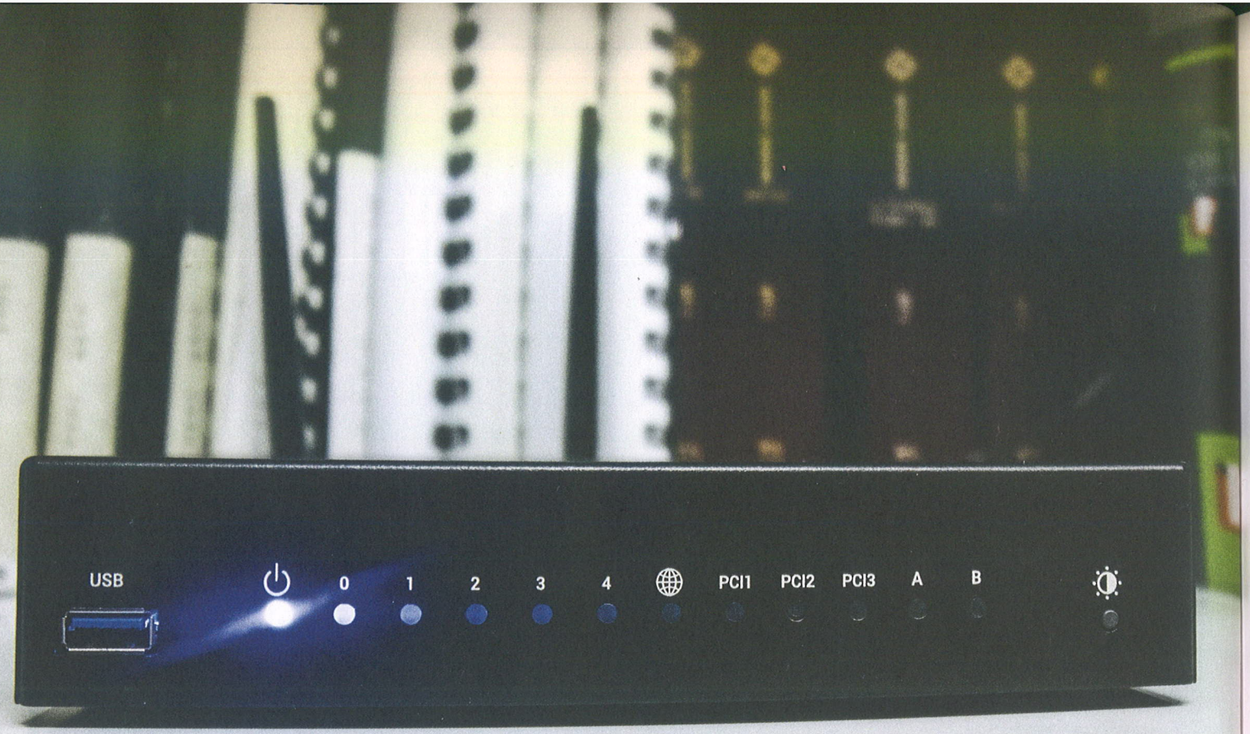


Quelloffener WLAN-Router Turris Omnia aus Tschechien

Sicherer Netzwerker

Router fallen immer wieder durch schlechte Sicherheit negativ auf – nicht nur solche der Telekom. Der Turris Omnia aus Tschechien will das mit quelloffener Hard- und Software besser machen. Jan Rähm

README

Aus der Tschechischen Republik kommt ein Router, der die Konkurrenz mit besonders guten Sicherheitsmerkmalen, feiner Hardware und komplett offengelegten Quellen ausstechen möchte. Wir haben uns den Turris Omnia der CZ.NIC im Praxistest angesehen.

Vor gut einem Jahr sorgte eine Crowdfounding-Kampagne unter Netzwerkspezialisten für einiges Aufsehen: Die tschechische CZ.NIC suchte nach Unterstützern für einen Internet-Router, der sich von der Masse der Geräte auf dem Markt abhob. Er sollte nicht nur besonders hochwertig ausgestattet sein, sondern auch von der Hardware bis zur Software quelloffen und außerdem besonders sicher. Die Spendensammlung verlief erfolgreich, und seit einigen Wochen liefert der Hersteller das Gerät nun unter dem Namen Turris Omnia aus. Wir konnten uns ein erstes Exemplar des Routers für einen kurzen Test sichern.

Die Telekom lässt grüßen

Internet-Router gibt es wie Sand am Meer. Doch die kleinen Kisten, die zu Hause oder im Büro die Verbindung ins Internet herstellen, sorgen immer wieder für Aufsehen. Der jüngste spektakuläre Fall: Ende November 2016 blieb rund 900 000 Kunden der Telekom stunden- und teils tagelang der Internet-Zugang verwehrt, weil die von der Telekom gelieferten Speedport-Router aufgrund eines Angriffs den Dienst verweigerten.

Die Ironie der Angelegenheit: Der Angriff hatte noch nicht einmal den Telekom-Routern gegolten. Er zielte über das TR-069-Protokoll auf die verwundbare Fernwartungsschnittstelle eines völlig anderen Gerätetyps. Um die angepeilten Router über diese vorhandene Sicherheitslücke in ein Botnetz einbinden zu können, fluteten die Angreifer das Internet erst einmal wahllos mit Port-Knocking-Paketen, um einen Kommunikationskanal zu den betroffenen Systemen zu öffnen.

Auch die Speedport-Router der Telekom verfügen über eine entsprechende Fernwartungsfunktion, deren Implementation allerdings für den geplanten Angriff nicht verwundbar ist. Zudem wurde sie auf den Routern überhaupt nicht genutzt. Die Telekom hatte allerdings auf den Geräten trotzdem fahrlässigerweise den entsprechenden Zugangsport 7547/tcp sperrangelweit offen stehen lassen, obwohl Kunden das Unternehmen schon seit 2014 vor dieser potenziellen und völlig überflüssigen Sicherheitslücke gewarnt hatten.

Die Quittung für diese unglaubliche Schlamperei lieferte der Angriff: Die vielen auf der unnötig offenstehenden Fernwartungsschnittstelle eintreffenden Anfragepakete konnte zwar den betroffenen Port nicht öffnen und schon gar nicht die grundsätzlich immunen Systeme infizieren. Sie brachte aber die Telekom-Router durch die schiere Masse der Pakete derart aus dem Tritt, dass sie ihren Betrieb ganz einstellten.

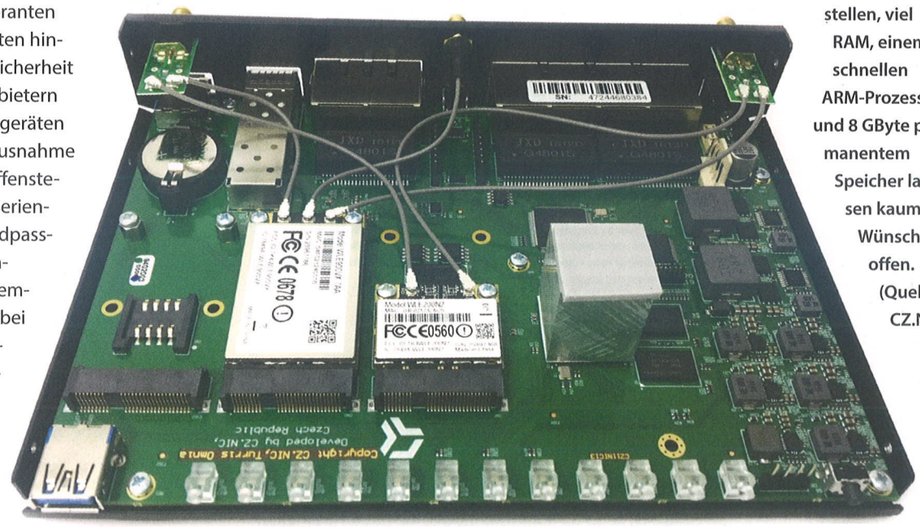
Solche ignoranten Nachlässigkeiten hinsichtlich der Sicherheit stellen bei Anbietern von Netzwerkgeräten leider keine Ausnahme dar: Sinnlos offenstehende Ports, serienweite Standardpasswörter und angreifbare Systemsoftware sind bei vielen Herstellern an der Tagesordnung. Der arglose Kunde bemerkt das aber oft erst, wenn es bereits zu spät ist. Doch selbst wenn aufmerksame Anwender den Anbieter warnen, ignoriert der – wie im aktuellen Fall die Telekom – oft die Sicherheitsmängel geflissentlich, bis es zur Katastrophe kommt.

Bei der Entwicklung des Turris Omnia dagegen stand die Sicherheit von Anfang an im Fokus, der Internet-Router versucht seine Anwender mit zahlreichen Features zu schützen. Entwickelt wurde er von einem Team der CZ.NIC, dem tschechischen Pendant zur deutschen DENIC: Sie zeichnet als Top-Level-Registrar zuständig für die entsprechende Länderdomain CZ.

Darüber hinaus investiert das Non-Profit-Unternehmen auch in Forschung und Entwicklung. So analysiert die CZ.NIC Störungen und Angriffe in und auf Netze. Die Erkenntnisse daraus nutzt die Organisation für eine verteilte Firewall, die auch die Nutzer des Turris Omnia schützen soll.

Hightech schlicht verpackt

Seit dem Ende der Crowdfunding-Phase kann man den Turris Omnia regulär bei CZ.NIC vorbestellen. Zur Auswahl stehen zwei Varianten, die sich lediglich im Ausbau des Arbeitsspeichers unterscheiden. Für 289 Euro gibt es den Router mit 1 GByte RAM, für 329 Euro mit der dop-



1 Leistungsfähige Hardware in schlichter Optik: Die Bestückung mit drei Mini-PCI-Express-Schnittstellen, viel RAM, einem schnellen ARM-Prozessor und 8 GByte permanentem Speicher lassen kaum Wünsche offen. (Quelle: CZ.NIC)

2 Exot im Router-Markt: Der Turris Omnia bringt nicht nur fünf plus eine Gigabit-Ethernet-Schnittstelle und schnelles ac-WLAN mit, sondern bietet sogar einen SFP-Port. (Quelle: CZ.NIC)

pelten Kapazität. Unter der Haube glänzt der Turris Omnia mit einer potenten Ausstattung. Als Herz der Maschine dient eine mit 1,6 GHz getaktete ARM-CPU mit zwei Rechenkernen, der ab Werk 8 GByte dauerhafter SSD-Speicher zur Verfügung stehen.

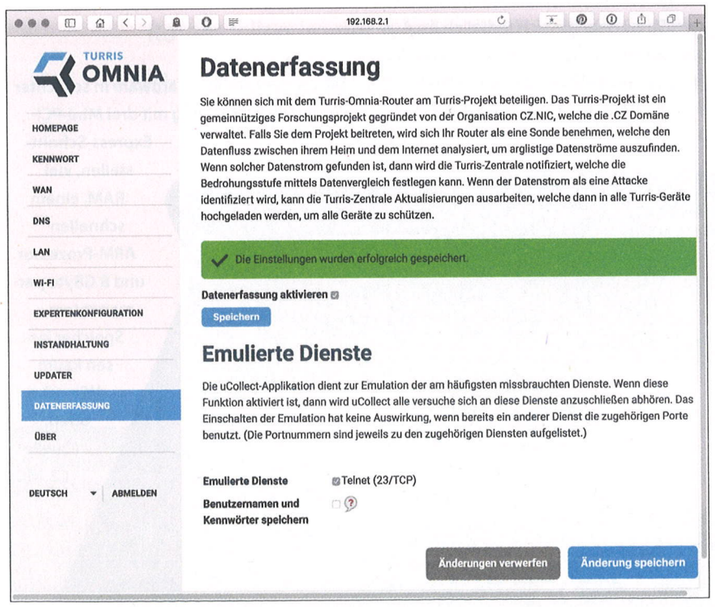
Dank dreier Mini-PCI-Express-Steckplätze, von denen einer auch das SATA-Protokoll unterstützt, lässt sich der Festplattenspeicher mit SSD-Blades erweitern. Bei Auslieferung stecken in zwei der drei Plätze je ein WLAN-b/g/n- und ein WLAN-ac-Modul 1. Alternativ lassen sich neben Speichermedien auch andere Module einsetzen, wie beispielsweise ein LTE-Modem oder andere WiFi-Module. Für den Einsatz von Mobilfunkmodulen ist der Router mit einem SIM-Karten-Einschub auf dem Mainboard vorbereitet.

Die gesamte Hardware des Turris Omnia wird komplett vom aktuellen Linux-Kernel unterstützt. Bis auf eine Ausnahme liegen für alle Komponenten freie Treiber samt entsprechender Dokumentation vor; lediglich die WLAN-Schnittstelle benötigt ein Binary vom Hersteller.

Optisch präsentiert sich der Turris Omnia ziemlich nüchtern. Die Technik steckt in einem für (semi-)professionelle Netzwerktechnik üblichen, schnörkellosen Metallgehäuse. Über den aktuellen Betriebszustand geben zwölf frontseitige LEDs Auskunft, deren Helligkeit und sogar Farbe sich mithilfe eines Schalters auf der rechten Gehäuseseite regeln lässt. Neben den LEDs auf der linken Seite der Front wartet eine von zwei USB-3.0-Schnittstellen auf ihren Einsatz.

Die Rückseite des Routers dominieren die drei WLAN-Antennen, die man je nach geplantem Einsatz leicht wechseln kann. Beim Blick auf die Anschlüsse überrascht der sogenannte SFP-Port: Er nimmt verschiedene Module zur Vernetzung auf und ist in Geräten dieser Preisklasse eher selten anzutreffen.

Über die SFP-Schnittstelle 2 binden Sie den Router beispielsweise per Glasfaser ins LAN ein oder ans Internet an. Alternativ nimmt der Port auch Modems für VDSL oder andere Verbindungstechnologien auf. Setzen Sie bereits ein Breitbandmodem ein, verbinden Sie es über die GbE-fähige WAN-Schnittstelle und ein Netzwerkkabel mit dem Turris Omnia. Fünf Gigabit-Netzwerk-Buchsen und ein zweiter USB-3.0-Anschluss komplettieren die Schnittstellenvielfalt.



3 Verteilter Schutz nach Wunsch: Die Distributed Firewall der CZ.NIC müssen Sie bewusst aktivieren. Erst dann überträgt der Router Daten zur Analyse an den Anbieter.

Offen im positiven Sinn

Die Software des Systems basiert auf dem quelloffenen Router-Betriebssystem OpenWRT, auch die Hardware ist fast lückenlos dokumentiert und beschrieben. Das erlaubt Nutzern beispielsweise, die verteilte Firewall im Quellcode zu überprüfen oder, sofern man über entsprechende Fähigkeiten verfügt, den Router auch komplett nachzubauen.

Aber auch, wenn Sie nicht soweit gehen wollen, können Sie das installierte System erweitern und umbauen oder die Software durch eine andere Distribution ersetzen. Denkbar wären beispielsweise ein Netzwerkspeichersystem (NAS) oder ein kleiner Heimserver – sowohl out-of-the-box mit der vorinstallierten Software oder auf Basis einer selbstgewählten Linux-Spielart.

Die bereits angesprochene verteilte Firewall zählt zu den herausragenden Alleinstellungsmerkmalen des Routers. Sie soll den Nutzer auch vor Angriffen schützen, die ganz neu aufkommen. Diese Attacken will die CZ.NIC erkennen, analysieren und aus den Erkenntnissen schnellstmöglich Gegenstrategien entwickeln, die der Anbieter dann an die Geräte der Kunden überträgt.

Dazu sammelt der Hersteller den Datenverkehr zwischen Kunde und Internet, erklärt Turris-Entwicklungsleiter Bedřich Kosata vom Domain-Registrar CZ.NIC: „Dadurch, dass wir den Verkehr vieler für uns anonymer Kunden kennen, haben wir eine große Datenbasis, die wiederum den Kunden zugute kommt." Die Daten analysiert CZ.NIC auf ungewöhnliche Muster hin. Bei auffälligem oder gar verdächtigem Verhalten im Datenverkehr warnt man den Kunden.

Im Auslieferungszustand ist die Firewall aber deaktiviert, der Kunde muss sie erst einmal explizit einschalten. Damit überlasse man den Anwendern die freie Entscheidung, erklärt Kosata, ob sie den Datenverkehr analysiert haben möchten 3. Darüber hinaus nutze die CZ.NIC die gesammelten Daten auch ausschließlich zur Analyse des Verkehrs, man unterliege dabei sehr strengen Regeln zum Datenschutz.

Zu den weiteren Sicherheitsmaßnahmen gehört die automatische Update-Funktion. Direkt bei der Einrichtung fragt der Router nach, ob Sie die Funktion nutzen wollen. Mögen Sie die Software lieber „gut abgehangen", können Sie auf den Auto-Updater auch verzichten. Angesichts der jüngsten IT-Sicherheitsvorfälle empfiehlt sich das aber nur bedingt.

Für durchdachte Sicherheit beim Turris Omnia spricht auch, dass beispielsweise ab Werk keine Ports in Richtung Internet offenstehen. Komfortfunktionen wie UPnP sind deaktiviert, das WLAN aktivieren Sie erst im Rahmen der Ersteinrichtung. Auch alle Zugangsdaten müssen Sie während der geführten Inbetriebnahme selbst setzen.

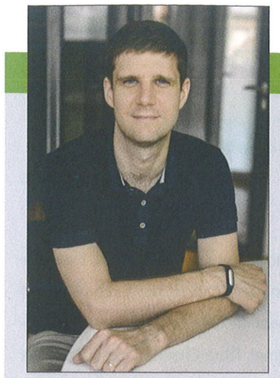
Simpel oder komplex?

Die Installation des Turris Omnia lässt sich schnell abhaken. Zunächst versorgen Sie das Gerät mit Strom und verbinden dann die WAN-Schnittstelle per Kabel mit einem Modem. Außerdem schließen Sie für die Ersteinrichtung einen eigenen Rechner ebenfalls per Netzwerkkabel an einen der fünf Ethernet-Ports des Routers an. Rufen Sie anschließend am Rechner das Webinterface des Rou-

4 Vorsicht bei der Kanaleinstellung fürs WLAN: Wählen Sie eine Frequenz oberhalb von Kanal 128, liegen Sie sowohl technisch als auch juristisch daneben.

SFP: Small Form-factor Pluggable. Eine Spezifikation für modulare, hot-swap-fähige optische oder elektrische Transceiver für Gigabit-Ethernet, Fibre Channel und SONET. Die Originalspezifikation sieht 5 Gbit/s Datenrate vor, inzwischen gibt es SFP+ mit bis zu 10 Gbit/s.

UPnP: Universal Plug and Play. Ursprünglich von Microsoft entwickelter Standard zur Geräteansteuerung in IP-basierten Netzwerken. Heute spezifiziert das UPnP-Forum herstellerübergreifend den Standard und zertifiziert entsprechende Geräte.



Bedřich Kosata
Entwicklungsleiter CZ.NIC

Interview: Bedřich Kosata, Entwicklungsleiter des Turris Omnia

Der Turris Omnia ist nicht das erste Hardware-Projekt der tschechischen CZ.NIC. Welche Aspekte im Vordergrund der Entwicklung des besonders sicheren Routers standen, erklärte Turris-Omnia-Entwicklungsleiter Bedřich Kosata im Gespräch mit LU-Autor Jan Rähm am Rande des OpenWRT-Summits in Berlin.

LinuxUser: *Als Domain-Registrar kümmert sich die CZ.NIC um die gleichnamige Top-Level-Domain der Tschechischen Republik. Wie kam das Unternehmen denn dazu, daneben auch noch Netzwerkgeräte für Endanwender zu entwickeln?*

Bedřich Kosata: Wir sind ein Non-Profit-Unternehmen und wollen Gewinne mit der CZ-Domain für das Wohl der Öffentlichkeit einsetzen. Deswegen stehen bei uns Open Source und IT-Sicherheit im Fokus. So dachten wir uns, es wäre sehr aufschlussreich zu sehen, welcher Verkehr zwischen dem Internet und den Heimnetzwerken abläuft und wer versucht, auf welche Weise Heimnetzwerke anzugreifen. Daraus entwickelte sich dann die Idee zum Turris-Projekt: Wir gaben den Leuten spezielle Router, um eben diesen Datenverkehr zu beobachten und zu sehen, ob wir Anomalien, Schadsoftware oder Ähnliches identifizieren können.

LU: *Seit wann gibt es das Projekt Turris?*

BK: Die Idee hatten wir Ende 2012, 2013 starteten wir mit dem Projekt. Anfangs wollten wir gar keine eigene Hardware herstellen, fanden aber keine Produkte, die unseren Ansprüchen genügten. Da mussten wir wohl oder übel die Hardware selbst von der Pike auf entwickeln. 2014 lieferten wir die ersten zwei Router-Modelle kostenlos aus, im Tausch gegen die Daten der Benutzer. Wer mitmachen wollte, unterschrieb einen Vertrag für drei Jahre. Im Gegenzug haben wir die Boxen gewartet und Updates bereitgestellt, aber eben auch Daten zum Analysieren gesammelt.

LU: *Nun ist der Turris Omnia fertig – der dritte Router der CZ.NIC und der erste, der per Crowd-Funding finanziert wurde. Wie haben Sie es geschafft, das Gerät völlig quelloffen zu gestalten?*

BK: Wir suchten alle Chips so aus, dass der Mainline-Kernel sie unterstützt, auch alle Treiber mussten quelloffen vorliegen. Die einzige Ausnahme stellt der WLAN-Treiber dar: Einen komplett freien Treiber werden Sie da nicht finden; es gibt immer eine binäre Firmware, die nicht offenliegt.

LU: *Wie sieht es mit dem Sicherheitskonzept aus?*

BK: Das beginnt schon beim Basis-Setup. Zu den größten Sicherheitsproblemen im Internet zählen ja bekanntlich voreingestellte Passwörter. Deswegen zwingen wir den Anwender dazu, schon während der Einrichtung eigene, ausreichend starke Passwörter zu vergeben. Das macht unseren Router von Anfang an sicherer als andere Geräte. Hinzu kommen regelmäßige Softwareaktualisierungen und solche hochentwickelten Dinge wie die Distributed Firewall.

LU: *Distributed Firewall – was ist das genau?*

BK: Die Firewall sammelt Daten aus verschiedenen Quellen – von den Routern selbst, aber auch aus unserer Firma oder von außen aus dem Internet. Daraus erstellen wir eine IP-Greylist und beobachten die auffälligen Adressen ganz besonders. Verbindet sich ein Router zu einer davon und entdecken wir dabei auffällige oder schädliche Aktivitäten, dann warnen wir unsere Anwender.

LU: *Das ist nicht jedermanns Sache – zerstören Sie dabei nicht die Privatsphäre?*

BK: In der Vorgabe ist die Distributed Firewall ja nicht aktiv, der Nutzer muss sie explizit einschalten. Uns interessieren auch nicht die privaten Daten, sondern insbesondere die Protokolle der lokalen Firewall: So sehen wir, wer versucht, sich von außen am Router anzumelden, und welche Dienste besonders attackiert werden. Was auf dem eigenen Router vor sich geht, kann sich der Anwender in einem speziellen Portal ansehen, das auch zeigt, welche Datenmengen zwischen Router und Internet hin und her wandern.

Wir sammeln nur Daten, die wir wirklich brauchen, insbesondere Metadaten – wer spricht mit wem im Netz. Die Inhalte interessieren uns nicht. Unsere Analytiker sehen nur anonymisierte Datensätze, zudem vernichten wir nach 10 Tagen alle Einzeldaten und verfügen dann nur noch über aggregierte Verkehrsdaten. Das ist auch Teil unserer Datenschutzerklärung, der die Anwender zustimmen müssen.

LU: *Gibt es neben der Distributed Firewall und der lokalen Absicherung der Router weitere Sicherheitsmaßnahmen?*

BK: Wir haben zusätzlich Honeypots in Form virtueller Router und Server aufgesetzt, um festzustellen, wie Angreifer bei Eindringversuchen agieren. Da gibt es etwa einen Honeypot für Telnet und einen für SSH. Beim Telnet-Zugang präsentieren wir dem Angreifer nur einen Login, in den er dann immer wieder Username und Passwort eingibt, bis er genervt aufgibt. Das versorgt uns aber mit interessanten Daten speziell über Botnetze. Der SSH-Honeypot präsentiert dem Angreifer ein System, in das er vorgeblich eindringen kann. So sehen wir, welche Schadsoftware er zu installieren versucht, und analysieren sie. Die Honeypots laufen isoliert von den Routern der Anwender, sodass diese nicht kompromittiert werden können.

LU: *Seit einiger Zeit haben quelloffene Router ja das Problem der Zulassung: Vor allem die US-amerikanische FCC, aber auch die EU schreiben eine gewisse Abschottung der Funkschnittstellen vor.* Wie gehen Sie damit um?

BK: Das ist ein echtes Problem. Wir stecken mitten in der FCC-Zertifizierung, was uns ziemlich bremst. Wir wollten den Router ja so offen wie möglich gestalten, jetzt müssen wir einen Teil der Hardware abschotten. Zurzeit versuchen wir mit dem Hersteller der WiFi-Karten eine gute Lösung für alle Seiten zu finden. Letztlich werden wir für den US-Markt aber wohl eine eigene, mit einem Lockdown versehene Version anbieten müssen, um die FCC-Zertifizierung zu bekommen.

LU: *Vielen Dank für das Gespräch, Herr Kosata.*

ters auf, landen Sie auf der Startseite des simplen, aber effektiv gestalteten Einrichtungsdialogs. Er führt Sie in zehn Schritten durch die Inbetriebnahme.

Dabei setzen Sie unter anderem auch alle Zugangsdaten und nehmen das WLAN gut abgesichert in Betrieb. Allerdings haben sich die Entwickler hier einen kleinen Schnitzer genehmigt: Der Turris Omnia zeigt auch die hierzulande nicht für den WLAN-Betrieb im 5-GHz-Netz zugelassenen WLAN-Channels oberhalb von Kanal 128 an 4. Wählen Sie versehentlich einen davon aus, dann finden regulationskonform arbeitende Endgeräte das drahtlose Netz nicht, zudem begehen Sie einen Gesetzesverstoß.

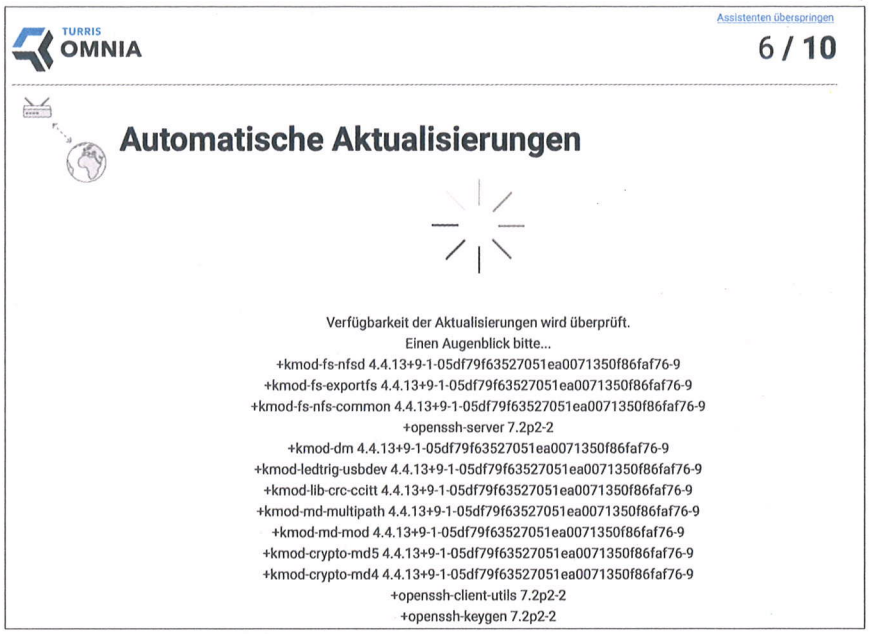
Die gesamte Einrichtung geht in wenigen Minuten über die Bühne. Muss die Software viele Updates laden 5, dauert es je nach Bandbreite des Internetanschlusses eventuell ein wenig länger. Anschließend gelangen Sie in das einfache Webinterface des Turris Omnia, wo Sie nur rudimentäre Einstellungen vornehmen können. Diese genügen zwar für den allgemeinen Betrieb, lassen jedoch wichtige Funktionen wie Netzspeicher (NAS) aus. Alle Optionen sind gut und verständlich beschrieben, trotz kleinerer Schwächen in der deutschen Lokalisierung.

Im erweiterten Bereich sieht das schon ganz anders aus: Ungeachtet der optisch ansprechenden Gestaltung und guten Gliederung verlangen die hier gebotenen Optionen tiefergehendes Fachwissen. Hier bietet sich die Möglichkeit, so gut wie jeden Aspekt des Routers und der Software zu beeinflussen – weit über das Maß dessen hinaus, was selbst ein anspruchsvoller Heimanwender oder kleinere Büros benötigen 6.

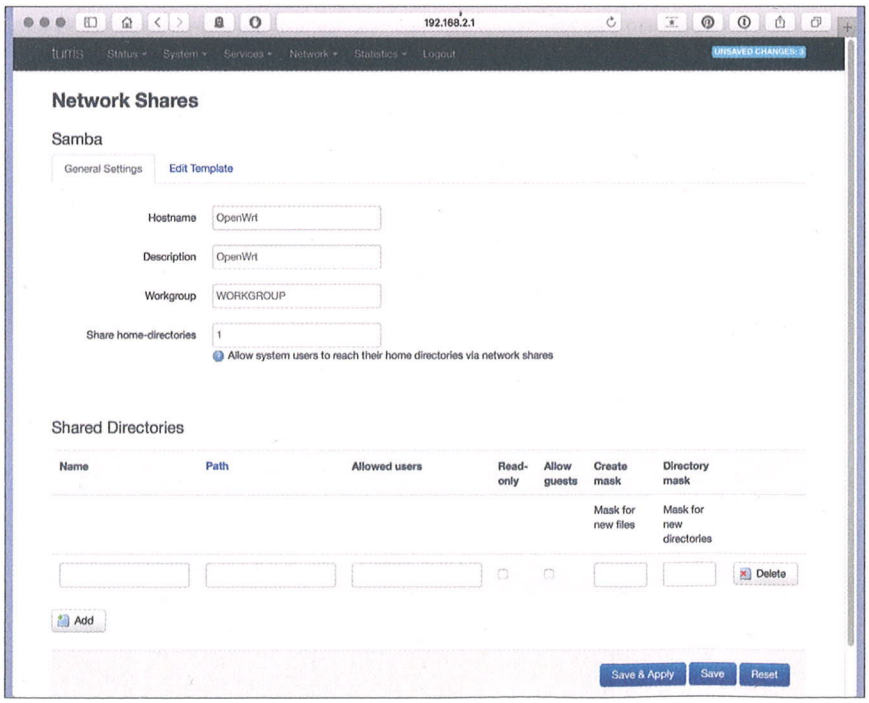
Licht und Schatten

Im Test in einem Büro in der Innenstadt von Berlin erreichten wir mit dem Turris

Omnia regelmäßig WLAN-Datenraten von über 800 Mbit/s netto. Das entspricht fast exakt der maximal möglichen Bruttodatenrate von 1,3 Gbit/s, die 802.11ac theoretisch erlaubt. Kein anderer ac-Router, den wir zum Vergleich in Betrieb nahmen, erzielte höhere Datendurchsätze.



5 **Vorbildlich: Bereits während der Ersteinrichtung bietet der Turris Omnia das Aktualisieren aller Softwarekomponenten an.**



6 **Vorwissen gefragt: Die erweiterte Weboberfläche des Turris Omnia verlangt wie hier bei der Freigabe von Netzwerk-Laufwerken profundes Linux-Wissen vom Anwender.**

Damit ordnet sich der Turris Omnia in Sachen WLAN-Performance in der absoluten Spitzengruppe ein und muss sich vor keinem Konkurrenten verstecken.

Der Turris Omnia hat allerdings auch Schattenseiten, vor allem beim Preis/Leistungsverhältnis. Mit Anschaffungskosten von 289 respektive 329 Euro positioniert sich der Router zwar preislich im oberen Mittelfeld, lässt dabei aber Schnittstellen für analoge oder ISDN-Telefone vermissen. Dafür muss man noch einmal zusätzlich in die Tasche greifen. Auch der Software fehlen Telefoniefunktionen, die sich mit etwas Hintergrundwissen aber eventuell nachrüsten ließen.

Dass dieser Teil der Kommunikationsschnittstellen sowohl hard- als auch softwareseitig fehlt, dürfte vor allem jenen potenziellen Anwendern übel aufstoßen, die bereits einen All-IP-Anschluss mit integrierter Telefonie nutzen.

Fazit

Beim Turris Omnia handelt es sich um ein exzellentes Stück Hardware. Sowohl die Verarbeitung als auch das zugrundeliegende, offene Konzept bieten keine Angriffspunkte für Kritik. Gerade dadurch stechen aber die fehlenden Telefoniefunktionen besonders ins Auge. Die Update-Funktion macht einen guten Eindruck – angesichts der Organisation hinter dem Turris-Omnia-Projekt darf der Anwender auch auf eine lange Zeit des Supports hoffen.

Die verteilte Firewall muss im Langzeittest zeigen, was sie kann. Wer sich bei dem Gedanken nicht wohlfühlt, dass Dritte seine Daten analysieren, muss diese Option nicht aktivieren und kann der integrierten Firewall vertrauen: Sie lässt sich, entsprechendes Wissen vorausgesetzt, sehr fein konfigurieren. Es fehlt jedoch eine klare und trotzdem halbwegs umfangreiche Konfigurationsoberfläche für Nicht-Linux-Experten. (jlu) ■

Weitere Infos und interessante Links
www.linux-user.de/qr/38163