19. April 2007, von Michael Schöfer
Sicherheitslücke beim "Fritz!WLAN-Stick" von AVM

Kürzlich habe ich mir ein neues Notebook gekauft. Da ich damit auch vom Küchentisch aus ins Internet wollte und keine Lust hatte, meine Wohnung über das heutige Maß hinaus zu verkabeln, erwarb ich kurzerhand einen WLAN-Router von AVM mit dazu passendem WLAN-USB-Stick. Es ist ja so einfach: "Der FRITZ!WLAN USB Stick wird vor dem ersten Einsatz einmal kurz an den USB-Host der betreffenden FRITZ!Box WLAN angesteckt. Die (...) Parameter der FRITZ!Box werden nun automatisch auf den FRITZ!WLAN USB Stick übertragen. Anschließend wird der FRITZ!WLAN USB Stick an den Computer angesteckt und die auf den Stick geladenen Parameter der Funkzelle werden - wiederum automatisch - auf den Computer übermittelt. Im Anschluss daran verfügt die WLAN-Steuerungssoftware über diese Informationen und kann somit den Zutritt zu der gesicherten Funkzelle erlangen. WLAN-Fehlkonfigurationen und lange Einrichtungszeiten gehören so der Vergangenheit an. AVM Stick & Surf bietet also maximale Sicherheit bei maximalem Komfort", heißt es dazu auf der Website von AVM. Komfort? Ja. Aber maximale Sicherheit? Nein! Oder zumindest nur eine eingeschränkte.

Man kann nämlich den WLAN-Schlüssel, der den Stick wie oben beschrieben automatisch mit der Basisstation verbindet und das System gegenüber Angriffen von außen abschottet, am Notebook jederzeit im Klartext (!) auslesen. Dazu muss man in der Steuerungssoftware bloß auf das Symbol der Basisstation klicken - schon ist er frei zugänglich. Das hat mich doch sehr gewundert. Natürlich ist meine Fritz!Box mit WPA2 verschlüsselt, der WLAN-Schlüssel selbst besteht aus einer ausreichend langen Kombination von Buchstaben, Zahlen und Sonderzeichen. Nach heutigem Wissen also kaum zu knacken. Bekanntlich haben nicht alle Menschen gute Absichten. Und Vorsicht ist die Mutter der Porzellankiste. Außerdem wird überall vor dem Gebrauch von unverschlüsselten oder nur unzureichend - etwa mit WEP - verschlüsselten WLAN-Funknetzen gewarnt.

Logischerweise schrieb ich gleich an den Hersteller und bekam prompt folgende Antwort: "Durch die Aktivierung der Option 'WLAN-Verschlüsselung verbergen' ist die eingetragene WLAN-Verschlüsselung nicht mehr auslesbar. Bitte klicken Sie mit der rechte Maustaste auf das Symbol des FRITZ!WLAN Sticks, dann auf Eigenschaften. Dort können Sie diese Option aktivieren." Ich dankte für die rasche Reaktion, aber das hatte ich schon ausprobiert. Das Problem wird dadurch leider nicht gelöst, weil jeder Benutzer des Notebooks diesen Vorgang auf dem gleichen Weg wieder rückgängig machen kann. Die von AVM genannte Funktion, unter Eigenschaften das entsprechende Häkchen setzen bzw. entfernen, ist (bis zur Version 05.04.17) nicht durch ein Kennwort vor Änderungen geschützt. Letzteres würde wenigstens Abhilfe schaffen.

Nur wenn ich das Notebook zuvor als Administrator starte und die WLAN-Verbindung per Stick aktiviere, können andere Benutzer nicht auf die Einstellungen der Steuerungssoftware zugreifen (die Menüs in der Taskleiste sind dann auf dem eingeschränkten Benutzerkonto gesperrt). Wenn jedoch der andere Benutzer das Notebook selbst startet und die WLAN-Verbindung eigenhändig aktiviert, kann er auf alles ohne Einschränkung zugreifen. Um das Auslesen des Schlüssels zu verhindern, müsste ich mich also jedesmal erst als Administrator anmelden, bevor ich anderen Benutzern das Notebook überlasse. Ehrlich gesagt ziemlich umständlich und daher unpraktikabel. "Wäre es nicht besser, die Einstellungen des Sticks mit Hilfe eines Kennworts zu schützen, wie das bei den Einstellungen der WLAN-Basisstation möglich ist?", hakte ich nach.

Wieder kam nach kurzer Zeit Antwort, aber bedauerlicherweise keine Lösung des Pro-

blems. Ich hatte offenbar überhaupt nichts, wie zunächst befürchtet, falsch gemacht. AVM musste nämlich zugeben: "Die von Ihnen gewünschte Funktion [der Kennwortschutz] wird derzeit nicht unterstützt", schrieb man mir. "Ich habe Ihre Anfrage daher als Verbesserungsvorschlag an den zuständigen Produktmanager in unserem Haus weitergeleitet. Ob und wann eine Umsetzung erfolgen wird, steht zum jetzigen Zeitpunkt allerdings noch nicht fest. Verbesserungsvorschläge und Wünsche unserer Kunden werden gerne berücksichtigt, da unsere Produkte natürlich davon 'leben'. In der Vergangenheit haben wir deshalb bereits unzählige Verbesserungsvorschläge in die Tat umgesetzt (nicht selten schon direkt in der nächsten Version)."

Ich muss demzufolge wohl oder übel abwarten, bis AVM diese Sicherheitslücke mit einem neuen Firmware-Update schließt. Bis dahin gebe ich das Notebook am besten keinem anderen Benutzer in die Hand. Bei mir geht das. Doch was machen eigentlich diejenigen, bei denen solche Restriktionen aus privaten oder beruflichen Gründen nicht möglich sind?