

Turris Omnia: Open-Source-Router mit Virtualisierung

Unter dem Namen Turris entwickelt der gemeinnützige Verein cz.nic einen Open-Source-WLAN-Router auf OpenWRT-Basis (www.turris.cz). cz.nic ist hauptamtlich der Verwalter der tschechischen nationalen Internet-Domain .cz und stark im Projekt DNSSEC zur kryptographischen Absicherung der Namensauflösung engagiert.

Das Projekt legt seinen Schwerpunkt auf Netzwerksicherheit, wozu cz.nic eine adaptive verteilte Firewall entwickelt hat. Sie überwacht den Datenverkehr auf jedem Router und meldet Anomalien an einen zentralen Server. Der analysiert die Daten und generiert neue Firewall-Regeln gegen schädlichen Verkehr, die dann per automatischem Update auf die Router zurückfließen. Dabei gehen auch Informationen von dritter Seite ein, unter anderem vom csirt.cz, dem tschechischen Computer Security Incident Response Team.

Welche Daten erhoben werden, soll jeder Turris-Nutzer über sein persönliches Konto online



Der WLAN-Router Turris Omnia soll dank adaptiver Firewall Angriffe effizient unterbinden.

nachschlagen können. Das sei – neben der Warnung vor konkreten Angriffen – die einzige Stelle, an der die Verkehrsdaten mit dem Nutzer korreliert würden. Ferner steht der Quelltext der Router-Firmware zur Einsicht bereit. So will cz.nic Befürchtungen wegen Verletzungen der Privatsphäre kontern.

Als Unterbau hat cz.nic einen eigenen WLAN-Router entwickelt, der im Endausbau mit einem 1,6 GHz schnellen Dual-Core-ARM-Prozessor (Marvell

Armada 385), 1 GByte RAM und 4 GByte Flash-Speicher läuft. Die restliche Hardware ist der Basis angemessen: 6 Gigabit-Ethernet-Ports, SFP-Slot für Glasfaser-Module (FTTH/FTTP), schnelles Simultan-Dualband-WLAN (IEEE 802.11n-300, 11ac-1300, optional), 2 USB-3.0-Ports, 2 Mini-PCI-Express-Slots, ein optionaler mSATA-Slot. So soll man Turris auch – wie bei anderen WLAN- Routern üblich – als NAS-Ersatz, Print- oder DLNA-Medienserver einsetzen kön-

nen. Neu: Per Virtualisierungsserver laufen eigene Software-Projekte direkt auf dem Router, ohne die Kernfunktion zu gefährden.

Aus den Prototypen soll nun per Crowdsourcing das Serienprodukt Turris Omnia werden. Binnen 24 Stunden nach Veröffentlichung auf der Plattform Indiegogo hat das Projekt sein gestecktes Ziel von 100 000 US-Dollar erreicht. Bei Redaktionsschluss stand die Marke über 200 000 Dollar, womit die Entwickler auch eine App für Mobilgeräte zum Fernsteuern des Routers programmieren werden. Bei Erscheinen dieser c't dürfte die Schwelle für Unterstützung einer Raspi-artigen I/O-Schnittstelle erreicht sein, womit Raspi-Anwendungen auch auf dem Router laufen und externe Hardware steuern können. Der Turris Omnia soll im April 2016 ausgeliefert werden und je nach Ausbau ab 100 US-Dollar zu haben sein. (ea@ct.de)

ct Turris Omnia bei Indiegogo: ct.de/y2cu

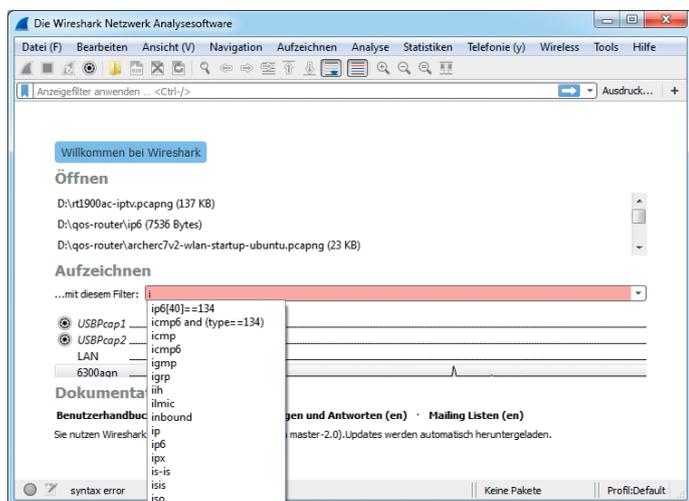
Netzwerk-Analysetool Wireshark springt auf Version 2

Das zur Fehler- und Protokollanalyse in Netzwerken beliebte Tool Wireshark ist Mitte November in Version 2.0.0 erschienen (siehe c't-Link). Zu ihren wichtigsten Neuerungen gehören die komplett neue Bedienoberfläche, ins Menü einbindbare Plug-

ins, ein optimierter VoIP-Player, eine WLAN-Werkzeugleiste sowie Verbesserungen bei Graphen (IO, Laufzeit, Fensterskalierung) und im SSL-Dissektor. Die Liste der neu unterstützten Protokolle von „Aeron“ bis „ZVT Kasenschnittstelle“ in den Release

Notes (siehe Link) füllt fast eine Browser-Seite.

Beim Installieren unter Windows wandert nicht nur wie bisher der Netzwerk-Paketfänger WinPCAP auf die Platte, sondern auf Wunsch auch die USB-Variante USBPcap, sodass man Problemen mit USB-Geräten auf die Spur kommen kann. Bei den Capture- und Anzeigefiltern gibt Wireshark endlich interaktive Hilfestellung: Es bietet nach dem ersten Zeichen die möglichen Protokollkürzel nebst History an und ergänzt den Filterbegriff, wo nötig, auch um Beispiele für korrekt formatierte Parameter. Bei Redaktionsschluss funktionierte das nur unter Windows und MacOS X: Die GTK-Oberfläche der Linux-Version 2.0.0 half nur beim Anzeigefilter, die Qt-Oberfläche stand bei Opensuse 13.x nur für das ältere Wireshark 1.12 zur Verfügung. Bei Ubuntu gab es Wireshark nur in der älteren Version. (ea@ct.de)



Beim Erstellen von Filtern gibt Wireshark endlich Hilfestellung: Es blendet die korrekten Kürzel für bekannte Protokolle nebst History ein, optional ergänzt um Parameterbeispiele.

ct Wireshark 2.0.0 für Windows und OS X: ct.de/y2cu

Netz-Notizen

AVM hat für drei Fritzbox-Modelle ein Firmware-Update herausgebracht, das **IPv6-Unterstützung auf LTE nach 3GPP Rel. 8** bringt. Die Version 6.30 steht für die Fritzboxen 6810 LTE, 6840 LTE und 6842 LTE zur Verfügung.

Trendnet erweitert sein Produktangebot um **drei SFP+-Module für 10 GBit/s**. Sie sind alle für LC-Faserstecker, aber unterschiedliche Distanzen vorgesehen: TEG-10GBS40 (40 km, Single Mode, 1629 Euro), TEG-10GBS10 (10 km, Single Mode, 279 Euro) und TEG-10GBSR (550 m, Multi-Mode, 179 Euro).

nmap 7.00 bringt unter anderem 171 neue NSE-Skripte, verbesserte IPv6-Unterstützung und SSL/TLS-Analyse mit (siehe Link).

ct Netzwerk-Scanner nmap: ct.de/y2cu