erforderlich, da fortlaufend Lücken im System entdeckt werden und mittels Update geschlossen werden müssen, um

[1] wie beispielsweise "DD-WRT" oder "OpenWRT" oder kommerzielle Gerätesoftware Hersteller
[2] Beispielsweise können sogar ganz große Internet Service Provider mittels DDOS Angriffen, die genau über verwundbare, kleine WLAN Router ausgeführt warden ("UDP Amplification attacks"), lahm gelegt werden.
Siehe auch https://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks/

Fremdzugriff auf das System und dessen Funkparameter zu verhindern. Anders formuliert: **Der vorliegende Gesetzesentwurf geht von einem perfekten System ohne Sicherheitsfehler aus, in dem zu keinem Zeitpunkt ein Nachbesserungsbedarf besteht**.

Kritische Sicherheitslücken werden zum überwiegenden Teil erst im Betrieb der vom Entwurf betroffenen Systeme entdeckt. Die nachträgliche Absicherung von Sicherheitslücken wird deshalb erst während des Lebenszyklus des betroffenen Gerätes möglich und meist vom Hersteller durchgeführt in der Form von downloadbaren Updates bereitgestellt. Durch den vorliegenden Entwurf sind derartige Sicherheitsupdates durch den Hersteller oder durch den Endnutzer über alternative Gerätesoftware (Firmware) jedoch signifikant erschwert bzw. unmöglich gemacht.

JedeR der/die mit einem Computer arbeitet, kennt die Notwendigkeit, regelmäßig Softwareupdates einzuspielen und kann daraus folgern, dass dieses „perfekte" System realitätsfremd ist. Diese Notwendigkeit, Updates durchzuführen, gilt auch für die Software von Funkanlagen, vor allem z.B. WLAN Geräten in privaten Haushalten und Unternehmen. Ein unsicheres lokales Netzwerk bietet eine sehr einfache Möglichkeit, private Daten unrechtmäßig zu kopieren und oder zu verändern. WLAN Router ohne Software Updates sind ein Einfallstor für diverse IT-Sicherheitsprobleme. [3] [4] [5]

Zum Status quo: Vor Umsetzung dieser Richtlinie ist es technisch möglich, Updates für die Software der verwendeten Funkanlagen (beispielsweise WLAN Router für private Haushalte oder Unternehmen) oder aber auch alternative Firmwares, die aktuellere Software-stände beinhaltet, aufzuspielen und sich somit um die Sicherheit des eigenen Systems – und somit der eigenen Privatsphäre oder im Fall von Unternehmen die Sicherheit von Firmenstrategien und Betriebsgeheimnissen – zu kümmern.

Mit der Umsetzung der Richtlinie entfällt diese Möglichkeit aufgrund des Entgegenkommens gegenüber den BetreiberInnen. Die Kosten der BetreiberInnen sollen nämlich möglichst geringgehalten werden. Privatpersonen und Unternehmen

[3] http://www.heise.de/newsticker/meldung/Wurm-Alarm-bei-Linksys-Routern-2115285.html
[4] http://www.heise.de/security/meldung/Wieder-eine-Routerluecke-Loechriges-Webinterface-beim-Linksys-WRT120N-2119285.html

[5] http://futurezone.at/digital-life/millionen-wlan-router-haben-sicherheitsluecke/24.574.532

haben deshalb nur noch die Möglichkeit den BetreiberInnen zu vertrauen.

Schlusserläuterungen

In Anbetracht dessen, **dass das Recht auf Schutz der Privatsphäre ein Grundrecht ist** und das Bedürfnis nach geringeren Kosten lediglich einen Wunsch der BetreiberInnen darstellt, halten wir es für unumgänglich, die Einhaltung des § 3 Abs 3 Z 5 sicherzustellen, indem den BetreiberInnen die Haftung für die Sicherstellung von personenbezogenen Daten und der Privatsphäre der NutzerInnen und der TeilnehmerInnen auferlegt wird.

Darüber hinaus empfiehlt es sich, die im Gesetzesentwurf mehrfach gewählte Möglichkeit zu präzisierenden Regelungen per Verordnung auch im Zusammenhang mit dem Schutz der Privatsphäre und dem Schutz personenbezogener Daten zu ermöglichen. Da diese Materie tief in den Konsumentenschutz eindringt, halten wir es für unverzichtbar, dass Verordnungen hinsichtlich des § 3 Abs 3 Z 9 im Zusammenhang mit § 3 Abs 3 Z 5 in enger Zusammenarbeit mit der für Konsumentenschutz zuständigen Sektion (derzeit im BMASK angesiedelt) zu erarbeiten sind.

Aus Sicherheitsperspektive ist explizit festzuhalten, dass der vorliegende Entwurf die Gefahr in sich birgt, die Sicherheit informationstechnischer Systeme in Österreich drastisch zu gefährden.

Dieses Problem ist angesichts der steigenden Vernetzung informationstechnischer Systeme auch im Rahmen von kritischer Infrastruktur und der rasant steigenden Verbreitung von Kleingeräten ohne Update-Funktion im Internet of Things (IoT) oder vernetzte Industrieanlagen als besonders kritisch zu bewerten.

Des Weiteren werden erfolgreiche Geschäftsmodelle von österreichischen Firmen verunmöglicht. Viele Firmen, welche WLAN im Tourismus und städtischen Bereich (Freewave, Winterski-Gebiete, WLAN für Gäste) anbieten, brauchen die Möglichkeit, Fernupdates auf WLAN Router zu spielen.

Deshalb fordern wir alle zur Verfügung stehenden Spielräume im Rahmen der Umsetzung auszunutzen um die dargelegten negative Auswirkungen zu minimieren. Darüber hinaus ist eine Novellierung der zugrundeliegenden EU-Richtlinie 2014/53/EG zum frühestmöglichen Zeitpunkt dringend anzuraten.