05/2011 Deutschland € 14,90 Österreich € 16,40 Schweiz SFR 29,80
www.TecChannel.de

IDG

TECCHANNEL COMPACT

IT EXPERTS INSIDE

★ LAN ★ WLAN ★ Breitband

NETZWERK

Sicherheit

- Sichere WLAN-Konfiguration
- Netzwerkzugriffsschutz (NAP) mit Windows
- Netzwerkschutz mit Linux

Ratgeber

- Alles was Sie über IPv6 wissen müssen
- VDSL, Glasfaser, LTE und Co. im Vergleich

Praxis

- Windows 7 als Hotspot
- Tipps: WLAN einfacher und schneller
- RADIUS- & IMAP-Server einrichten

Netzwerk-Tools für Admins

TEC CHANNEL
SILBER-PAKET

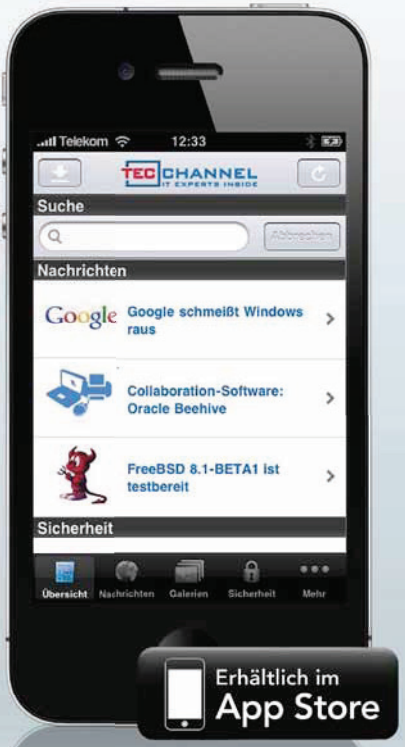
Die neue TecChannel App

Alles drin. Immer dabei. Jetzt fürs iPhone.

News, Infos, Tipps & Tricks für unterwegs!

- topaktuelle News
- Hintergründe
- Analysen
- Tests und Bilderstrecken

» Gratis laden



Vorraussetzungen: Kompatibel mit iPhone, iPod touch und iPad. Erfordert iOS 3.0 oder neuer.

www.tecchannel.de/iphoneapp

Einfach QR-Code mit dem Codereader Ihres iPhones einscannen.Sie werden direkt in den App-Store verlinkt und können die App downloaden. Einen kostenlosen Reader erhalten Sie z.B. unter http://get.beetagg.com/. Es entstehen lediglich Kosten für die Verbindung ins (mobile) Internet.

IDG BUSINESS MEDIA GMBH

Editorial

Nahtstellen

Es ist ja nicht gerade so, dass Netzwerkadministratoren mit der täglichen Hege und Pflege des ihnen anvertrauten Netzwerks nicht ausgelastet wären. Allein das Thema Netzwerksicherheit nimmt mittlerweile eine gehörige Portion der Ressourcen ein. Da bedarf es eigentlich keiner weiteren Herausforderung(en).

Die stehen aber, wie so häufig in der IT, mal wieder Schlange. Allen voran die Einführung von IPv6, vor der sich viele Unternehmen noch gekonnt wegducken. In der Berichterstattung über das neue Protokoll ist von Euphorie bis Panikmache alles zu finden. Mit ein wenig mehr Gelassenheit dürfte sich aber auch diese Problematik lösen lassen. Im Großversuch hat das Protokoll am World IPv6 Day Anfang Juni 2011 seine erste Bewährungsprobe durchaus bestanden.

Beim ersten weltweiten Feldtest zu IPv6 waren viele große Webseiten auch über IPv6 abrufbar. Und siehe da, das Internet ist nicht implodiert, zwar gibt es noch eine Reihe Detailprobleme, aber prinzipiell war der Test erfolgreich. Und zwar so erfolgreich, dass einige Betreiber wohl überlegen, es gleich beim Doppelbetrieb von IPv4 und IPv6 zu belassen. Gewiss, nicht alle Herausforderungen an die Netzwerk-IT haben das Kaliber einer derartigen Protokolleinführung, viele sind aber nicht minder spannend. Und manchmal ist eine neue Aufgabe ja in dem Fall interessanter als ausschließlich Routine.

In diesem Compact haben wir jede Menge Praxisartikel zusammengestellt, die Sie bei gewohnten und neuen Pflichten unterstützend begleiten wollen.

Malte Jacobs

Impressum

Chefredakteur: Michael Eckert (verantwortlich, Anschrift der Redaktion)
Redaktion TecChannel:
Lyonel-Feininger-Straße 26, 80807 München,
Tel.: 0 89/3 60 86-897
Homepage: www.TecChannel.de,
E-Mail: feedback@TecChannel.de
Autoren dieser Ausgabe werden bei den Fachbeiträgen genannt
Verlagsleitung: Michael Beilfuß

Grafik und Layout:
stroemung GmbH (Michael Oliver Rupp, Oliver Eismann), Multimedia Schmiede, Twentyfirst Communications (Bernd Maier-Leppla)
Titel: Clemens Strimmer, Foto: Hersteller
Anzeigen: Anzeigenleitung: Sebastian Woerle
Tel.: 0 89/3 60 86-628
Ad-Management: Edmund Heider (Ltg.) (-127)
Anzeigenannahme: Martin Behringer (-554)
Druck: Sachsendruck GmbH, Paul-Schneider-Strasse 12, 08525 Plauen

Gesamtvertriebsleitung IDG Deutschland: Josef Kreitmair
Produktion: Jutta Eckebrecht (Ltg.)
Bezugspreise je Exemplar im Abonnement:
Inland: 12,30 Euro, Studenten: 10,95 Euro,
Ausland: 13,05 Euro, Studenten: 11,70 Euro
Haftung:
Eine Haftung für die Richtigkeit der Beiträge können Redaktion und Verlag trotz sorgfältiger Prüfung nicht übernehmen. Veröffentlichungen in TecChannel-Compact erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt. Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: Alleiniger Gesellschafter der IDG Business Media GmbH ist die IDG Communications Media AG, München, eine 100-prozentige Tochter der IDG Inc., Boston, Mass., USA.
Verlag:
IDG Business Media GmbH
Lyonel-Feininger-Straße 26
80807 München
Tel.: 0 89/3 60 86-0, Fax: -118
Homepage: www.idg.de
Handelsregisternummer: HR 99187
Umsatzidentifikationsnummer: DE 811257800
Geschäftsführer: York von Heimburg
Mitglied der Geschäftsführung: Michael Beilfuß
Vorstand: York von Heimburg, Keith Arnot, Bob Carrigan
Aufsichtsratsvorsitzender: Patrick J. McGovern

TecChannel ist Mitglied der IDG Business Media GmbH und somit ein Teil der IDG-Verlagsgruppe. Darin erscheinen unter anderem auch folgende Zeitschriften:

IDG COMMUNICATIONS MEDIA AG

PC WELT · Macwelt · ChannelPartner · GameStar · CIO · COMPUTERWOCHE · DigitalWorld · GamePro

Abonnement, Einzel- und Nachbestellung, Umtausch defekter Datenträger:
TecChannel Kundenservice, Postfach 81 05 80, 70522 Stuttgart, Tel: (+49) 07 11/72 52-276, Fax: -377, für Österreich 1/21 95 560, für Schweiz, 0 71/3 14 06-15, E-Mail: shop@TecChannel de

Inhalt

1 Grundlagen

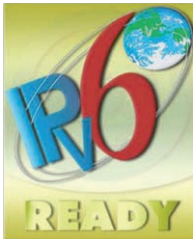
Netzwerke bilden in Unternehmen jeder Größe die Basis der IT-Infrastruktur. Doch die Innovationszyklen moderner Netzwerkkomponenten schrumpfen – umso wichtiger ist das Wissen um neue Verfahren und Lösungen. Dieses Kapitel informiert Administratoren und Entscheidungsträger über IPv6, Zugangstechniken, professionelle DSL-Router, internetbasierte Fax-Systeme und Smart Grids.

1.1 Ratgeber – Alles was Sie über IPv6 wissen sollten

Es ist die Basis des Internets, ohne es gäbe es kein Google, kein Facebook, keine Videokonferenzen, keinen E-Mail-Verkehr – das Internet Protocol in der Version 4, kurz IPv4. Doch der Jubilar, der 2011 sein 30-jähriges Bestehen feiert (1981 im RFC 791 definiert), droht, Opfer seines eigenen Erfolgs zu werden.

In einer Zeit, in der immer mehr Handys online gehen, Stromzähler im Zuge der Smart Grids vernetzt werden oder das intelligente Haus langsam Realität wird, gehen IPv4 die Adressen aus, um diese Devices und Rechner im Netz erreichbar zu machen. Ähnlich wie Hausnummern und Postleitzahlen ermöglichen es die mehr als vier Milliarden IP-Adressen, dass die Geräte im globalen Netz eindeutig angesprochen werden können. Abhilfe könnte das neue Internetprotokoll in der Version 6, IPv6, schaffen, denn es umfasst rund 340 Sextillionen (2 hoch 128) Adressen, womit sich nun wirklich jede Kaffeemaschine, wenn nicht gar jedes Sandkorn rund um den Globus, mit einer Adresse ausstatten lassen sollte. Neu ist IPv6 in Wirklichkeit nicht, es hat bereits 15 Jahre auf dem Buckel, reift aber erst jetzt zur Praxistauglichkeit heran.

Achtung: Sind Sie schon IPv6-ready?



Der letzte IPv4-Adressblock (www.potaroo.net/tools/ipv4), so der Stand während der Recherchen zu diesem Artikel, ist laut der für die globale Vergabe zuständigen Internet Assigned Numbers Authority (IANA, www.iana.org) bereits an die regionalen Registrierungsorganisationen (für Europa ist RIPE zuständig) vergeben.

RIPE verteilt den Rest in den nächsten Tagen beziehungsweise Wochen. Danach ist Schluss, zusammenhängende öffentliche Adressblöcke wird es dann nicht mehr geben. „Wer bis dahin nicht auf das neue IPv6-Protokoll umgestellt hat, steht möglicherweise im Regen", warnt Michael Rotert, Vorstandsvorsitzender bei eco, dem Verband der deutschen Internetwirtschaft.

Welche Konsequenzen die Adressknappheit schon jetzt hat, erzählte uns ein Praktiker: Im Kundenauftrag sollte er für eine geplante Unternehmensexpansion an mehreren Standorten einen zusammenhängenden IP-Adressblock reservieren. Er bekam aber keinen mehr. Jetzt muss das Unternehmen mit gesplitteten Adressräumen leben, was Routing und Netzmanagement nicht unbedingt vereinfacht und damit höhere Kosten verursacht.

1.1.1 Alles nur Panikmache?

Werden die Adressen wirklich knapp, oder ist alles nur Panikmache? Gegner des neuen Internet Protocol v6 verweisen in diesem Zusammenhang gerne darauf, dass das Problem der Adressknappheit doch bereits hervorragend mit NAT gelöst sei. Bei der Network Adress Translation werden innerhalb eines Unternehmensnetzes private IP-Adressen verwendet, die jedoch im öffentlichen Internet – vereinfacht ausgedrückt – nicht sichtbar sein dürfen.

Deshalb werden die internen Adressen am Übergang zum Internet in eine offizielle IPv4-Adresse übersetzt. Das Unternehmen benötigt so nur eine einzige, offiziell registrierte IP-Adresse. Zudem führen IPv6-Skeptiker gerne das Argument an, dass IPv6-Adressen im Internet bisher kaum genutzt würden, sodass die Entscheider in den Unternehmen noch viel Zeit hätten und deshalb abwarteten.

1.1.2 IPv6 hat wenig Charme

Die Zurückhaltung der Unternehmen erklärt Jürgen Zimmermann, Projektleiter IP-Einführung bei der Telekom Deutschland GmbH, unter anderem damit: „Die Einführung von IPv6 über Dual-Stack-Anschlüsse mag für manche Geschäftskunden einen ähnlichen Charme haben wie früher die Umstellung von der vier- auf die fünfstellige Postleitzahl. Wenn jedoch in diesem Jahr die letzten IPv4-Adressen vergeben werden, ist IPv6 die mittel- bis langfristige Voraussetzung dafür, dass die Webangebote aus dem gesamten Internet erreicht werden können." Zudem dürfte in den nächsten Jahren der Bedarf an IP-Adressen drastisch steigen, wenn etwa für die rund 40 Millionen Haushalte in Deutschland die von der EU vorgeschriebene (Strom-)Zählerfernauslesung realisiert werden soll. „Das ist jedenfalls nur über IPv6-Adressen zu realisieren", ist Zimmermann überzeugt. „Zusammen mit der wachsenden Zahl an M2M-Anwendungen (etwa für Hausautomatisierung und Security-Anwendungen) wird ein Haushalt in den nächsten Jahren zwischen 50 und 500 direkt aus dem Netz adressierbare IP-Adressen benötigen."

Gegen dieses Prinzip verstößt IPv4 in Kombination mit NAT, denn die so angeschlossenen Rechner können nicht ohne Weiteres aus dem Internet direkt angesprochen werden – ein Umstand, der bei Protokollen und Services wie FTP, SIP oder IPsec, die auf den oberen Netzschichten aufsetzen, immer wieder zu Problemen führt und mehr oder weniger zuverlässig Workarounds erfordert.

Rechner auf Abwegen: Dieses Notebook suchte im WLAN-Hotspot von alleine nach Kommunikationspartnern, die IPv6 sprechen.

Allerdings sind sich Hersteller, Carrier und Service-Provider in Gesprächen mit der Computerwoche auch einig, dass derzeit in Sachen IPv6-Migration kein Anlass zur Panik besteht. „Noch gibt es die Killerapplikation für IPv6 nicht", führt etwa Alexander Pilger, Senior Consultant bei Controlware, aus. Gleichzeitig warnen die IT-Hersteller aber davor, das Thema ähnlich wie bei der Jahr-2000-Problematik auf die lange Bank zu schieben. Unisono geht man davon aus, dass größere Unternehmen für eine IPv6-Migration mit einem Projektrahmen von 15 bis 18 Monaten rechnen müssen. „Zudem könnte in etwa einem Jahr, wenn der Schuh zu drücken beginnt", so gibt Pilger zu bedenken, „qualifiziertes IPv6-Beratungs-Know-how ein knappes Gut werden." Deshalb raten eigentlich alle Befragten, sich bereits heute vorzubereiten, um für den Tag x gewappnet zu sein.

1.1.3 Migrations-Checkliste

Steffen Jansen, Trainer und Consultant bei Fastlane, hat in Sachen Migrationsnotwendigkeit eine einfache Checkliste parat: Demnach sollte sich mit einer Migration auf IPv6 beschäftigen, wer zwei der folgenden drei Kriterien innerhalb der nächsten drei Jahre für sein Unternehmensnetz nicht sicher ausschließen kann:

- weltweite Vernetzung mit Business-Partnern und eigenen Standorten insbesondere im asiatischen Raum,
- höherer Stellenwert von Peer-to-Peer-Anwendungen und
- Compliance-Zwänge.

Auch Axel Föry, bei Cisco im Rahmen des Borderless Networking für IPv6 zuständig, rät Unternehmen, nicht einfach zu migrieren, sondern sich die Frage zu stellen, was es für ihr Business bedeuten kann, wenn sie nicht IPv6-bereit sind. Föry zufolge steht zumindest in den großen deutschen Unternehmen 2011 die IPv6-Technik auf der Agenda, „und es kann für Partner, Zulieferer oder Kunden teuer werden, wenn sie nicht vorbereitet sind und plötzlich in ihren Geschäftsbeziehungen per IPv6 kommunizieren müssen".

Deshalb sollten Unternehmen jetzt die Chance ergreifen, ohne hohen Zeit- und Kostendruck einen IPv6-Masterplan zu erstellen, um dann im Bedarfsfall schnell umstellen zu können. Die alte Ausrede „Warum sich mit IPv6 befassen, es wird im Netz ohnehin nicht genutzt" zählt im Jahr 2011 nicht mehr. So hatte beispielsweise die Internet Society den 8. Juni 2011 zum „World IPv6 Day" deklariert (http://isoc.org/wp/worldipv6day/). An diesem Tag wurden unter anderem die Interoperabilität der unterschiedlichen IPv6-Implementierungen getestet. Mit von der Partie waren Internetschwergewichte wie Google, Facebook, Akamai oder Yahoo.

Hierzulande haben quer durch die Bank eigentlich alle deutschen Provider IPv6-Pläne in der Schublade. „Im Sommer 2011 beginnt voraussichtlich die Umstellung für die Content-Angebote der Telekom wie Music-, Video- oder Software-Load und das T-Online-Portal", kündigt IP-Projektleiter Zimmermann an.

1.1.4 Carrier rüsten für IPv6

Darüber hinaus sind bei der Telekom auch andere IP-basierte Dienste wie DSL/VDSL-Anschlüsse für Privatkunden oder hochwertige Anschlüsse mit fester IP-Adresse (CompanyConnect) für Geschäftskunden als IPv6-Varianten geplant.

Ähnlich sieht die Situation bei anderen aus: So munkelt man in der Branche, dass auch Kabel Deutschland im Jahresverlauf wohl IPv6-Internetzugänge offerieren werde. Und auch 1&1 gibt an, dass der Konzern intern bereits „IPv6-ready" sei und theoretisch jederzeit umstellen könne. Ähnlich äußert sich Dennis Knake, der Sprecher von QSC. Das eigene Netzwerk sei bereits IPv6-fähig, ein Rollout werde wohl im Verlauf des Jahres 2011 stattfinden. Grund für die Verzögerung seien derzeit noch fehlende Endgeräte.

1.1.5 Hersteller stellen Produkte um

Das ist ein Mangel, doch der dürfte bereits bald der Vergangenheit angehören. Vergangenes Jahr preschte etwa AVM vor und kündigte für etliche seiner populären

Fritzboxen ein IPv6-Update an. Auch bei D-Link glaubt man, dass IPv6 im Jahr 2011 bei den Carriern im Edge-Bereich an Bedeutung gewinnt und etliche Anbieter selbst im Consumer-Sektor auf das neue Protokoll umstellen. Deshalb liefert das Unternehmen künftig nur noch IPv6-fähige Endgeräte aus. Ältere, für den Enterprise-Bereich konzipierte Geräte, so D-Link-Manager Mike Lange, seien schon seit Längerem von Haus aus IPv6-bereit oder Upgrade-fähig.

IP-Konverter: Der SX 2600CV von Silex bindet Altgeräte in IPv6 ein.

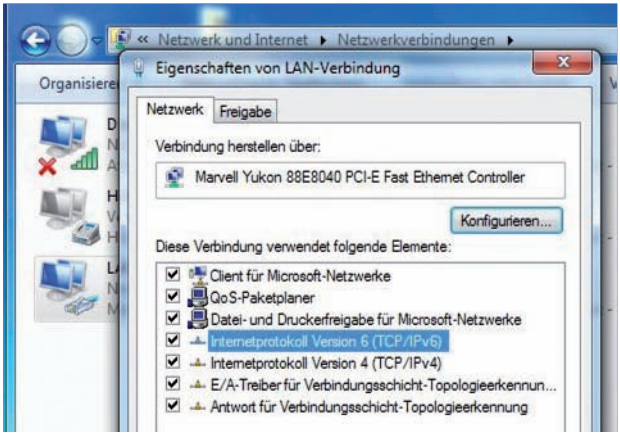
Anders sieht es jedoch bei den meisten Consumer-Geräten aus. Da hier meist Prozessorleistung und Arbeitsspeicher nicht ausreichen, wird der Anwender um eine Neuanschaffung nicht herumkommen. Ähnlich beschreibt man die Situation beim Wettbewerber Netgear.

Dagegen ist IPv6 bei den Herstellern von Enterprise-Equipment kein Thema. „Wo es möglich ist, wird es auch für alte Geräte ein Upgrade geben", bringt etwa Cisco-Manager Föry die Haltung seines Hauses auf den Punkt.

1.1.6 IPv6-bereit in Theorie und Praxis

Jedoch warnt Controlware-Consultant Pilger davor, blind den Readyness-Versprechen zu vertrauen. Die IT-Hersteller verstünden hierunter teilweise Unterschiedliches. So seien beispielsweise alle aktuellen Betriebssysteme wie etwa Windows, Apple, Solaris, Linux oder BSD IPv6-fähig. Allerdings unterstütze nicht jedes System alle Features. Deshalb solle der Anwender genau prüfen, inwieweit IPv6 wirklich implementiert ist und was IPv6 für die Performance der Komponenten bedeutet. Ebenso verhält es sich dem Berater zufolge mit der Hardware. Relativ gut bewertet Pilger hier den Umsetzungsstatus bei Netzkomponenten wie Routern, Firewalls oder Intrusion-Detection- und -Prevention-Systemen. Nachholbedarf sieht er noch bei Content-Security-Systemen oder Personal Firewalls. Pilger weist ausdrücklich darauf hin, die Sicherheitsrisiken im IPv6-Umfeld nicht zu unterschätzen: „Die bösen Jungs sind schon IPv6-ready. Es gibt bereits Angriffs-Tools und Viren-Konstruktions-Kits, wo per Knopfdruck zwischen IPv4 und IPv6 ge-

wechselt werden kann.“ Im Gegenzug werden klassische Netzwerk-Scans sehr aufwendig. „Pro Subnetz benötigt ein Angreifer 100 Millionen Pings pro Sekunde, das entspricht bei einem Durchsatz von 40 Gbit/s mehr als 5800 Jahren“, rechnet der Berater vor. Im Umkehrschluss bedeutet dies aber auch, dass sich ein Netz nicht mehr einfach mit Netzwerkscannern auf Sicherheitslücken untersuchen lässt.



Details: Betriebssysteme wie Windows 7 aktivieren bereits automatisch das IPv6 – was ohne Sicherheitsmaßnahmen problematisch ist.

Zusätzliches Angriffspotenzial ergibt sich, wenn Betriebssysteme wie Windows 7 automatisch IPv6 aktivieren, aber im Unternehmen keine Sicherheitsmaßnahmen für IPv6 etabliert sind. Ohne angemessene Vorkehrungen muss der erste Schritt an dieser Stelle die Deaktivierung von IPv6 sein. Pilger zufolge sollte bei der Einführung von IPv6 die zentrale Frage aus Sicht der Informationssicherheit lauten: Wie kann das heute mit IPv4 erreichte Sicherheitsniveau eines Unternehmens auch mit IPv6 gehalten werden?

1.1.7 Diese Veränderungen bringt IPv6 für Unternehmensnetze mit sich

Adressraum: Wartete IPv4 mit seinen 32 Bit langen Adressen noch mit rund 4,3 Milliarden Adressen auf, stehen unter IPv6, das 128-Bit-Adressen verwendet, rund 340 Sextillionen Adressen zur Verfügung. Die für den Benutzer augenfälligste Änderung dabei ist die neue Schreibweise: Die 128-Bit-Adressen werden hexadezimal notiert – etwa so: 2001:0db8:85a3:08d3:1319:8a2e:0370:7344. Eine URL mit IPv6 und Port-Nummer schreibt sich dann wie folgt: http://[2001:0db8:85a3:08d3:1319:8a2e:0370:7344]:8080/. Dabei wird die Adresse in der Regel in zwei Bereiche unterteilt: Die ersten 64 Bit bilden allgemein gesprochen das Präfix, das sich aus der Netzadresse des Providers und des Subnetzes zusammensetzt. Die anderen 64 Bit

werden aus dem Interface Identifier erzeugt, der sich etwa aus der MAC-Adresse einer Netzschnittstelle bilden kann. Um eine gewisse Anonymität wie bei IPv4 zu gewährleisten, werden auch wechselnde Interface Identifier sowie variierende Provider-Präfixe diskutiert.

Besondere Adressen: Wie bei IPv4 existieren unter IPv6 besondere Adressen, etwa Link-lokale Adressen (Link Local Unicast), die nur im gleichen Teilnetz erreichbar sind und von Routern eigentlich nicht weitergeleitet werden sollen.

Unique Local Unicasts definieren im IPv6-Umfeld private IP-Adressen. Allerdings wird derzeit noch über den genauen Aufbau dieser Adressen diskutiert, etwa ob es eine eindeutige Site-ID geben soll.

Ferner existieren **Multicast-Adressen** etwa für Broadcasts oder um alle Router in einem Bereich zu adressieren.

Vereinfachte Header: Unter IPv6 wurde der Aufbau der Header auf eine feste Länge von 40 Bytes festgelegt. Damit soll unter anderem im Vergleich zu IPv4 ein schnelleres Routing erreicht werden.

Autokonfiguration: Hier weisen sich die Geräte unter IPv6 automatisch selbst eine Adresse zu, weshalb das Verfahren auch als „Stateless Address Configuration" bekannt ist. Allerdings kann die Adressvergabe auch via DHCPv6 erfolgen, die sogenannte Stateful Address Configuration. Des Weiteren sind Mischformen zwischen Autokonfiguration und DHCPv6 möglich.

Mobile IP ist eine Erweiterung des Standards und soll es ermöglichen, dass ein Endgerät überall – egal ob im Unternehmen oder im Home Office – unter der gleichen IP-Adresse erreichbar ist.

Multihoming macht es einfacher, ein Netz gleichzeitig von mehreren Providern mit IP-Adressen und Internet-Connectivity zu versorgen. In der Praxis könnten dadurch Unternehmen Netzbetreiber leichter wechseln oder gar dauerhaft mit mehreren Providern gleichzeitig arbeiten und so eventuell durch den verschärften Wettbewerb Kosten sparen.

IPsec ist im Gegensatz zu IPv4 nun keine Option mehr, sondern ein fester Bestandteil des Protokolls.

Bessere Multimedia-Fähigkeit: Im Gegensatz zum Vorgänger gehören nun QoS-Mechanismen von Haus aus zu IPv6. Dabei werden etwa Datenströme (Flows) neu klassifiziert, um den Transport von Audio- und Videodaten zu optimieren. Verbessern sollen sich auch die Flusskontrolle und die Erkennung von Engpässen.

ICMPv6: Eine zentrale Bedeutung für das Funktionieren des Internet Protocols hat das Internet Control Message Protocol. Konnte dieses unter IPv4 noch von der Firewall geblockt werden, ist es nun zwingend erforderlich. Mit ICMPv6 wird auch das Address Resolution Protocol (ARP) der IPv4-Welt abgelöst. Seine Nachfolge tritt das Neighbor Discovery Protocol (NDP) an. Aufgrund seiner zentralen Bedeutung für die Steuerung des Datenverkehrs sollten sich Netzadministratoren gerade unter Sicherheitsaspekten besonders intensiv mit ICMPv6 befassen.

Diese Zusammenstellung kann nur einen ersten Überblick über die Veränderungen im IPv6-Umfeld liefern. Wer tiefer in die Materie einsteigen will, sollte auf den Webseiten der IETF (Internet Engineering Task Force) einen Blick auf die einzelnen RFCs im Tool-Bereich werfen (http://tools.ietf.org/).

1.1.8 Fazit: IPv6 als Chance betrachten

Angesicht des Aufwands und der zu erwartenden Tragweite dürften viele Unternehmen der IPv6-Migration mit Sorge entgegensehen. Bernd Stock, Account Manager bei Controlware, hält das für einen Fehler. IT-Entscheidern erteilt er den Ratschlag, „die IPv6-Migration nicht nur als Bürde zu sehen, sondern auch als Chance zu betrachten". Das neue Internet Protocol biete eine Vielzahl zusätzlicher Möglichkeiten, die es jetzt zu nutzen gelte.

Jürgen Hill

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation Computerwoche.

Jürgen Hill ist Redakteur bei unserer Schwesterzeitschrift Computerwoche und dort für Produkte & Technologien zuständig.

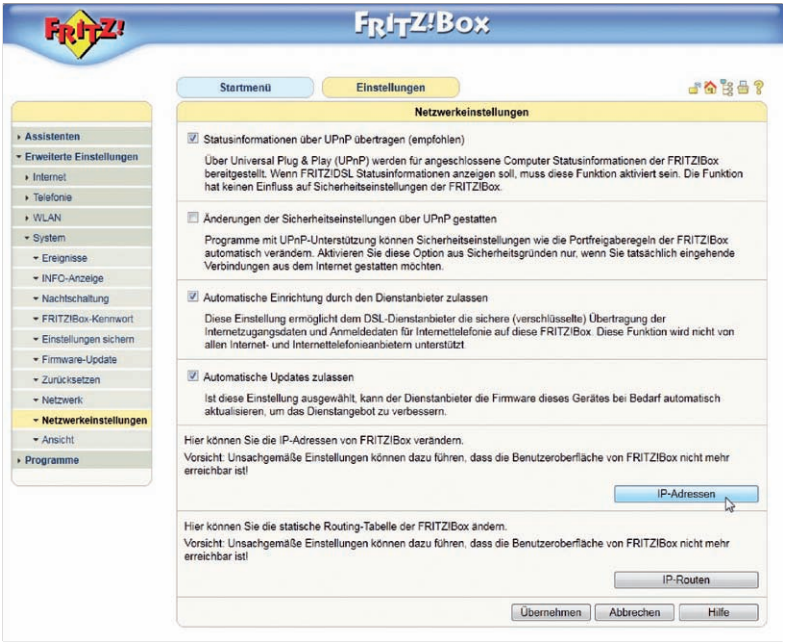
TecChannel-Links zum Thema	Webcode	Compact
Ratgeber – Alles was Sie über IPv6 wissen sollten	2035716	S.9
Ratgeber – Anforderungen an professionelle DSL-Router	2035759	S.17
Breitband für alle – Zugangstechnologien im Überblick	2035913	S.25
Ratgeber – Faxen übers Internet	2035270	S.33
Smart Grids Intelligente Stromnetze der Zukunft	2035308	S.39

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

1.2 Ratgeber – Anforderungen an professionelle DSL-Router

Auch für kleine Unternehmen ist heute ein Internetzugang essentiell. Die zentrale Bedeutung kommt dabei dem Router zu, der die Schnittstelle zwischen Büro und Außenwelt bildet sowie den Datenverkehr zu den Geräten steuert und verwaltet.

Den Zugang zum Internet stellt per Vertrag ein Internet-Provider zur Verfügung. Als Zugabe bekommt der Kunde eine mehr oder minder subventionierte Hardware mitgeliefert. Oft handelt es sich dabei um ein Modell der bekannten Fritz!Box, die vom deutschen Hersteller AVM (www.avm.de) aus Berlin hergestellt wird.



Details: Ein Merkmal aller Router/Firewall-Geräte für den Home-Bereich ist eine übersichtliche Weboberfläche, wie in diesem Beispiel bei einer Fritz!Box von AVM.

Anwender oder Firmen, die ihren Internetzugang über die Telekom erhalten, bekommen dann zumeist eine der ebenfalls sehr verbreiteten Speedport-Boxen zur Verfügung gestellt. Die verschiedenen Modelle dieser Kombinationen aus Router/Firewall, NAT-Gateway (Network Adress Translation) und WLAN-Access-Point haben sich im Lauf der vergangenen Jahre zu eine Art Standard entwickelt, der sich besonders im kleinen Firmenumfeld etabliert hat. Allerdings haben die Her-

steller ihre Router immer weiterentwickelt und Funktionserweiterungen implementiert. So können einige Geräte mittlerweile auch Drucker und Festplatten beziehungsweise externe Speichersysteme in das Netzwerk integrieren oder ihren Dienst als Media-Server verrichten.

1.2.1 Vor- und Nachteile von Fritz!Box und Co.

So scheint es denn auch für kleine Firmen und mittelständische Unternehmen zunächst eine gute Idee zu sein, diese als Teil des Providervertrags mitgelieferten Geräte auch für die Anbindung der Firma einzusetzen. Gerade die Home-Highend-Geräte aus diesem Umfeld, wie etwa die Fritz!Box Fon WLAN 7390 oder das Telekom-Speedport-Modell W920V, können mit einem eindrucksvollen Leistungsspektrum aufwarten. Zu den Vorteilen dieser Boxen zählen unter anderem:

- schnelle und einfache Konfiguration über eine Weboberfläche,
- integrierte SPI-Firewall (Stateful Packet Inspection),
- integrierter WLAN-Access-Point,
- Telefonieunterstützung und
- die Möglichkeit, Endgeräte wie mobile Festplatten und Drucker mithilfe der Boxen im Netzwerk bereitzustellen.

Gerade die vielen zusätzlichen Funktionen, die nicht der eigentlichen Aufgabe dienen, das interne Netz mit dem Internet möglichst sicher zu verbinden, sind jedoch im professionellen Einsatz überflüssig oder sogar schädlich:

- So bieten fast alle Home-Lösungen eine breite Unterstützung für sogenannte UPnP-Geräte an (Universal Plug & Play), die es ermöglicht, auch Geräte wie Stereoanlagen oder die ganze Haussteuerung über ein IP-basiertes Netzwerk anzusteuern. Mithilfe dieser Technik besteht bei vielen Geräten zudem die Möglichkeit, die Sicherheitseinstellung einschließlich der Freigabe von Ports zu steuern – so treten schnell ungewollt Sicherheitslücken auf.
- Die Stateful Packet Inspection ist für den professionellen Einsatz nur bedingt tauglich.
- Obwohl die Integration eines Druckers in das Netz über die Router-Box auch im Business-Umfeld sinnvoll sein kann, sind die Möglichkeiten dieser Geräte dabei zu beschränkt (beispielsweise keine Überwachung/Verwaltung, Drucker kann sich nicht in anderen Netzwerksegmenten befinden).
- VPN-Unterstützung (Virtual Private Network) ist zumeist nur rudimentär vorhanden (beispielsweise das Routing in multiple Netze).
- Der WLAN-Access-Point ist für den professionellen Einsatz (unter anderem Trennung in Gast-/Firmennetzwerke) in der Regel nicht zu gebrauchen.
- Die Weboberflächen stellen nur ein sehr eingeschränktes Feature-Set dar (das aber für den Heimbereich mehr als ausreichend ist) – geht es um komplexere

Einstellungen, so muss hier oft mit einer sehr kryptischen und unzureichend dokumentierten Kommandozeile gearbeitet werden.

1.2.2 Anforderungen an eine professionelle Lösung

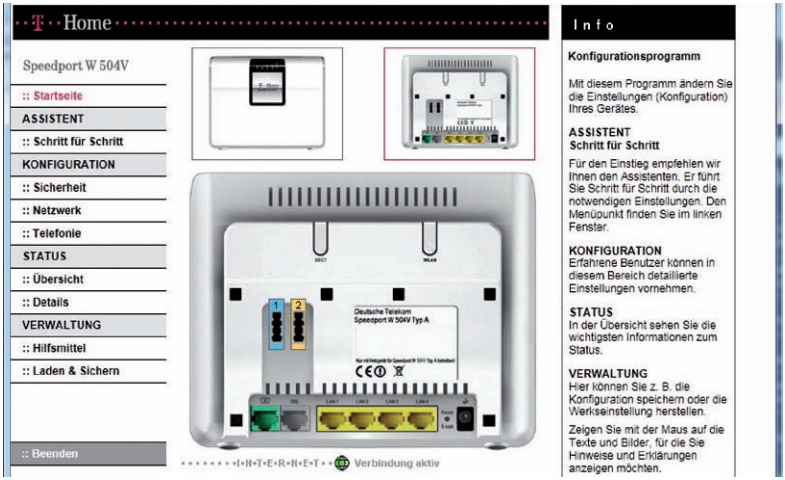
Wie diese Aufstellung zeigt, sind Geräte wie die Fritz!Box oder das Speedport für das häusliche Einsatzgebiet in der Regel vollkommen ausreichend. Doch welche Forderungen stellt der Profi an die Router/Firewall-Geräte, die den Zugang des Firmennetzwerks zum Internet regeln?

Überwachung mit SNMP: Gerade im Bereich des Managements offenbaren sich viele Schwächen der „Highend Home"-Geräte im Vergleich zu den professionellen Business-Verwandten. Für den Einsatz in einem professionellen Netzwerk ist eine Integration der Router in eine SNMP-Umgebung (Simple Network Management Protocol), beispielsweise mit dem kostenfreien Nagios, dringend erforderlich. Das ist aber in der Regel mit der Fritz!Box & Co. nicht möglich.

Ein Blick auf die Home-Variante: Zwar sind auch hier Port-Freigaben möglich, der Profi vermisst aber eine feine Granulierung bei den Einstellungen.

Durch den Einsatz von SNMP ist es dem Administrator möglich, sowohl den Netzwerktransfer als auch die Auslastung der CPU und des Arbeitsspeichers oder auch die Firmware-Versionen zentral im Blick zu haben. So sind dann auch automatisierte Aktionen, zum Beispiel ein Neustart des Routers bei absinkender Leistung oder bei zu hohem Transfer auf einem Port, einfach zu konfigurieren. Zwar ist es beispielsweise auf einer Fritz!Box möglich, ein angepasstes lauffähiges Linux-System inklusive SNMP-Support einzurichten. Das ist jedoch mit erheblichem

Aufwand verbunden, und es handelt es sich bei dem Gerät danach nicht mehr um die Standardauslieferung. Managementsoftware und Syslog: Ein weiterer wichtiger Punkt ist das „Logging“ mit Monitoring-Lösungen. So ist leider kaum eine Highend-Home-Lösung in der Lage, Syslog-Meldungen zu erstellen, zu speichern oder an einen zentralen Überwachungsserver zu schicken.

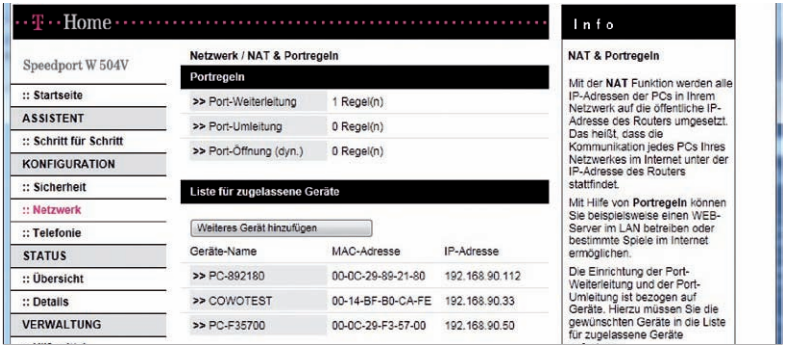


Ebenfalls sehr verbreitet: Speedport, eine Gerätebezeichnung der Telekom und von T-Online – dahinter stecken verschiedene Hersteller wie Siemens, AVM oder ‚wie hier bei der „W 504V“, Arcadyan.

Installation und Konfiguration: Mit den insgesamt guten Assistenten im Web-Browser ist die Installation von Home-Produkten wie der Fritz!Box in der Regel problemlos möglich. Geht es jedoch darum, eine größere Anzahl von Geräten auszuliefern, so muss entweder ein automatisierbarer Softwareassistent oder besser noch eine zentrale Managementsoftware zum Einsatz kommen. Während die Standardgeräte für den Heimbetrieb solche Funktionalitäten nicht bieten können, stellen Profi-Produkte, wie sie beispielsweise von den Herstellern SonicWall und Lancom angeboten werden, schon ab Werk solche Funktionen zur Verfügung.

Schutzfunktionen: Wird der DSL-Router direkt für die Internetanbindung ohne einen Proxy-Server dazwischen genutzt, so steigen die Anforderungen für den professionellen Einsatz deutlich an. Eine integrierte, objektorientierte Stateful-Packet-Inspection (SPI)-Firewall gehört hier zur Pflichtausstattung. Was unterscheidet diese Art der SPI-Firewall von der Funktionalität, die zumeist in den Highend-Home-Boxen à la Fritz!Box angeboten wird? Grundsätzlich kann heute eine Firewall, die nur eine „Stateful Packet Inspection“ ausführt, nicht mehr als sicher angesehen werden. Malware, Viren und Trojaner werden aktuell in anderen Protokollen (wie beispielsweise innerhalb des HTTP-Protokolls) gekapselt und können so von einer „normalen“ Firewall nicht entdeckt werden. Im professio-

nellen Umfeld muss ein solches Gerät deshalb den gesamten Datenstrom lesen und auch „verstehen“, um entsprechend auf die Bedrohung reagieren zu können. Solche Geräte werden von den Herstellern dann häufig als UTM-Firewalls (Unified Threat Management) bezeichnet.



Telekom-Router: Die Konfigurationsmöglichkeiten eines Speedport W 504V.

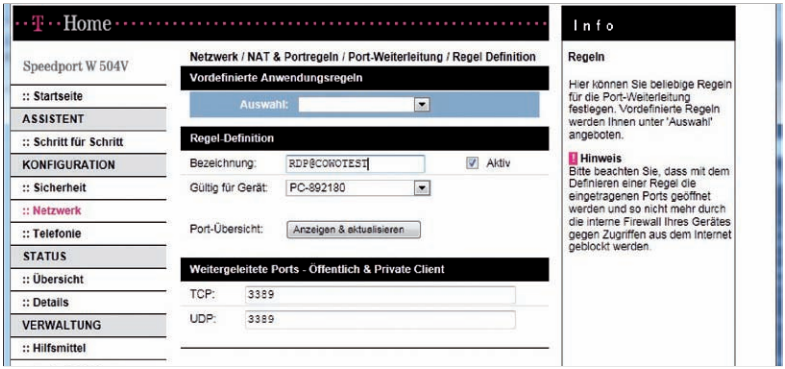
Zusätzliche Schutzeinrichtungen: Weiterhin sollte gegen mögliche Angriffe aus dem Internet ein Intrusion-Prevention-System mit integriertem DoS-Schutz zur Verfügung stehen. Abgerundet werden die Features eines „perfekten Profi-Systems“ schließlich durch einen Content-Filter, der über eine im Internet geführte Datenbank die Anzeige von Webseiten gemäß ihrer Einstufung wie beispielsweise Gewalt oder Pornografie verhindern kann.

1.2.3 Die Praxis: Vorteile einer professionellen Lösung

Aber aus dem Profi-Umfeld kommen noch weitere Anforderungen, wie etwa: VPN-Sicherheit über XAUTH (http://xauth.org/info/) oder Zertifikate, mehrere hardwarebeschleunigte parallele VPN-Tunnel, IPSec over HTTPs, Rogue Access Point Detection oder auch Voice over WLAN. Gerade beim praktischen Einsatz eines WLANs (heute faktisch Standard in allen Firmennetzwerken) zeigen sich die Stärken der professionellen Lösung deutlich: Mithilfe solcher Geräte stehen dann unter anderem folgende Möglichkeiten zur Verfügung:

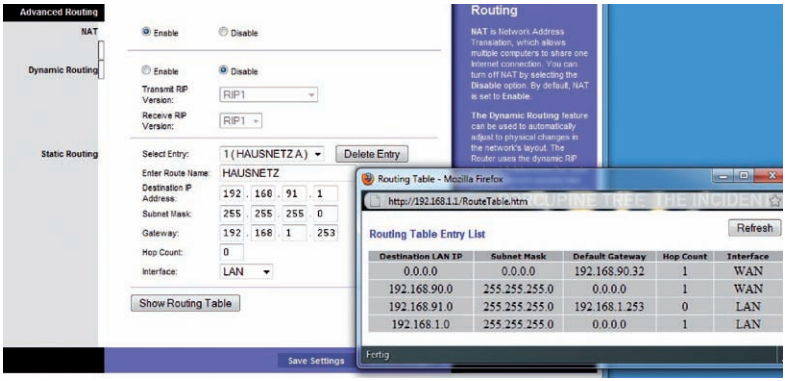
- Separate WLAN-Netze lassen sich mit jeweils individuellen Einstellungen beispielsweise für Gäste oder Mitarbeiter von Partnerfirmen mittels Multi-SSID (Service Set Identifier, bezeichnet den Namen eines Funknetzes) einrichten.
- Der WLAN-Zugang kann gefiltert werden: So können unter anderem nur bestimmte Client-System zugelassen oder auch gesperrt werden. Ein entsprechender Protokoll-Filter ist ebenfalls konfigurierbar, so dass nur ganz bestimmte Protokolle über diese drahtlose Verbindung möglich sind.

- Hohe Sicherheitsanforderungen können durch die Möglichkeit unterstützt werden, auch über das WLAN IPSec-Verbindungen (Internet Protocol Security) zu betreiben.



Zusatzfunktionen: Dank einer gezielten Port-Weiterleitung ist zumindest eine entsprechende Nutzung von RDP über feste IP-Adressen oder dynamisches DNS möglich.

Ein weiterer wichtiger Pluspunkt der professionellen Geräte im Vergleich zu Fritz!Box und Co. entsteht durch die Möglichkeit, mit ihrer Hilfe auch Mehrfachanbindungen zu erlauben: Die Home-Geräte richten sich nach den Gegebenheiten, die standardmäßig in diesem Umfeld zu finden sind: Für gewöhnlich wird es dort nur einen einzigen DSL-Zugang geben, der dann auch von diesen Boxen unterstützt wird – fällt dieser Zugang aus, so besitzt auch das gesamte dahinterliegende Netzwerk keinen Zugang mehr zum Internet.



Professionell: Was bei einem Heimgerät nicht möglich ist, war bei einem schon etwas „betagten" Router der Marke Cisco/Linksys BEFSR41v4 bereits selbstverständlich: bis zu 20 statische Routen.

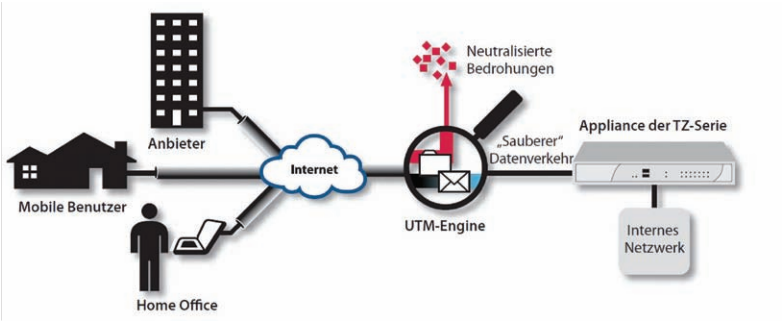
Viele Unternehmen verfügen hingegen über mehrere, leistungsstarke Verbindungen. Deshalb können Profi-Geräte bei einem Ausfall der DSL-Anbindung beispielsweise automatisch auf ISDN zurückschalten. Werden über die Router standortübergreifende VPN-Verbindungen eingerichtet, so kann der Administrator dann im Notfall über die ISDN-Verbindung entsprechend eingreifen.

Eine solche Mehrfachanbindung ist für Profi-Zwecke auch in Hinblick auf die Bandbreite interessant: So können beispielsweise mehrere DSL-Anschlüsse zur besseren Ausnutzung der Bandbreite häufig auch als „WAN Loadbalancing" miteinander kombiniert werden.

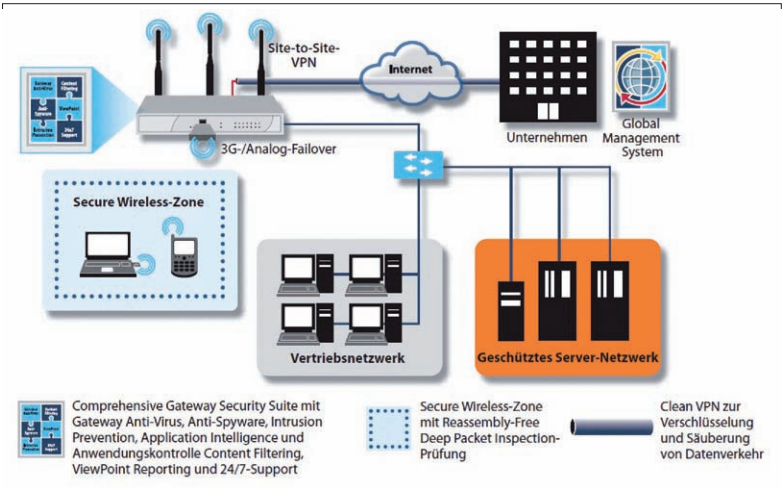
1.2.4 Fazit: Fritz!Box und Co. sind nichts für Profis

Router- und Firewall-Produkte wie die Fritz!Box, die von Providern als „Zugabe" zum Internetanschluss mitgegeben werden, sind für den privaten Bereich durchaus in Ordnung. Dort ist es immer auch möglich, dass die vorhandene Technik und die Geräte an die Möglichkeiten und Einschränkungen dieser Geräte angepasst werden. Ganz anders ist jedoch die Situation im professionellen Umfeld – und das gilt nicht nur für große Firmen mit entsprechend umfangreichen IT-Abteilungen, sondern auch für kleine und mittlere Betriebe: Die Sicherheit des eigenen Netzwerks sowie aller Geräte und Anwendungen darin ist ganz entscheidend von dieser einen Ressource abhängig

Ganz gleich ob es um das professionelle Management der Geräte oder beispielsweise um das Einrichten von dedizierten WLAN-Netzen oder VPNs geht: Mit den Home-Routern vom Schlage der Fritz!Box – und das gilt auch für die Highend-Geräte aus diesem Bereich – stoßen Anwender schnell an die Grenzen der Verwaltbarkeit und der Machbarkeit. Wenn dann noch Kriterien wie eine möglichst hohe Verfügbarkeit oder gar ein Managementzugriff aus der Ferne über eine redundante ISDN-Leitung hinzukommen, dann kann die Entscheidung nur für eine Lösung aus dem professionellen Umfeld ausfallen.



Sicherheit: Eine sogenannte „UTM-Maschine" sorgt dafür, dass ein internes Firmennetzwerk von unerwünschten Inhalten verschont bleibt.



Für den professionellen Einsatz: Diese Skizze soll verdeutlichen, dass eine professionelle Lösung nicht nur einfach den Internet-Zugang ermöglicht, sondern vielfältige andere Features zur Verfügung stellt, die im professionellen Einsatz gefordert werden, wie beispielsweise ein sicheres WLAN.

Abschließend sollte bei einer Entscheidung für ein solches System auch der Blick auf die Firewall-Funktionen sehr kritisch ausfallen: Wie in diesem Artikel ausgeführt, reichen die Fähigkeiten einer „normalen" SPI-Firewall heute keinesfalls mehr aus, um ein Netzwerk vor den Bedrohungen aus dem Netz zu schützen: Fast alle bekannt gewordenen großen Angriffe und Malware-Attacken der zurückliegenden Monate kamen gekapselt in die Netze – verpackt in ein HTTP-Paket, das ein Anwender beim normalen Ansurfen einer Webseite mitgebracht hatte. In solchen Fällen ist eine Fritz!Box machtlos; hier können nur professionelle Geräte mit der entsprechenden Technik helfen, die den kompletten Netzwerkverkehr untersuchen und „verstehen".

Thomas Bär, Frank-Michael Schlede

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation Computerwoche.

1.3 Breitband für alle – Zugangstechnologien im Überblick

Mit ihrer Breitbandstrategie will die Bundesregierung die flächendeckende Versorgung mit entsprechenden Zugängen und den Ausbau der Netze unterstützen. Auf der entsprechenden Website des Bundesministerium für Wirtschaft und Technologie (www.zukunft-breitband.de/BBA/Navigation/breitbandstrategie.html) sind denn auch ehrgeizige Ziele zu lesen: „Bis 2014 sollen für 75 Prozent der Haushalte Anschlüsse mit Übertragungsraten von mindestens 50 Megabit pro Sekunde zur Verfügung stehen."

Davon ist die Breitbandrealität noch weit entfernt: Unter den Top 20 der Länder, die Breitbandinitiativen priorisieren, ist Deutschland immer noch nicht zu finden. Und die Wirtschaftsprüfer von Deloitte (www.deloitte.com) kommen in ihrer Studie „Breitband Reloaded" zu dem Ergebnis, dass im Januar 2011 hierzulande lediglich 150.000 Endkunden bereits einen Glasfaseranschluss nutzten und erst 600.000 Haushalte an Glasfasernetze angebunden waren. Gründe für den schleppenden Ausbau sieht das Beratungshaus in den hohen Anschlusskosten von bis zu 3300 Euro bei Fiber to the Home (FTTH).

Schöne neue Welt: Die Breitbandstrategie der Bundesregierung sieht bereits für 2014 eine hohe Verbreitung von Internetanschlüssen mit mindestens 50 Mbit/s vor.

Die dominierende Technik ist hierzulande xDSL mit einem Marktanteil von 88 Prozent, sagt Robert Stumpf, Senior Executive und Netzexperte bei Accenture

(www.accenture.com). Kurz- und mittelfristig dürften aber die Kabel-TV-Anbieter Marktanteile erobern. Sie erreichen mehr als 60 Prozent aller deutschen Haushalte und können mit der Umrüstung auf die Spezifikation Docsis 3.0 (Data Over Cable Service Interface Specification) für Kabelmodem-Schnittstellen kurzfristig Bandbreiten um die 100 Mbit/s anbieten. Allerdings wird es diese leitungsgebundenen Techniken aufgrund der hohen Investitionskosten kaum flächendeckend geben. Wer nicht in einem der Ausbaugebiete wohnt, muss sich mit dem Gedanken anfreunden, dass sich dort ein schneller Breitbandzugang nur via Satellit oder per LTE realisieren lässt. Oder er muss selbst zur Schaufel greifen, wie jüngst E-Plus-Chef Thorsten Dirks laut Medienberichten auf dem Kongress des Zentrums für Telekommunikations- und Medienwirtschaft (ZfTM, www.zftm.de) in Duisburg scherzte: „Wenn die Leute auf dem Land DSL haben wollen, dann müssen sie einen Graben aufmachen und ein Kabel reinlegen."

1.3.1 Technologie-Mix prägt die Zukunft

Für Unternehmen, die ihre Standorte oder Filialen vernetzen, Home-Office-Anwender anbinden oder Außendienstmitarbeiter mobilisieren wollen, hat dies zur Konsequenz, dass sie künftig mit einem Mix aus verschiedenen Techniken planen müssen. Dabei ist nicht jede Technologie für jede Anwendung geeignet. „Geht es um die Internetnutzung im klassischen Sinne (Web Browsing), eignen sich alle Angebote", geht Björn Claaßen, Chief Operating Officer beim Netz- und Last-Mile-Spezialisten Keymile (www.keymile.com/de/), ins Detail. „Anwendungen mit höheren Anforderungen an die Performance (hoch auflösendes IPTV, 3D-TV, Online-Storage und andere Cloud-Dienste) sind nur mit leitungsgebundenen Techniken möglich." Satellit und LTE sieht er wegen hoher Verzögerung und geringer Up- und Downstream-Bandbreiten nicht als ernst zu nehmende Konkurrenz für Glasfaser und Co. Damit bleibt dem Anwender selbst im Breitbandzeitalter das Thema WAN-Optimierung nicht erspart, wenn er die Antwortzeiten der verwendeten Applikationen verbessern will. Martin Walzer, Manager Systems Engineering bei Blue Coat Systems (www.bluecoat.de), hat Trost parat: „Latenzzeiten lassen sich immer durch die Optimierung der übertragenen Protokolle verkürzen."

1.3.2 Glasfaser – das Gold der Zukunft

München, Köln, Hamburg, Hannover, Braunschweig, aber auch Schwerte, Coburg, Hanau, Kornwestheim oder Lünen – in immer mehr bundesdeutschen Kommunen werden Glasfasernetze bis zum Endkunden geplant oder schon verlegt. Wer in den erschlossenen Ausbaugebieten wohnt, erhält bereits heute Bandbreiten von bis zu 100 Mbit/s oder gar höher. Und angesichts von Anwendungen wie IP-basierten Videokonferenzlösungen, Arbeiten in der Cloud oder hoch auflösendem IP-TV sowie 3-D-TV sind viele Experten euphorisch. Hartwig Tauber, Geschäftsführer des FTTH Council (www.ftthcouncil.eu), einer europäischen Indus-

trievereinigung mit 150 Mitgliedern aus der Glasfaserbranche, ist sich beispielsweise sicher, „dass langfristig an der Glasfaser kein Weg vorbeiführt, da selbst VDSL nicht die benötigten Bandbreiten liefert".

Für Business-Anwender hätte der Siegeszug der Glasfaser noch eine andere Bedeutung: Sie wären nicht mehr auf die teuren SDSL-Verbindungen mit symmetrischen Upstream- und Downstream-Raten angewiesen, denn die Glasfaserzugänge offerieren auch schnelle Upload-Raten für ein remotes Arbeiten.

1.3.3 Die Grenzen der DSL-Technik

Die DSL-Technik stößt in den Ballungszentren längst an ihre Grenzen. Dort häufen sich die technischen Probleme und die Ausfälle. Wer vor zwei Jahren noch einen 18-Mbit/s-Anschluss hatte, erlebte oft eine schleichende Verlangsamung auf nur noch 10 Mbit/s. Andere wiederum stellen fest, dass ihr DSL-Anschluss zur Primetime am Abend komplett den Dienst versagt oder massive Störungen aufweist. Die Ursachen hierfür liegen in der Physik. Die typische Teilnehmeranschlussleitung (TAL, letzte Meile) besteht in Deutschland aus bis zu 2000 ungeschirmten Kupfer-Doppeladern, mit denen in den alten Bundesländern bis zu 1000 Telefonanschlüsse versorgt werden. Ursprünglich waren diese Kabel für die Übertragung von Frequenzen bis zu 3,1 Kilohertz konzipiert. Mit DSL werden nun über diese Kabel Frequenzen von bis zu 1 Megahertz transportiert.

Um zu verhindern, dass sich diese hohen Frequenzen gegenseitig stören, sollten nach Meinung der Technikexperten bei den Netzausrüstern lediglich 60 bis 80 Prozent der Kupferadern einer TAL mit DSL beschaltet werden, wobei der Wert auch vom Zustand des Kabels abhängt. Erschwerend kommt hinzu, dass noch Quereinstrahlungen von Starkstromverbrauchern (etwa Aufzüge und Straßenbahnen, aber auch Baukräne) die Übertragung stören. Langfristig dürfte das Kupfer in Verteilnetz und Teilnehmeranschlussleitung (TAL) an seine Grenzen stoßen, bilanziert auch das Beratungsunternehmen Deloitte in seiner Studie „Broadband Reloaded". Mehr Zukunftssicherheit böten Fiber to the Building (FTTB) und Fiber to the Home (FTTH). Björn Claaßen, Chief Operating Officer bei Keymile, bestätigt das: Im Mix der heute aktuellen Breitbandtechnologien sei die Glasfaser „die zukunftssicherste Lösung mit quasi unbegrenzten Bandbreiten". Allerdings sind die Gesamtkosten für Glasfaseranschlüsse um einiges höher als für VDSL. Während ein Haushalt im Schnitt für rund 700 Euro mit VDSL versorgt werden kann, betragen die Kosten für FTTB schon rund 1500 Euro. Und für FTTH errechnen die Wirtschaftsprüfer gar Kosten von bis zu 3300 Euro.

1.3.4 Bescheidene Glasfasernachfrage?

Rund 80 Prozent dieser Investitionen entfallen auf Grabungskosten und die Verlegung von Kabeln innerhalb der Gebäude. Zudem erweisen sich die Erdarbeiten in

den Innenstädten oft als schwierig und treiben die Kosten weiter in die Höhe. Dementsprechend ist es an der Glasfaserfront auch ruhiger geworden. So munkeln etwa Insider, dass der Regio-Carrier Mnet in München seinen Glasfaserplänen weit hinterherhinke. Nach dem öffentlichkeitswirksamen ersten Spatenstich im Herbst 2007 hätten die Münchner bis heute erst 15.000 Glasfaserkunden gewonnen. Zur bremsenden Wirkung der technischen Schwierigkeiten kommt der aus Sicht vieler Anwender geringe Nutzen: Ihnen fehlen noch die Inhalte und Services, die höhere Ausgaben lohnend erscheinen lassen. Die Motivation zu wechseln ist oft gering, zumal die Kunden auf die Preise achten und von DSL seit Jahren sinkende Kosten gewöhnt sind. Die Argumente der Glasfaserbetreiber reichen da oft nicht aus. Laut Deloitte sind die Anbieter häufig auch noch nicht so weit, die Nachfrage mit attraktiven Bundles anzukurbeln. Wie es gehen könnte, zeigt derzeit France Télécom, das unter dem Namen „La Fibre" unterschiedliche Pakete schnürt. Neben Internet-Access beinhalten sie HDTV, Internettelefonie und Online-Musik. Deloitte zufolge haben sich die Glasfaser-Provider bislang aber eher zu stark auf den Privatkundenbereich konzentriert. Dabei berge eine Kombination von Cloud-Services und schnellen Glasfaseranschlüssen große Marktchancen im Business-Kunden-Segment. Hier scheint bereits ein Umdenken stattzufinden: Viele Provider investieren derzeit in den Ausbau ihrer Data Center.

Offen ist zudem noch, mit welcher Technik ausgebaut wird. Zuvor müssen die Provider den Bandbreitenbedarf der nächsten 20 bis 25 Jahre abschätzen. Die Entscheidung für eine Technik ist auch für künftige Business-Modelle entscheidend. Experten zufolge eignet sich die GPON-Technik (Gigabit Passive Optical Network) weniger für einen offenen Markt und erschwert Mitbewerbern den Netzzugang. Wenn sie sich in der Breite durchsetzt, dürfte es einen Wettbewerb, wie die Anwender ihn von DSL her kennen, nicht mehr geben.

1.3.5 Kabel-TV – wie Phönix aus der Asche

Als die Deutsche Telekom (www.telekom.de) zwischen 2000 und 2003 ihr TV-Kabelnetz auf Druck der EU und nationaler Wettbewerbsbehörden verkaufen musste, gaben viele Experten der Technik keine Zukunft. Digitales Fernsehen via Satellit und schneller Internetzugang via xDSL galten als die relevanten Zukunftstechnologien. Von vielen wurde das Netz damals nur noch müde als „Investitionsruine Schwarz-Schilling" belächelt.

Knapp zehn Jahre später ist das Netz wie Phönix aus der Asche auferstanden und setzt die etablierten Carrier in Sachen Glasfaserausbau in Zugzwang. So heizt der größte TV-Kabel-Provider Kabel Deutschland (www.kabeldeutschland.de) den Preiskampf bei den Internetangeboten weiter an: Ein Internetzugang mit bis zu 6 Mbit/s im Downstream und bis zu 465 Kbit/s im Upstream inklusive Internet- und Telefon-Flatrate ist für 17,90 Euro im Monat zu haben. Sechs Millionen Haushalte in Ausbaugebieten versorgt das Unternehmen schon heute mit 100-Mbit/s-Anschlüssen (6 Mbit/s im Upload) zum Kampfpreis von 19,90 Euro pro Monat in

den ersten zwölf Monaten. Bis März 2012 will der Konzern dann mehr als zehn Millionen Haushalte versorgen. Insgesamt sind rund 22 Millionen Haushalte an das TV-Netz angeschlossen. Das Geschäft dominieren vier Player: Kabel Deutschland, Unitymedia (www.unitymedia.de), Kabel BW sowie Tele Columbus (www.telecolumbus.de). Selbst für Business-Anwender ist das Kabelnetz heute eine Access-Alternative bei der Filialvernetzung – vor allem Selbstständige sowie kleine und mittlere Unternehmen zeigen Interesse. Auch wenn Kabel Deutschland, wie Pressesprecher Marc Gassen einräumt, „primär die Privatkunden im Fokus hat", schnürte das Unternehmen Produktpakete für professionelle Anwender.

1.3.6 Kabelpakete

Unter der Bezeichnung „Internet &Telefon Business 32" ist ein Bundle erhältlich, das einen Internetzugang (32 Mbit/s down, 2 Mbit/s up), vier Telefonleitungen sowie ein Hosting-Angebot für E-Mail und Website enthält.

In Sachen E-Mail erhält der User 500 Postfächer mit jeweils 2 GByte Speicherplatz. Für die Homepage stehen 4 GByte Speicher sowie zwei Wunsch-Domains zur Verfügung. Hierfür verlangt das Unternehmen während der Mindestvertragslaufzeit von zwölf Monaten rund 30 Euro pro Monat. Wer auf den Telefonanschluss verzichtet, kann für 24,90 Euro pro Monat auch einen reinen Internetzugang mit 100 Mbit/s erhalten. Befürchtungen, dass das TV-Kabel den Business-Anforderungen nicht genügen könnte, entgegnet Gassen: „Wir hatten in Sachen Internetzugang 2009 eine gemessene Verfügbarkeit von 99,85 Prozent." Zudem stünden Business-Kunden bei technischen Beeinträchtigungen eigene Berater 24 Stunden täglich an sieben Tagen der Woche zur Verfügung.

Möglich wurde dies, weil Kabel Deutschland und andere TV-Netz-Provider ihre Netze konsequent in Richtung Internet ausgebaut haben, um neue Zielgruppen und Einnahmequellen zu erschließen. „Pro TV-Kunde erzielen wir einen durchschnittlichen Umsatz von acht bis zehn Euro, während wir bei den Internetkunden monatlich bei rund 30 Euro liegen", rechnet Gassen vor. Hierzu mussten die Betreiber beispielsweise in einen Rückkanal investieren, der für interaktive Dienste oder Internet erforderlich ist. Ähnlich wie bei VDSL setzten die Kabler zudem auf eine hybride Infrastruktur, bei der Glasfaser zum Einsatz kommt und das Koaxkabel nur noch auf den letzten Metern verwendet wird. Ferner war die Aufrüstung auf die Kabelmodemspezifikation Docsis 3.0 notwendig, denn erst diese unterstützt Bandbreiten von bis zu 200 Mbit/s und überbrückt im Gegensatz zu DSL größere Entfernungen. „Technologisch sind die Kabelnetze xDSL überlegen, da sie hohe Bandbreiten von über 100 Mbit/s ermöglichen", bestätigt Robert Stumpf, Senior Executive bei Accenture und Netzexperte. Früher oder später dürften die TV-Netzbetreiber, so Klaus von den Hoff, Leiter der Time-Practice bei Arthur D. Little (www.adlittle.de), aber die Konkurrenz der Glasfaser spüren. Er rät den Betreibern deshalb, im Zuge des LTE-Ausbaus Quadruple-Play-Angebote zu schnüren, die einen mobilen Datendienst beinhalten.

1.3.7 Satellit – Backup und Lückenbüßer

Kein Breitbandzugang? Was sich viele Städter angesichts von xDSL, Kabel-TV und Glasfaserzugängen nicht vorstellen können, ist nach Angaben des TÜV Rheinland (www.tuv.com) für fast 1,1 Millionen Haushalte noch immer traurige Realität. Weitere acht Millionen Haushalte können, so die TÜV-Untersuchung, nur mit maximal 2 Mbit/s ins Netz. Abhilfe verspricht hier der Internetzugang via Satellit. Moderne Sat-Zugänge haben nicht mehr viel gemein mit den ersten satellitengestützten Datendiensten. So gehört es heute zum guten Ton, dass der Rückkanal ebenfalls über Satellit läuft und nicht mehr via Telefonmodem. Und die Bandbreiten erreichen mittlerweile Breitbandniveau.

Damit ist der Internetzugang via Satellit auch für Business-Kunden interessant – sei es als Backup-Verbindung für den Notfall, als bedingt mobile Lösung etwa auf Baustellen oder als vollwertige Lösung für Gebiete, in denen UMTS und Co. fehlen. Für den Satelliten spricht zudem, dass bei ihm – im Gegensatz zum Mobilfunk – die Geschwindigkeit und der Empfang nicht von der Entfernung zu den Sendemasten abhängen, sondern überall gleich sind.

1.3.8 70 Gbit/s Datendurchsatz

Wie leistungsfähig der Datentransport über das Weltall mittlerweile ist, demonstriert die Eutelsat-Tochter Skylogic (www.skylogic.it) mit Partnern. Dank des neuen KA-Satelliten, der im Dezember 2010 in seine Umlaufbahn geschossen wurde, kann Eutelsat nun mit einem Datendurchsatz von 70 Gbit/s aufwarten (siehe auch Internet per Satellit – KA-SAT erfolgreich gestartet, Webcode **2033173**).

Als paneuropäischer Satellit konzipiert, leuchtet er Europa und den Mittelmeerraum aus. Um eine möglichst effiziente Nutzung der verfügbaren Frequenzen zu ermöglichen, wurde das Empfangsgebiet in 82 Spotbeams unterteilt – vereinfacht ausgedrückt kann man einen Spotbeam etwa mit der Funkzelle einer Mobilfunkbasisstation vergleichen. Deutschlandweit werden sieben Spotbeams mit einem Durchmesser von jeweils 250 Kilometern schnelle Internetdienste bereitstellen. Sie sind fix installiert, und der Anwender kann normalerweise nicht einfach von einem Spotbeam in einen anderen wechseln. Am Boden sorgt ein über Europa verteiltes Netz von acht Gateways (eines befindet sich in Berlin) für die Verbindung zwischen Satellit und Internet. Die Gateways selbst sind über einen Glasfaserring miteinander verbunden. Entsprechende Zugangspakete, wie sie beispielsweise die Internetagentur Schott (www.satspeed.com) offeriert, reichen von Basic-Tarifen (down 6,144 Mbit/s, up 1,024 Mbit/s) für monatlich 13,90 Euro bis hin zu Premium-Paketen (down 10,24 Mbit/s, up 4.096 Mbit/s) zum Monatspreis von 44,90 Euro – wobei die Tarife jeweils für das erste Jahr gelten. Will der Anwender die Satellitenhardware, bestehend aus Schüssel, LNB und Modem beziehungsweise Router, kaufen, so muss er hierfür rund 300 Euro einkalkulieren. Viele Anbieter offerieren das Equipment aber auch auf Mietbasis.

1.3.9 Zukunft: Roaming ohne Gebühren

Bedenken, dass Websurfen via Satellit aufgrund der Latenzzeiten keinen Spaß macht, entgegnet Stephan Schott, Technical Director bei der Internetagentur: „Sie können damit ganz normal flüssig surfen und auch VoIP nutzen." Hierzu verwendet Schott Kompressionsverfahren, um das Datenvolumen zu reduzieren. Schott räumt allerdings ein, dass die Latenzzeit (die Daten legen hin und zurück 72.000 Kilometer zurück) bei 520 Millisekunden liegt: „Für Powergamer ist das nichts."

Dafür kann der Anbieter demnächst mit anderen Argumenten punkten: So ist ein Prepaid-Angebot geplant, das etwa als temporärer Zugang für den Zweitwohnsitz interessant ist oder für Unternehmen als Backup-Lösung.

Im Gespräch sind auch Lösungen, die es erlauben, den Zugang auch an anderen Lokationen, etwa im europäischen Ausland, zu nutzen – ohne Roaming-Gebühren, wie sie bei den Mobilfunkern anfallen. Hier müsste dann der Anbieter für einen begrenzten Zeitraum den Zugang in einem anderen Spotbeam freischalten. Für die weißen Flecken hat Schott die Mehrteilnehmerlösung „Satspeed" entwickelt. Mit ihr können bis zu 24 Häuser via Sat mit Datenraten von bis zu 10 Mbit/s im Down- und 4 Mbit/s im Upstream angeschlossen werden.

1.3.10 LTE – die mobile Breitbandhoffnung?

Als die UMTS-Frequenzen im Jahr 2000 für rund 51 Milliarden Euro in Deutschland versteigert wurden, waren die Erwartungen hoch: Mit den Mobilfunknetzen der dritten Generation (3G) sollte endlich die schnelle mobile Datenübertragung Einzug halten. Noch größer war in der Folge aber die Enttäuschung: Hohe Latenzzeiten und je nach Auslastung der Funkzellen stark schwankende Übertragungsraten machten das Arbeiten mit remoten Anwendungen zur Qual.

Abhilfe verspricht nun die vierte Mobilfunkgeneration (4G), auch als Long Term Evolution (LTE) bekannt. Geringe Latenzzeiten sollen Anwendungen wie VoIP, IP-Video, schnelle Online-Spiele und Echtzeitanwendungen ermöglichen. Und mit theoretischen Spitzenraten von bis zu 170 Mbit/s stellen große Datenmengen auch kein Problem mehr dar. Euphorisch feiert mancher Marketier LTE bereits als Ersatztechnik für den klassischen Kupferanschluss.

Early Adaptors sollten allerdings Vorsicht walten lassen, da zwischen der Theorie und der Realität große Lücken klaffen und sie im Alltag mit etlichen Einschränkungen leben müssen:

- Zurzeit werden primär die weißen Flecken, in denen es kein DSL oder andere Breitbandanschlüsse gibt, mit LTE versorgt.
- Das verwendete Equipment arbeitet im 800-Megahertz-Frequenzbereich und kann deshalb später nicht mobil etwa in Großstädten genutzt werden.
- Angepriesene Datenraten von bis zu 50 beziehungsweise 100 Mbit/s sind unrealistisch. In der Regel sind sie nur unter optimalen Empfangsbedin-

gungen zu erhalten. Den Stand der Technik gibt die Telekom wieder: Sie wirbt mit nur 3 Mbit/s.

- Im Kleingedruckten der Verträge verstecken sich Fallen. Hier gelten ähnlich wie im Mobilfunk Einschränkungen wie „kein VoIP", „kein P2P", „Volumenbegrenzungen" etc. Damit ist LTE oft kein echter Ersatz für einen schnellen Festnetzanschluss.

1.3.11 LTE-Praxis

Dass LTE-Equipment nicht überall funktioniert, rührt daher, dass für LTE mehrere Frequenzbereiche (800 Megahertz, 1,8, 2,0 und 2,6 Gigahertz) genutzt werden. Mit der Vergabe des 800-Megahertz-Bandes – auch als digitale Dividende bekannt – verknüpfte die Bundesnetzagentur (www.bundesnetzagentur.de) die Bedingung, dass die mit Breitband unterversorgten Landstriche zuerst bedient werden müssen. Erst danach dürfen die Carrier LTE in den wirtschaftlich lukrativeren Ballungsräumen und Metropolen in Betrieb nehmen (siehe auch LTE in der Großstadt – Telekom startet Netz in Köln, Webcode **2035775**).

In den Städten kommen dann die Frequenzen aus dem Gigahertz-Spektrum zum Einsatz, weshalb sich hier das heute übliche LTE-Equipment meist nicht verwenden lässt. Auch wenn der LTE-Rollout schneller vonstatten geht als geplant und bereits im Sommer erste Städte mit LTE-Angeboten aufwarten, sollten IT-Entscheider ihre Mobilstrategie noch mit der klassischen 3G-Technik planen. Viele Experten gehen nämlich davon aus, dass es zumindest in Deutschland eine LTE-Flächendeckung auf lange Sicht nicht geben wird.

Bei allen Einschränkungen und offenen Fragen ist immerhin festzustellen, dass LTE in Sachen mobile Datenübertragung im Vergleich zu den heutigen 3G-Techniken UMTS und HSPA eine Revolution darstellt. So konnte sich die Computerwoche in einem weißen Flecken nahe dem bayerischen Ebersberg im O2-Netz (http://o2online.de/) vom LTE-Potenzial überzeugen: Im Test erreichten die Kollegen Latenzzeiten um die 30 Millisekunden, sodass etwa das Arbeiten mit einer Citrix-Desktop-Lösung kein Problem darstellte. Dabei ermittelten die Kollegen durchschnittliche Download-Raten um die 40 Mbit/s und in der Gegenrichtung um die 12 Mbit/s.

Jürgen Hill

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation Computerwoche.

Jürgen Hill ist Redakteur bei unserer Schwesterzeitschrift Computerwoche und dort für Produkte & Technologien zuständig.

1.4 Ratgeber – Faxen übers Internet

Trotz Internet und E-Mail gehört das gute, alte Faxgerät immer noch zur Standardausrüstung in jedem Büro. Dabei müssen selbst eingefleischte User des Web zugeben: In manchen Bereichen übertrumpft das altmodische Fax die modernere E-Mail. Beispielsweise werden gefaxte Dokumente eher akzeptiert als E-Mails, wenn es auf Beweisbarkeit ankommt und eine manuelle Unterschrift verlangt wird. Bei Bestellungen etwa vertrauen viele Kunden dem Fax mehr als der elektronischen Post. Auch bei Spam, Viren und E-Mail-Flut – also in Sachen Sicherheit – punktet das Fax. Ein Fax ist absolut sicher vor Viren, und die Spam-Problematik hält sich in Grenzen. Zudem ist es aufmerksamkeitsstärker als eine Mail: Ein Fax wird in der Regel vor dem Entsorgen angeschaut. Kurzum: Das Fax ist die perfekte Symbiose von papierener Tradition und moderner Technik. Das macht Faxdienste für viele Unternehmensbereiche immer noch interessant.

Heute wird das Fax in der Regel am Rechner produziert und oft von dort auch gleich verschickt. Fax-Softwarelösungen für PCs erledigen diese Arbeit. Doch nicht jeder kann diese nutzen – die wenigsten PCs oder Notebooks sind direkt an eine Telefonleitung angeschlossen. Wer DSL nutzt oder in einem Netzwerk arbeitet, hat so oft das Nachsehen.

An diese Kunden und an solche, die sich Faxgerät und Faxsoftware ganz sparen wollen, wenden sich die Anbieter von Internet-Fax-Services. Die Vorteile: Die Anschaffung von Faxhardware und -software und deren Installation entfallen. Das ganze Gefummle mit Faxgerät oder Faxprogrammen wird durch leicht handhabbare, zuverlässige und ohnehin meist vorhandene Internettechnik ersetzt. Ein Internet-Anschluss und ein Web-Browser oder Mail-Programm genügen. Davon profitieren mobile Mitarbeiter, denn auch von unterwegs aus lassen sich so Faxe empfangen und versenden. Kunden können sich für diesen Dienst komfortabel und auf direktem Weg auf der Website anmelden und den Service innerhalb kürzester Zeit nutzen. Doch Vorsicht: Gerade im Business-Bereich lauern hier Fallen.

1.4.1 Faxen via Web

Internet-Faxdienste lassen sich grundsätzlich auf zwei verschiedene Arten realisieren: als webbasierte Dienste und als Mail-basierte Dienste. Die rein webbasierten Faxdienste wickeln den Faxverkehr vollständig über das WWW und ein Web-Interface ab. Der Sender ruft die Homepage eines Faxdiensteanbieters auf und trägt dort auf dem Webformular Text, Empfängername und Empfängerfaxnummer ein. Einige, aber nicht alle Dienste ermöglichen dabei, auch den Anhang von Text- oder Bilddateien in Standardformaten wie PDF zu senden. Anschließend wird die Nachricht vom Dienstleister an den nächstgelegenen Faxserver auf der Empfängerseite weitergeleitet. Dieser Zielserver überträgt mittels seines eigenen Faxmodems die Nachricht beziehungsweise das Dokument zum Empfängerfax. Das geschieht in der Regel zum Ortstarif.

Webbasierte Dienste bieten damit vollkommene Standortunabhängigkeit und problemlosen, mobilen Zugang. Der End-User braucht lediglich einen PC oder ein Notebook mit Internetzugang und Web-Browser. WWW-Faxe sind damit besonders praktisch, wenn man von unterwegs Faxe verschicken oder empfangen will. Ein normaler Webfaxdienst eignet sich ohne Zusatzoptionen allerdings nur für den Versand kürzerer Nachrichten.

1.4.2 Unified Messaging – Beispiel GMX

Die wenigsten Dienste beschränken sich auf die reine Übermittlung von Faxnachrichten: Häufig handelt es sich bei den Profi-Diensten um Anbieter mehr oder weniger kompletter „mobiler Bürolösungen" – im Fachjargon Unified Messaging –, die Voice-, E-Mail-, SMS- und Faxnachrichten per Internet anbieten. Typische Vertreter solcher Lösungen sind 3-Box, GMX und Web.de.

In Deutschland sind die beiden Freemail-Anbieter GMX (www.gmx.de) und Web.de die bekanntesten Online-Dienstleister, die ihren Kunden einige United-Messaging-Funktionen kostenfrei und andere gegen Bezahlung anbieten. Bei GMX erhalten Nutzer des E-Mail-Dienstes, die den Tarif Pro (2,99 Euro monatlich) oder Top (4,99 Euro monatlich) wählen, eine persönliche Telefonnummer, mit der sie Faxe empfangen können. Faxe werden dabei in PDFs umgewandelt und per E-Mail-Anhang an die Browser-basierte Mailbox zugestellt. Der GMX-Kunde kann beliebig viele Faxe empfangen. Unter *Mein GMX – Fax und Voice – Fax senden* haben GMX-Mitglieder auch die Möglichkeit, umgekehrt textbasierte Faxnachrichten zu erstellen und zu versenden. Die ersten zehn Faxe pro Monat sind im Top-Tarif kostenlos. Zudem können Faxe auch direkt aus Anwendungen wie Word und PowerPoint heraus verschickt werden.

1.4.3 Beispiel Web.de

Kunden des E-Mail-Dienstes von Web.de bekommen auch in der Freemail-Version eine Sprach-/Fax-Mailbox. Gefaxt werden kann ans dem In- und Ausland über das Web-Interface. Das Versenden einer Inlandfaxseite kostet für Nichtmitglieder 30 Cent, für kostenpflichtige Mitglieder 20 Cent. Eingegangene Faxe werden als PDF-Datei in einer E-Mail im Posteingang abgelegt. Hierfür erhält jedes Mitglied eine eigene Nummer, die auch für Sprachnachrichten genutzt werden kann. Zudem können Dokumente im PDF-Format über die PDF-Faxfunktion direkt aus dem persönlichen Web.de-Postfach verschickt werden.

1.4.4 Fax-to-Mail

Die zweite Möglichkeit von Internetfaxdiensten ist, Faxe über ein E-Mail-Gateway zu verschicken und zu empfangen. Bei Dienstleistern, die diesen Service anbieten,

erhält man eingehende Faxe (Fax-to-Mail) in Form einer Grafikdatei (TIF, GIF oder PDF) als Dateianhang einer Mail. Der Faxdienst übernimmt die Weiterleitung über das Internet an den Empfänger und sorgt auch für die Umwandlung des Faxes in eine E-Mail. Ausgehende Sendungen (Mail-to-Fax) werden über E-Mail an das Fax-Gateway des Anbieters geschickt und kommen beim Empfänger am Faxgerät an. Die Vorteile der Mail-Gateways gegenüber der Web-Lösung: Das Verfahren eignet sich insbesondere für längere Dokumente. Kunden erhalten ihre persönliche Faxnummer, die permanent empfangsbereit ist. Der Aufwand ist gering und durch das Umgehen der langsamen webbasierten Clients besonders schnell. Der Anwender kann E-Mails und Faxe bequem in seinem normalen E-Mail-Programm versenden und empfangen. Er hat dabei stets den Überblick und die genaue Kontrolle über den Versand- beziehungsweise Empfangsstatus.

Es gibt jedoch auch Nachteile: Während sich webbasierte Faxdienste flexibel einsetzen lassen und schnell auch mal unterwegs auf Geschäftsreise erlauben, Faxe zu senden oder zu empfangen, ist die E-Mail-Lösung wesentlich restriktiver: Einer der Kommunikationspartner muss über ein Fax und damit einen Telefonanschluss verfügen – bei Fax-to-Mail ist dies der Sender. Die E-Mail-Lösung eignet sich also eher zum stationären Einsatz.

1.4.5 Wer profitiert?

Fax-to-Mail bietet sich beispielsweise für Unternehmen an, die im Ausland präsent sein wollen, ohne dort gleich ein eigenes Büro mit teuren Endgeräten eröffnen zu müssen. In diesem Fall kann der Auslandsmitarbeiter Faxe von der Zentrale per Mail empfangen. Auch für Mitarbeiter, die viel unterwegs sind und überall Zugriff auf die eingehenden Faxe benötigen, ist Fax-to-Mail interessant: Denn unterwegs muss man auf ein stationäres Faxgerät verzichten, die E-Mails lassen sich dagegen von nahezu überall in der Welt abrufen. Ein umständliches Hinterherfaxen eingehender Nachrichten ins Hotel entfällt damit. Und wer sehr kurzfristig eine Faxnummer benötigt und weder auf den Telekom-Techniker warten kann noch die hohen Einrichtungsgebühren bezahlen will, findet in Fax-to-Mail ebenfalls eine vernünftige Alternative.

1.4.6 Mail-to-Fax

Andere Vorteile hat der umgekehrte Vorgang: Mail-to-Fax. Hier muss der Empfänger über ein Faxgerät und einen Telefonanschluss verfügen. Mail-to-Fax ist besonders attraktiv beim Verschicken von Massensendungen: Anders als mit Faxgerät bleibt die Telefonleitung in diesem Fall nur für kurze Zeit belegt – nämlich für die einmalige Übertragung der E-Mail.

Im Empfängerfeld können fast beliebig viele Empfänger stehen. Einen weiteren Vorteil bietet Mail-to-Fax, wenn zwar ein Faxgerät vorhanden ist, dieses aber für

eingehende Faxe zugänglich sein soll. Typische Situation: Man wartet auf wichtige Faxdokumente, müsste aber auch dringend ein paar Faxe verschicken.

1.4.7 Vorsicht, Werbung

Einige der Faxdienstleister sind kostenlos und finanzieren sich durch Werbung. Wer diese Dienste in Anspruch nimmt, muss sich darüber im Klaren sein, dass nicht nur die Website mit Reklame verziert ist, sondern auch das Fax selbst. Für viele Geschäftszwecke ist dies nicht tragbar. Außerdem: Oft müssen Besucher erst umfangreiche Fragebögen ausfüllen, bevor sie den Service nutzen können. Die Daten werden dann an Werbekunden weitergegeben. Noch am erträglichsten sind Dienste, die Werbung nur spärlich und lediglich für das eigene Angebot auf das Fax platzieren. Andere benutzen die ganze erste Seite für Werbung, der eigentliche Text befindet sich auf der Folgeseite. In der Regel weiß der Faxsender auch nicht, welche Werbung sein Schreiben ziert, schlimmstenfalls können es Erotikanzeigen sein. Im Business-Bereich ist von werbefinanzierten Faxen deshalb abzuraten. Neben der Reklame kommen bei kostenlosen Services weitere Einschränkungen hinzu. So ist die Zahl der kostenlosen Faxe pro Tag meistens beschränkt. Auch der Umfang der einzelnen Faxe ist bei vielen Anbietern begrenzt. Zudem können oft keine Anlagen oder Bilder mitverschickt werden.

1.4.8 Faxen via Mail-Gateways und Web

In den folgenden Tabellen erhalten Sie eine Übersicht über ausgewählte Anbieter von Faxdiensten via Mail-Gatways und Web. Neben dem Angebot haben wir zusätzlich die entstehenden Kosten angegeben.

Faxen via Mail-Gateways: Die Diensteanbieter im Überblick.

Dienst	URL	Angebot	Kosten
GermanyFax	http://germanyfax.de/pages/kostenlos-faxen.php	Mail-to-Fax Gateway, mit einfacher kostenloser, eingeschränkter Faxfunktion. Unbeschränkt Faxen in verschiedenen Tarifstufen	Kostenlos; sonst ab 7,5 Cent pro Fax bei 5 Euro monatl. Mindestumsatz
Fax senden	www.fax-senden.de	Mail-to-Fax, Fax-to-Mail und Web-to-Fax: Versand von Internetfaxnachrichten mit Texten, Bildern oder PDFs. Auch Excel, Word. Sehr übersichtliche, gut strukturierte Website.	Instant: 65 Cent 1 Seite Exklusiv: ab 15 Cent 1 Seite Premium: individuelle Enterprise Services ab 100 Euro Umsatz monatlich.

eFax	www.efax.com	Mail-to-Fax und Fax-to-Mail: Nationaler und internationaler Faxversand und -empfang.	Ab 11 Euro / Monat; Versand 9 Cent pro Seite, Empfang von bis 130 Seiten kostenlos
Faxverteiler	www.faxverteiler.com	Dienst für größere Faxaktionen im Einzelauftrag und Monats-Abo (z.B. regelmäßige Fax-Mailings). Versand und Empfang z.B. als PDF im Monats-Abo über Web-Tool Faxsuite.	9,90 Euro / Monat, Einzelaufträge ab 1,7 Cent pro Faxseite.
2Mail2	http://2mail2.com	Mail-to-Fax und Fax-to-Mail:Hier bekommt man eine Berliner Festnetznummer, die Fax- und Sprachnachrichten aufzeichnet und per E-Mail weiterleitet. Versand von doc pdf- oder anderen Dokumenten nicht möglich.	Mehrere Tarife. z.B. Basic (2 Euro / Monat): Empfang: 20 Faxe; Versand: 5 Cent national.
Computron	www.gnetx.com	Mail-to-Fax und Fax-to-Mail: Wer keinen Internet-Gnetx-Anschluss für die Abfrage seiner E-Mails zur Verfügung hat, beispielsweise auf Reisen, kann sich die elektronische Post mit diesem Dienst faxen.	Mail-to-Fax: Einrichtungsgebühr: 5 Euro; monatliche Pauschale 2,50 Euro. Zusätzlich sind Kosten pro Sendeminute fällig.
Email4Fax	www.email4fax.de	Mail-to-Fax: Weltweiter Faxversand per Mail oder Browser. Faxnachrichten können aus Websites (z.B. Online-Shops) generiert werden, Attachments als TIF, PDF oder TXT.	Ab 7,5 Cent pro Seite.

Der Faxversand über das Web ist unabhängig vom Standort und besonders für mobile Anwender geeignet. Der Nutzer benötigt nur einen Rechner mit Internetzugang und einen Webbrowser.

Faxen via Web: Die Diensteanbieter im Überblick.

Dienst	URL	Angebot	Kosten
GMX	www.gmx.net	Unified-Messaging-System; Versand und Empfang von Faxen über eine persönliche Rufnummer; nur über kostenpflichtige Mitgliedschaft.	Tarif ProMail: 2,99 Euro monatlich; TopMail: 4,99 Euro monatlich inkl. 10 Freifaxseiten, Faxversand: 20 Cent pro Seite (BRD).

Web.de	www.web.de	Unified-Messaging-System; Versand und Empfang von Faxen auch bei kostenloser Mitgliedschaft, Komfortfunktionen über Smartfax möglich.	20 Cent pro Faxseite für Mitglieder, 30 Cent für Nichtmitglieder.
Directbox	www.directbox.com	Gut strukturierter Unified-Messaging-Dienst mit Faxversand und Empfang im Free-, Eco-, Get- und Pro-Tarif.	Free (0 Euro): 15 Cent pro Fax Eco (0,99 Euro): 5 frei, dann 15 Cent pro Fax Get (1,99 Euro): 10 frei, dann 15 Cent pro Fax Pro (3,99 Euro): 20 frei, dann 15 Cent pro Fax.
3-Box	www.3box.de	Komplettes Unified-Messaging-System für eingehende und ausgehende Nachrichten. Faxe lassen sich beliebig vergrößern, verkleinern und drehen.	15 Euro pro Monat, keine weiteren Gebühren.
Fax.de	www.fax.de	Umfangreicher, sehr professionell wirkender Fax-Dienstleister mit breitem Portfolio wie Fax- und Briefversand direkt aus Anwendersoftware, iPhone-App.	Je nach Leistung ab 5 Euro Monatsgebühr, Faxversand ab 4,9 Cent pro Seite.

Klaus Manhart

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation Computerwoche.

Dr. Klaus Manhart hat an der LMU München Logik/Wissenschaftstheorie studiert. Seit 1999 ist er freier Fachautor für IT und Wissenschaft und seit 2005 Lehrbeauftragter an der Uni München für Computersimulation. Schwerpunkte im Bereich IT-Journalismus sind Internet, Business-Computing, Linux und Mobilanwendungen.

TecChannel-Links zum Thema	Webcode	Compact
Ratgeber – Faxen übers Internet	2035270	S.33
Ratgeber – Alles was Sie über IPv6 wissen sollten	2035716	S.9
Ratgeber – Anforderungen an professionelle DSL-Router	2035759	S.17
Breitband für alle – Zugangstechnologien im Überblick	2035913	S.25
Smart Grids Intelligente Stromnetze der Zukunft	2035308	S.39

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

1.5 Smart Grids – Intelligente Stromnetze der Zukunft

Strom entwickelt sich allmählich zu einer kostbaren Ressource. So ist es nicht verwunderlich, dass sich die Verwaltung und Steuerung von Stromnetzen sogenannten Smart Grids zu einem lukrativen Zukunftsmarkt für die IT-Industrie mausert. Für die Endnutzer versprechen Smart Grids eine effizientere Energienutzung und niedrigere Strompreise. Gerade mit der Verbreitung dezentraler Energieerzeugungsanlagen wie etwa Windkraft, Photovoltaik oder Biogas sollte die Nachfrage nach Smart-Grid-Lösungen beziehungsweise entsprechender Technologien steigen. So könnten zum Beispiel digitale Stromzähler die dringend benötigten Daten für die zeitnahe Nachfrage und das aktuelle Angebot an Energie liefern. Aus diesen Informationen ließen sich neuartige Tarifmodelle für Endverbraucher errechnen. Der Konsument hätte dann die Möglichkeit, Nutzungsverträge gemäß seiner Gewohnheiten und Bedürfnisse abzuschließen. Im Bereich Lastenmanagement könnten ebenfalls neue Wege beschritten werden, um Kosten und Schadstoffe für die Energiegewinnung zu reduzieren.

Dem Smart-Grid-Konzept folgende wird in Echtzeit berechnet, wie viel Energie wo und wann entsteht und wie sie am besten gebraucht oder gespeichert wird. Dieser Ansatz ermöglicht es, die ständigen Schwankungen zwischen Angebot und Nachfrage an elektrischer Energie zu regulieren. Hier liegt ein Vergleich zum Cloud-Ansatz der IT nahe, bei dem es unter anderem ja ebenfalls darum geht, Spitzenlasten im Rechenzentrum (RZ) abzufangen und auf andere Data Center zu verteilen. Unsere Schwesterpublikation Computerwoche befragte Manager aus der IT-, der TK- und der Energiewirtschaft dazu, welche Auswirkungen Smart Grids haben und wie Unternehmen davon profitieren können.

1.5.1 Martin Böttner, Echolon: Smart Grids verändern Stromnetze nachhaltig

„Smart Grids werden die Stromnetze hinsichtlich Qualität und Effizienz sowie Administrierbarkeit durch den Energieerzeuger nachhaltig verändern. Die enorme Herausforderung für Smart Grids liegt allerdings in der Einbindung vorhandener Geräte, Gebäude und Anlagen sowie der Zukunftssicherheit und Skalierbarkeit dieser Netze. Bereits heute existieren Lösungen, mit denen sich jeder Betreiber und Hersteller elektronischer Geräte oder Gebäude auf einfache Art und Weise in ein Micro Smart Grid einbinden kann. Darunter verstehen wir das intelligente Stromnetz in der Nachbarschaft. Unsere Plattform ermöglicht beispielsweise den Zugriff über Apps, die auf dem Mobiltelefon hinterlegt sind.

Das Smart Grid stellt ein enormes Wachstumspotenzial für Unternehmen dar. Ähnlich dem Internet oder den Apps für das iPhone können sich neue Dienstleistungen etablieren und Mehrwerte geschaffen werden. Ein höchstinteressantes

Beispiel ist das Energie-Benchmarking, bei dem die Energieeffizienz von Liegenschaften verglichen wird. Derzeit werden in großem Maßstab Energie-Monitoring-Lösungen evaluiert. Diese bilden den ersten Schritt hin zu mehr Transparenz beim Energieverbrauch und zum Energie-Benchmarking."

Martin Böttner, Director EMEA East bei Echolon, einem Lösungsanbieter für intelligente Stromnetze.

„McDonald's hat beispielsweise bereits alle Lieferanten von Küchengeräten angewiesen, ihre Produkte auf Basis unserer Technik kommunikationsfähig zu machen, um damit die Grundlage für die Integration in das Smart Grid und Demand-Response-Konzepte zu schaffen."

1.5.2 Gabriele Riedmann de Trinidad, Deutsche Telekom: Es wird Hunderte von Smart Grids geben

„In einigen Jahrzehnten werden wir mit Smart Grids in der Lage sein, unseren Energiebedarf fast ausschließlich aus erneuerbaren Energien zu decken. Und damit meine ich nicht nur den Strom für Haushalte und Unternehmen, sondern auch die Energie, die wir für unsere Mobilität benötigen. Die Speichertechniken werden so weit entwickelt sein, dass es einen ständigen Stromfluss von Produzenten und Speichern zu Konsumenten gibt – wobei viele Konsumenten auch gleichzeitig Produzenten sein werden."

Gabriele Riedmann de Trinidad, Leiterin Konzerngeschäftsfeld Energie bei der Deutschen Telekom.

„Dieses Szenario mag futuristisch klingen – aber wir müssen heute anfangen, die Technik von morgen zu entwickeln. Ein Smart Grid wird kein in sich geschlossenes

einzigartiges System sein, sondern es wird Hunderte Smart Grids geben. Dieses Stromnetz wird auch mit anderen Netzen kommunizieren – beispielsweise den vernetzten Häusern. Experten sind sich einig, dass Digitalisierung und Vernetzung in allen Lebensbereichen zunehmen werden. Schon bald wird es zum Alltag gehören, aus dem Auto heraus daheim die Heizung einzustellen oder die Jalousien herunterzulassen."

1.5.3 Bernd Grohmann, eQ-3: Herausforderung ist die fehlende Standardisierung

„Smart-Grid-Lösungen sind notwendig, um auch bei massivem Einsatz erneuerbarer Energien eine zuverlässige Stromversorgung sicherzustellen. So werden Smart Grids eine ‚Mikroerzeugung' von Strom überhaupt erst in makroökonomischen Dimensionen beherrschbar machen. In der Öffentlichkeit werden viele Szenarien im Kontext diskutiert, wie Elektronikgeräte im Haushalt künftig mit den Smart Grids interagieren. Für Gerätehersteller entsteht so mittelfristig die Notwendigkeit, sich mit der Smart-Grid-Integration zu beschäftigen. Allerdings bleibt anzumerken: Viele heute publizierte Szenarien sind unrealistisch, weil entweder der Nutzen in der Praxis zu gering wäre oder – was noch häufiger vorkommt – kaum mit Akzeptanz der Anwender zu rechnen ist."

Bernd Grohmann, Bereichsleiter Marketing & Business Development der eQ-3 AG.

„Primär ist Smart Grid ein Thema der Energieerzeuger, das sich aber sehr wohl auch auf andere Branchen auswirken wird. Der Bereich IT und Kommunikation wird von den Milliardenvolumen der Investitionen für Smart Grid profitieren. Den Effekt für die Hersteller von ‚weißer Ware' halten wir aufgrund der langen Beschaffungszeiträume eher für gering. Generell wird der Effekt von Smart Grids auf Gerätehersteller im privaten und gewerblichen Bereich stark von der Gestaltung neuer Stromtarife abhängen. Eine weitere Herausforderung ist die fehlende Standardisierung. Noch schwerer wiegt jedoch die Tatsache, dass die Anforderungen an das Smart Grid, dessen Architektur sowie an Systeme und Protokolle in Smart Grid keinesfalls als ausreichend definiert gelten können. So mutet es schon fast verblüffend an, wenn bestimmte Techniken sich selbst als ‚Gewinner' oder ‚Standard' in Smart Grid deklarieren."

1.5.4 Frank Knauer, HP: von der Telekommunikation lernen

„Beim Smart Metering installieren Netzbetreiber und Versorger Millionen intelligente Zähler und müssen dann gewaltige Datenmengen verarbeiten. Doch die Einführung gestaltet sich häufig aufwendiger als ursprünglich gedacht. Die Lösung ist jenseits der Branchengrenze zu finden: Mobilfunkanbieter haben bereits seit Jahren Infrastrukturen in Betrieb, die auf standardisierten Prozessen und Techniken basieren, die einer Advanced-Meter-Infrastruktur (AMI) entsprechen."

Frank Knauer, Director bei HP Enterprise Business, unter anderem verantwortlich für die Branchen Telekommunikation und Energie.

„Die Parallelen zu dieser Branche sind offensichtlich: Energie- wie Telekommunikationsanbieter verwalten Netze, die für Millionen von Geräten ausgelegt sind. Beide Branchen müssen diese überwachen, den Verbrauch auslesen, Services aktivieren, wechselnde Tarife übertragen und Daten in vielerlei Hinsicht auswerten sowie ihren Verbrauchern bereitstellen. Und beide Branchen benötigen aufgrund fehlender IP-Adressierung eine Spezialsoftware, um die Geräte in ihre IT-Landschaft einzubinden. Deshalb können Versorger die Telekommunikationslösungen fast eins zu eins übernehmen."

1.5.5 Toralv Dirro, McAfee: Smart Grids – neues Ziel für Würmer und Viren?

„Mit der Einführung von Smart Grids ergeben sich große Herausforderungen an die Sicherheit aller Komponenten im System und die Vertraulichkeit der Kundendaten. Schon beim Design muss der Sicherheitsaspekt berücksichtigt werden, denn schließlich könnte das Versagen einzelner Komponenten zum Zusammenbruch des ganzen Stromnetzes führen. Wie so ein Versagen in der Realität aussehen könnte, hat Mike Davis auf der Sicherheitskonferenz Black Hat gezeigt: Durch Sicherheitslücken in einem Kontrollgerät, einem Smart Meter, kann ein Angreifer dieses übernehmen. Sogar die Simulation eines Wurmes, der sich automatisch verbreitet, wurde gezeigt. Um ein derartiges Horrorszenario zu verhindern, wird derzeit viel Mühe in Pläne zur Absicherung gesteckt. Es bleibt nur zu hoffen, dass diese bei der Umsetzung dann nicht kurzfristigem Spareifer zum Opfer fallen."

Toralv Dirro, Security Strategist EMEA bei McAfee.

1.5.6 Michael Spreng, Cirquent: weit größer als das Internet

„Intelligente Energienetze – ein Thema der Energiewirtschaft? Richtig ist: Smart Grids werden Grundbausteine für eine effizientere Energiewirtschaft. Energieversorger stehen vor einer Aufgabe, wie sie Telecom-Unternehmen beim Netzausbau für Internet und Mobilfunk zu meistern hatten."

Dr. Michael Spreng, Berater im Bereich Service-Provider & Utilities bei der IT-Beratung- und Systemintegration Cirquent.

„Doch die Bedeutung von Smart Grids geht über die Energiewirtschaft hinaus. Das Internet erreicht derzeit im Mittel kaum mehr als zwei bis vier Computer oder Smartphones pro Haushalt. Smart Grids werden weit größer sein: Pro Haushalt werden 20, 30 oder mehr elektrische Geräte und Anlagen erreicht, erfasst und gesteuert werden. Dabei wird die Entwicklung der Smart Grids explosionsartig verlaufen – ähnlich wie bei Internet und Mobilfunk. Die Hardware etwa einer Gefriertruhe differenziert nicht – es werden deren Vernetzung und die verbundenen Services sein. Unternehmen, die ein Gerät mit Stromstecker herstellen, sollten sich deshalb vorbereiten."

1.5.7 Matthias von Bechtolsheim, Arthur D. Little: Demokratisierung der Energiewirtschaft

„Smart Grids haben einen dreifachen Nutzen: Sie helfen zunächst, Energie einzusparen (‚Energieeffizienz'). Durch ‚Smart-Home'- beziehungsweise ‚Smart-Building'-Lösungen wird eine intelligente Überwachung und Steuerung von Hei-

zung, Klimaanlagen und Beleuchtung möglich. Damit wird nur so viel Energie verbraucht wie notwendig. Zusätzlicher Komforteffekt: Man kann das ‚Smart Home' via Handy oder Smartphone fernsteuern und wird über Ereignisse wie den Ausfall einer Heizung sofort informiert. Dazu muss der von den Energieversorgern künftig zu installierende Smart Meter zu einem Energie-Management-System ausgebaut werden."

Matthias von Bechtolsheim, Partner bei Arthur D. Little.

„Smart Grids erlauben zudem, das schwankende Stromangebot erneuerbarer Energiequellen wie Windkraft und Photovoltaik effektiver zu nutzen (Lastausgleich). Wichtigste Bausteine des Smart Grids bei der Ausbalancierung von Stromangebot und -nachfrage werden das ‚Lastmanagement' sowie die ‚virtuellen Kraftwerke' sein. Beim Lastmanagement wird die Nachfrage nach Strom an die Zeiten des hohen Stromangebots angepasst: Wenn also der Wind besonders stark weht, wird ein Kühlhaus besonders tief heruntergekühlt, dafür wird die Kühlung bei geringem Windangebot zeitversetzt.

Virtuelle Kraftwerke steuern mehrere dezentrale Stromerzeuger wie KWK (Kraft-Wärme-Kopplung)-Anlagen, Photovoltaikanlagen, Windräder oder Laufwasserkraft so, dass ein stabiles Stromangebot (Bandenergie) entsteht. Der Ökostrom- und Gasanbieter Lichtblick startet mit dem „ZuhauseKraftwerk" einen solchen virtuellen Kraftwerksverbund aus zahlreichen Mikro-KWK-Anlagen.

Unternehmen profitieren durch Smart Grid im Wesentlichen über die Energieeinsparungen sowie über positive Effekte für ihr Nachhaltigkeitsimage. Maßnahmen zur Steigerungen der Energieeffizienz, etwa durch ‚Smart Building', schlagen sich in direkten Kosteneinsparungen nieder. Viele Unternehmen können damit aber auch die Nachhaltigkeit ihres Tuns glaubhaft demonstrieren. So ist es für IT-Dienstleister im Internet wichtig, ihren Usern saubere und nachhaltige Klicks zu bieten. Das Clean Datacenter, betrieben mit Strom aus Brennstoffzellen, die Wasserstoff aus Wind- und Solarenergie nutzen (‚H2BZ'), kann sich langfristig zu einer Killerapplikation im Smart Grid entwickeln, indem der klassische ‚Notstromdiesel' durch H2BZ ersetzt wird. Letztlich ist Smart Grid die Voraussetzung zur ‚Demokratisierung' der Energieversorgung. Verbraucher, private Haushalte wie auch Unternehmen werden zu Energieproduzenten (Prosumer). Zudem entstehen neue Energiedienstleister, die sich auf spezielle Anwendungen im Smart Grid konzentrieren. So hat die Deutsche Telekom Smart Grid bereits als Wachstumsbereich

ausgemacht, es ist Teil der „Strategie 2.0“. Ein Kampf um den Endkunden steht bevor: Wer dem Kunden IT, TK und Smart Meter aus einer Hand liefern kann, bestimmt die Kundenbeziehung und wird dem Kunden dann auch den Strom sowie zusätzliche Dienstleistungen liefern.

Technische Lösungen wie Smart Meters sind derzeit für eine technikaffine Minderheit interessant. Dagegen sind Energieeinsparangebote als ‚selbstfinanzierende Full-Service-Pakete' klar, einfach und verständlich. Sie dürften deshalb einen breiteren Teil der Bevölkerung ansprechen.“

1.5.8 Lars Weber, E.ON Metering: Die gesetzlichen Rahmenbedingungen fehlen

„Gemessen an den Publikationen und Veranstaltungen zu Smart Metern kann man wohl von einem Hype sprechen. Natürlich beflügeln die technischen Möglichkeiten durch Smart Meter die Fantasie der Netzbetreiber, Lieferanten und Kunden. Noch ist jedoch unklar, welche gesetzlichen Rahmenbedingungen in der Praxis Anwendung finden werden. Daran wird sich letztlich aber der technische Standard orientieren. Fällt dieser eher bescheiden aus, werden viele jetzt diskutierte Möglichkeiten so nicht realisierbar sein.“

Lars Weber, Geschäftsführer der E.ON Metering GmbH.

„Smart Meter nur als Hype zu sehen wäre jedoch zu kurz gegriffen. Auf dem Weg zu einer nachhaltigen Energiewirtschaft sehen wir die Smart Meter mit den dazugehörigen Systemen und Prozessen als notwendige Voraussetzung. Nur durch sie wird es gelingen, variable Tarife und die dezentrale Erzeugung in das Energieversorgungssystem zu integrieren und damit Einspeisung und Verbrauch optimal zu synchronisieren. Eine Energiewirtschaft 2.0 ist ohne Smart Meter nicht denkbar.“

1.5.9 Dirk Pfefferle, Verizon Business: keine Zukunft ohne intelligente Stromnetze

„Der Nachhaltigkeitsgedanke moderner Geschäftsmodelle erfordert innovative Ansätze beim Energieverbrauch. Für Firmen- und Privatkunden erfindet sich die

Energiebranche quasi neu; intelligente Stromnetze sind daran wesentlich beteiligt. Damit sich Smart Grids umsetzen lassen, müssen zahlreiche Voraussetzungen erfüllt sein: von enormem Planungsaufwand über Inbetriebnahme neuer Telekommunikationsnetze und Datenverwaltungsmodelle sowie innovative Konzepte für die Netzsicherheit bis hin zur Aktualisierung der Geschäftsprozesse der Energiewirtschaft. Größte Herausforderung ist die Finanzierung und die Frage, wie man die Verbraucher überzeugt – beides hängt zusammen."

Dirk Pfefferle, Geschäftsführer Verizon Business in Deutschland.

„Der Nutzen intelligenter Stromnetze für Gemeinwesen und Versorger ist klar: Am meisten profitiert die Umwelt. Der Verbraucher will zudem greifbare Vorteile, etwa eine niedrigere Stromrechnung. Doch dies ist eher der zweite Schritt, denn die Investitionen in Smart Grids dominieren zunächst das Bild. Jeder verbraucht Strom, deshalb ist das Tempo, mit dem intelligente Stromnetze realisiert werden, ein Thema, das jeden angeht – nicht nur die Energieproduzenten."

1.5.10 Sepp Lausch, Juniper Networks: Der Aufbau ist ein Mammutaufgabe

„Smart Grid ist ein Großprojekt, das in Umfang und Dauer vielleicht mit der Etablierung des Internets vergleichbar ist. Dementsprechend hohe Anforderungen werden auch an die Technik gestellt: Aufgrund der Vielzahl an Geräten, Generatoren, Zwischenstationen, Überwachungs- und Kontrollzentren, die alle miteinander interagieren, muss das Netz Interoperabilität und Offenheit bieten, gerüstet sein für Erweiterungen und enorme Belastungen, aber auch resistent gegenüber Cyber-Attacken.

Sepp Lausch, Area Director Enterprise bei Juniper Networks.

„Da die Folgen einer eventuellen Unterbrechung der Stromversorgung sehr schwerwiegend sein können, haben die Zuverlässigkeit und die Sicherheit des Netzes die höchste Priorität. Entsprechende Erfahrungen haben Netzhersteller bereits im Umgang mit Technologien wie IP und MPLS gesammelt."

1.5.11 Ed Davalos, AT&T: Smart Grids brauchen intelligente TK-Netze

„Die Diskussionen über Smart Grids beschränken sich häufig auf Stromnetze und Stromversorgungsunternehmen. Dabei stammt die Technik, die die Netze ‚intelligent' macht, aus der TK-Branche. Erst in Kombination mit einer Advanced-Metering-Infrastruktur (AMI) entstehen intelligente Stromnetze, die den Verbrauch einzelner Geräte autark an den Zeitpunkt koppeln, zu dem die meiste Energie im Netz vorhanden ist. Die AMI basiert auf automatisierten Kommunikationslösungen, die in Echtzeit Daten zwischen den Stromversorgern und den einzelnen Verbrauchern über Wireless-Netze übertragen. Für die Daten muss darüber hinaus eine ausreichende Kapazität gewährleistet sein. Um der steigenden Nachfrage nachzukommen, skalieren Carrier zudem ihre Kapazitäten. Allein wir haben 2009 rund 18 Milliarden Dollar in den Ausbau unserer Netze investiert. Smart Metering ist der erste Schritt zum Smart Grid. Wir entwickeln bereits weitere Anwendungen, die Smart Grids noch ‚intelligenter' gestalten."

Ed Davalos, Director Utility/Smart Grid bei AT&T.

1.5.12 Richard Hausmann, Siemens: intelligente Netze ohne Komforteinbuße

„Eine wachsende Bevölkerung, die Weiterentwicklung von Schwellenländern sowie neue Anwendungsbereiche für Strom tragen weltweit zu einem steigenden Verbrauch bei. Dazu kommt der Ausbau der stark schwankenden erneuerbaren Energien. Es ist an der Zeit, die Stromnetze gründlich zu optimieren – denn ein ‚intelligentes' Netz kann die nötigen milliardenschweren Investitionen deutlich reduzieren. Derzeit sind die Netze auf den Spitzenverbrauch am Tage ausgelegt und nachts nur gering ausgelastet. Gelingt es uns, den Energieverbrauch gleichmäßiger zu gestalten, können die Stromnetze effizienter dimensioniert werden."

Dr. Richard Hausmann, Siemens AG Sektor Energy, CEO und Leiter des Company Project Smart Grid Applications.

„Das Smart Grid braucht Anwendungen, die wir mit unserer Erfahrung über die gesamte Energiekette mitgestalten wollen – für intelligente Netze ohne Komforteinbuße. Wir haben deshalb das Konzernprojekt ‚Smart Grid Applications' ins Leben gerufen, dessen Leiter ich bin. Akkus von Elektroautos können in nur einer Stunde geladen werden, und dem Fahrer ist es egal, um welche Uhrzeit dies nachts geschieht. Intelligente Steuersysteme werden den optimalen Ladezeitraum ermitteln. Viele weitere Geräte kommen als Smart-Grid-Lösungen infrage wie Wärmepumpen, elektrische Warmwasserboiler und Nachtspeicherheizungen sowie Kühl- und Gefrierschränke. Wann diese Strom verbrauchen, ist dem Besitzer gleichgültig, Hauptsache, er hat warmes Wasser, die Heizung hält das Haus warm und die Lebensmittel bleiben kühl."

Jürgen Hill

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation Computerwoche.

Jürgen Hill ist Redakteur bei unserer Schwesterzeitschrift Computerwoche und dort für Produkte & Technologien zuständig.

TecChannel-Links zum Thema	Webcode	Compact
Smart Grids Intelligente Stromnetze der Zukunft	2035308	S.39
Ratgeber – Alles was Sie über IPv6 wissen sollten	2035716	S.9
Ratgeber – Anforderungen an professionelle DSL-Router	2035759	S.17
Breitband für alle – Zugangstechnologien im Überblick	2035913	S.25
Ratgeber – Faxen übers Internet	2035270	S.33

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

2 Infrastruktur

Die wachsenden Ansprüche an Geschwindigkeit, Verfügbarkeit und Flexibilität von Netzwerken schlagen sich nieder in den immer höheren Anforderungen an die jeweilige Infrastruktur. Die sechs Praxisbeiträge in diesem Kapitel geben IT-Managern und Administratoren leicht nachvollziehbare Arbeitsanleitungen zur Einrichtung und Anpassung von Netzwerkressourcen an die Hand.

2.1 Workshop – IMAP-Server Dovecot installieren und konfigurieren

Wenn Benutzer ihren Mail-Client starten und Mails empfangen, kommen diese von einem sogenannten Mail-Transfer-Agent entweder über einen POP3- oder einen IMAP-Server. Dort meldet sich ein Mail-Client an, der Mail-Server bestätigt die Identität des Nutzers, die Liste der Nachrichten wird heruntergeladen, und der Benutzer kann sie lesen. POP3- und IMAP-Server haben demzufolge nichts mit dem Versand von E-Mails, sondern lediglich mit dem Empfang zu tun. Für den Versand ist der Mail-Transfer-Agent zuständig. Das bedeutet: Bevor Sie sich an die Installation und Konfiguration des IMAP-Servers machen, bringen Sie den Mail Transfer Agenten zum Laufen. In Debian und Ubuntu ist das üblicherweise Exim, in openSUSE wird meist Postfix verwendet. Erst danach kommt der IMAP-Server dran. Der Linux- und Unix-Server Dovecot (www.dovecot.org) unterstützt IMAP rev1 und POP3; IPv6, SSL und TLS werden ebenfalls genutzt.

Der Server wird hauptsächlich mit Linux, Solaris, FreeBSD, OpenBSD, NetBSD und Mac OS X eingesetzt. Laut seinem finnischen Entwickler Timo Sirainen hat Dovecot auch sonst gleich mehrere Vorteile: Er sei schnell, einfach aufzusetzen und benötige wenig Speicher. Dovecot unterstützt die Standard-Mailbox-Formate mbox und Maildir. Die Indexierung erfolgt relativ transparent, und der Server ist kompatibel zu vorhandenen Mailbox-Tools. Der Version 1.1.5 und darüber wird als einem von drei IMAP-Servern die volle Konformität bescheinigt, im Gegensatz zu weitaus bekannteren wie Cyrus, Courier und Microsoft Exchange. Die Indexdateien der Mailboxen optimieren sich während der Laufzeit selbst, und der Server behebt Probleme wie unterbrochene Indexdateien ebenso selbstständig. Auftretende Probleme loggt der Server in verständlichen Meldungen mit; sie erscheinen standardmäßig in der Datei */var/log/syslog*.

Auf die Mailboxen und Indexdateien kann man von vielen Computern gleichzeitig zugreifen und diese ändern. Postfix- und Exim-Nutzer können für den Mail-Versand und darüber hinaus für die SMTP-Authentifizierung direkt auf das Dovecot-Backend zugreifen, ohne dass eine separate Konfiguration erforderlich ist. Über Plugins kann der Server erweitert werden, um so neue Kommandos hinzuzufügen. Verschiedene Funktionen wie *Quota* und *ACL*-Unterstützung sind vollständig in

Plugins ausgelagert. Dovecot ist laut Sirainen speziell auf Sicherheit ausgelegt. Der Finne ist von seinem Produkt so überzeugt, dass er dem Ersten 1.000 Euro zahlen will, der eine Sicherheitslücke findet.

2.1.1 Dovecot installieren

In Ubuntu und Debian gibt es insgesamt sechs Pakete zu Dovecot, von denen aber nur eines für die Installation benötigt wird: für den POP3-Server das Paket *dovecot-pop3d* und für den IMAP-Server, dessen Installation im Folgenden erläutert wird, das Paket *dovecot-imapd*. Während der Installation werden drei Konfigurationsdateien angelegt:

- /etc/dovecot/dovecot-ldap.conf
- /etc/dovecot/dovecot-sql.conf
- /etc/dovecot/dovecot.conf

Die Datei */etc/dovecot/dovecot.conf* enthält eine Beispielkonfiguration; dafür fehlt in den Ubuntu- und Debian-Paketen die in der Dokumentation erwähnte und in anderen Distributionen vorhandene dovecot-example.conf. Ist die Datei im Verzeichnis */etc/dovecot* nicht vorhanden, kopieren Sie diese aus dem Verzeichnis */usr/share/dovecot*. Die Datei */etc/dovecot/dovecot.conf* ist auch die erste, die man anpassen muss. Öffnen Sie diese Datei daher in einem Editor. Die Datei enthält bereits alle Programmparameter. Diese sind zunächst allerdings größtenteils auskommentiert, weil es sich jeweils um die Standardvorgaben handelt. Damit Dovecot ordnungsgemäß startet, müsste der Benutzer lediglich in der Zeile mit dem Parameter „protocols“ das Kommentarzeichen löschen und anschließend das Kommando */etc/init.d/dovecot start* aufrufen. Doch eventuell wollen Sie noch verschiedene weitere Werte in der Konfiguration anpassen.

2.1.2 Protokoll festlegen

Ganz wichtig ist es, das vom Dovecot-Server verwendete Protokoll festzulegen. Für einen IMAP-Server schreiben Sie in die */etc/dovecot/dovecot.conf* die Zeile:

```
protocols = imap imaps
```

```
# Base directory where to store runtime data.
#base_dir = /var/run/dovecot/

# Protocols we want to be serving: imap imaps pop3 pop3s managesieve
# If you only want to use dovecot-auth, you can set this to "none".
#protocols = imap imaps
protocols = imap imaps
```

Editieren: Ziemlich am Anfang der Konfigurationsdatei /etc/dovecot/dovecot.conf steht die „protocols“-Zeile. Tragen Sie hier das Gewünschte ein.

Trennen Sie die Protokolle mit einem Leerzeichen, nicht mit Komma. Falls Sie auch POP3 nutzen wollen, fügen Sie das Protokoll einfach hinzu. Anschließend können Sie Dovecot mit */etc/init.d/dovecot start* starten und testen, ob der IMAP-Server am Port 143 auf Verbindungen horcht:

```
# telnet localhost 143
Trying 127.0.0.1...
Connected to localhost.localdomain
Escape character is '^]'.
* OK Dovecot ready.
```

Funktioniert das nicht, prüfen Sie die „protocols"-Einstellung und stellen sicher, dass *listen=** in der Konfiguration steht, Dovecot also auf jedem Port horcht. Klappt alles, testen Sie die Verbindung von einem entfernten Rechner aus mit *telnet HOST 143*. Klappt das nicht, prüfen Sie, ob zwischengeschaltete Firewalls den Port sperren. Die sichere IMAPS-Verbindung testen Sie mit dem Befehl:

```
# openssl s_client -connect localhost:993
```

Von einem entfernten Rechner schreiben Sie anstelle von *localhost* den Host-Namen des IMAP-Servers. Der Befehl prüft darüber hinaus, ob Dovecot die SSL-Zertifikate korrekt erhält. Prüfen Sie danach, ob ein Login möglich ist.

```
# telnet localhost 143
a login username password
```

Anstelle von *username* und *password* setzen Sie einen vorhandenen Benutzernamen samt Passwort ein. Wenn Sie stattdessen ein *Authentication failed* erhalten, stellen Sie in der Konfigurationsdatei */etc/dovecot/dovecot.conf* die Parameter *auth_verbose = yes* und *auth_debug = yes* ein, starten Dovecot neu und versuchen es abermals. Jetzt sollte die Log-Datei genügend Informationen enthalten, um das Problem zu lösen.

Denken Sie daran, nach der Prüfung die Parameter wieder abzuschalten. Erhalten Sie stattdessen einen Alarm, dass das Passwort in Plaintext übertragen wird, schalten Sie in der Dovecot-Konfiguration um auf *disable_plaintext_auth = no*.

2.1.3 Wo sich die Mails befinden

Wenn das Protokoll geklärt ist, prüfen Sie im nächsten Schritt mit telnet, ob Dovecot die Inbox erkennt:

```
# telnet localhost 143

Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^]'.
* OK Dovecot ready.
```

```
a login username password
a OK Logged in.
b select inbox
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft Old
➥ $Forwarded NonJunk Junk $MDNSent receipt-handled)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen
➥ \Draft Old $Forwarded NonJunk Junk $MDNSent
➥ receipt-handled \*)] Flags permitted.
* 233 EXISTS
* 15 RECENT
* OK [UIDVALIDITY 1260711131] UIDs valid
* OK [UIDNEXT 87093] Predicted next UID
b OK [READ-WRITE] Select completed.
```

Erscheint nach *b select inbox* stattdessen die Meldung *NO Internal error [<date> <time>]*, kann das mehrere Gründe haben:

- Die Benutzerdatenbank enthält eine UID-Nummer für den Benutzer, die nicht dem Besitzer der Mail-Dateien entspricht.
- Wenn Sie LDAP nutzen, beachten Sie, dass die Datei */etc/dovecot/dovecot-ldap.conf* eine UID-Einstellung enthält, die nicht dem Besitzer der Dateien mit den Mails entspricht.
- Die Mail-Dateien des Benutzers sind nicht in dem Verzeichnis, das in der Dovecot-Konfiguration mit *mail_location* gesetzt wurde.

Die einfachste Methode, der Ursache auf den Grund zu kommen ist: Setzen Sie in der Konfiguration *mail_debug = yes* und versuchen es erneut. Anschließend sollte der Befehl *c list "" ** in telnet auch weitere bereits vorhandene Mailboxen anzeigen. Werden diese angezeigt und sind trotzdem im Mail-Client keine zu sehen, so liegt es am Mail-Client.

2.1.4 Mailboxen automatisch erkennen

Dovecot kann die Mailboxen automatisch erkennen. Das funktioniert aber nur, wenn ein Benutzer bereits Mails in der Inbox hat. Sollte das nicht der Fall sein oder wollen Sie weitere Optionen nutzen, konfigurieren Sie das mithilfe der Einstellung *mail_location*. Hier werden üblicherweise die folgenden Variablen verwendet:

- %u: vollständiger Benutzername
- %n: der Benutzername aus user@domain (identisch mit %u, wenn dort keine Domain angegeben ist)
- %d: Domain-Teil in user@domain (leer, wenn keine Domain vorhanden)

Für eine Maildir-Mailbox wird normalerweise folgende Einstellung benutzt:

```
mail_location = maildir:~/Maildir
```

Für das mbox-Format ist die folgende Einstellung typisch:

```
mail_location = mbox:~/mail:INBOX=/var/mail/%u
```

In beiden Beispielen werden das Mail-Format, der Ordner im Home-Verzeichnis und für *mbox* das Spool-Verzeichnis angegeben. Die Indexdateien werden üblicherweise im selben Verzeichnis gespeichert wie die Mails – für *maildir* in den aktuellen Mail-Verzeichnissen, für *mbox* im versteckten .imap-Verzeichnis. Das kann man ändern, indem man *:INDEX=location* hinzufügt, etwa so:

```
mail_location = mbox:~/mail:INBOX=/var/mail/%u
➥ :INDEX=~/imap-indexes
```

Nun sollte vonseiten Dovecots alles funktionieren. Wenn Sie sich mit einem Mail-Client nicht mit dem IMAP-Server verbinden können, liegt die Ursache vermutlich beim Mail-Client. Hier sollten Sie zunächst die SSL/TLS-Einstellungen prüfen. Stellen Sie sicher, dass der Client die Plaintext-Authentisierung nutzt, sofern Sie Dovecot nicht explizit anders konfiguriert haben. Falls der Client nur den Posteingang anzeigt, prüfen Sie, ob der Client vielleicht so eingestellt ist, dass er nur abonnierte Mailboxen anzeigt. In dem Fall sollten Sie die gewünschten noch abonnieren. Welche Mailboxen Sie abonniert haben, zeigt Ihnen telnet mit *d lsub "" **.

2.1.5 In Datei loggen

Standardmäßig loggt Dovecot seine Aktivitäten in die Datei */var/log/syslog*. Möchten Sie stattdessen eine eigene Datei benutzen, ändern Sie in der Datei */etc/dovecot/dovecot.conf* die Variablen *log_path* und *info_log_path*, etwa so:

```
log_path: /var/log/dovecot/error.log
info_log_path: /var/log/dovecot/info.log
```

Anschließend müssen Sie noch das Verzeichnis erzeugen und dessen Benutzerrechte festsetzen:

```
# mkdir /var/log/dovecot
# chown dovecot:adm /var/log/dovecot
# chmod 2755 /var/log/dovecot
```

Damit diese Verzeichnisse nicht überlaufen und eventuell den Festplattenplatz verschlingen, lassen Sie die Log-Dateien rotieren. Das erledigt das Programm *logrotate*. Im Verzeichnis */etc/logrotate.d* ist aufgeführt, welche Log-Dateien regelmäßig rotiert werden. Legen Sie dort die Datei */etc/logrotate.d/dovecot* an, um auch Dovecots Log-Dateien in die Rotation aufzunehmen. Die Datei kann zum Beispiel folgenden Inhalt haben:

```
/var/log/dovecot/error.log /var/log/dovecot/info.log {
daily
missingok
rotate 60
```

```
compress
delaycompress
notifempty
create 640 dovecot adm
sharedscripts
postrotate
if [ -f /var/run/dovecot/master.pid ]; then
/bin/kill -USR1 'cat /var/run/dovecot/master.pid'
fi
endscript
}
```

2.1.6 Authentifizierung des Benutzers testen

Wenn via Telnet der Login fehlschlägt und den Versuch mit der Meldung *NO Authentication failed* quittiert, gibt es dafür mehrere Gründe:

- Der Benutzer steht nicht in der Benutzerdatenbank.
- Der Benutzer steht in der Benutzerdatenbank, hat aber kein Passwort.
- Wenn Sie LDAP verwenden, ist in der pass_attrs-Einstellung in der Datei */etc/dovecot/dovecot-ldap.conf* kein Passwort spezifiziert.
- Sie haben den Benutzernamen und/oder das Passwort falsch geschrieben.

Mehr erfahren Sie, wenn Sie die Einstellung *auth_verbose = yes* in der Dovecot-Konfiguration einschalten. Erhalten Sie anstelle der oben genannten Meldung den Fehler *NO Login failed: Unsupported authentication mechanism*, sollten Sie die Einstellung *auth_mechanisms = plain* für jeden Authentifizierungsvorgang einschalten.

```
webserver:~# dovecot -n
# 1.0.15: /etc/dovecot/dovecot.conf
log_timestamp: %Y-%m-%d %H:%M:%S
login_dir: /var/run/dovecot/login
login_executable: /usr/lib/dovecot/imap-login
mail_privileged_group: mail
auth default:
  passdb:
    driver: pam
  userdb:
    driver: passwd
webserver:~#
```

Auflistung: Dovecot mit dem Parameter „-n“ aufgerufen, listet alle Variablen und Argumente, die nicht den Standardvorgaben entsprechen.

Die geläufigste Methode zur Authentifizierung für existierende Systemnutzer ist PAM (Pluggable Authentication Modules). Mit virtuellen Benutzern wird meist LDAP, eine SQL-Datenbank oder eine *passwd*-Datei benutzt. Auch für den Konfigurationstest kann man zunächst eine Passwortdatei *passwd.dovecot* anlegen mit nur der folgenden Zeile:

```
benutzer:passwort
```

Anstelle von *benutzer* und *passwort* geben Sie Ihren Nicht-Root-Benutzernamen ein sowie irgendein einfaches Passwort, das nur zum Testen verwendet wird. Bedenken Sie, dass das Passwort unverschlüsselt übertragen wird; wählen Sie daher nicht Ihr eigentliches Passwort. Danach ändern Sie die Konfigurationsdatei */etc/dovecot/dovecot.conf*. Fügen Sie im Bereich hinter *auth default* die drei Zeilen hinzu:

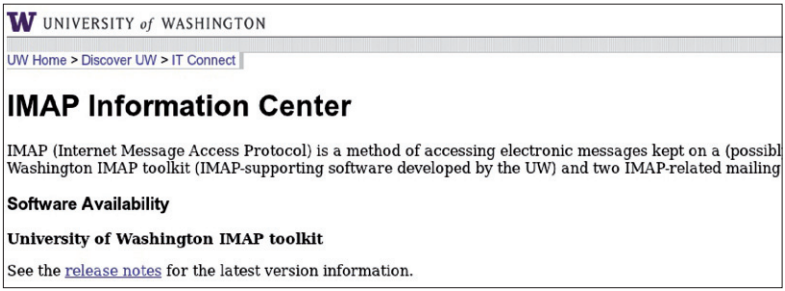
```
passdb passwd-file {
args = /etc/passwd.dovecot
}
```

Kommentieren Sie anschließend noch den Bereich *passdb pam* aus, damit die PAM-Authentifizierung nicht unnötigerweise versucht wird. Stellen Sie außerdem den Parameter *disable_plaintext_auth = no* ein, um die Plaintext-Authentifikation zu ermöglichen. Denken Sie aber daran, diese nach den Tests auf den Standardwert zurückzustellen. Nach dem Speichern der Konfiguration sollte *dovecot -n* nun unter anderem diese Ausgabe liefern:

```
auth default:
passdb:
driver: passwd-file
args: /etc/passwd.dovecot
userdb:
driver: passwd
```

2.1.7 Von anderen IMAP-Servern umsteigen

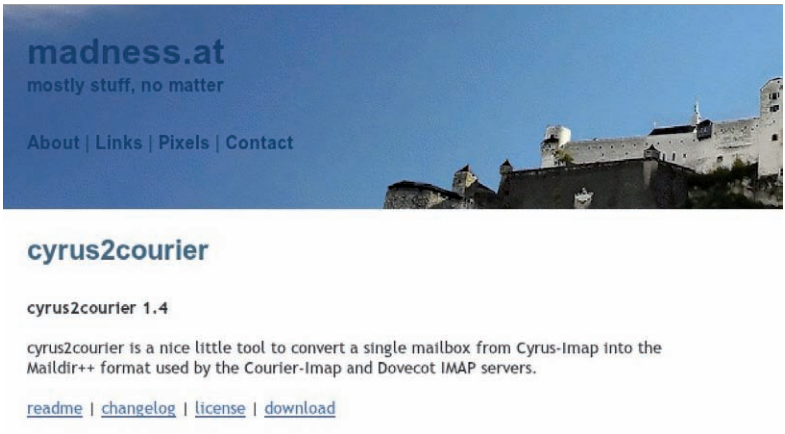
Wer von anderen IMAP-Servern zu Dovecot wechselt, muss ein paar Dinge berücksichtigen. So erlaubt etwa UW-IMAP (www.washington.edu/imap/) den Zugriff auf das gesamte Home-Verzeichnis. Viele Nutzer speichern daher ihre Mails im mail/-Verzeichnis und haben das auch als *mail/* im Client eingestellt. Dovecot hat damit Probleme, denn es interpretiert dies als *~/mail/mail/*. Das kann man abstellen, indem man die Vorgabe im Client entfernt.



Referenz: UW-IMAP, der IMAP-Server der Universität von Washington, gilt als Referenzserver.

Ein weiteres Problem mit UW-IMAP: Abonnierte Mailboxen sind als mail/box, *~/mail/box oder ~user/mail/box* in der versteckten Datei *.mailboxlist* aufgeführt. Entfernen Sie den mail/-Teil und benennen Sie die Datei anschließend um: Dovecot nutzt die versteckte Datei *.subscriptions*. Für UW-POP3 muss für Dovecot ein Patch verwendet werden (http://dovecot.org/patches/).

Courier (www.courier-mta.org/imap/) nutzt INBOX als privaten IMAP-Namensraum und bereitet ähnliche Probleme wie UW-IMAP. Die Datei *courierimapsubscribed* ist kompatibel zu Dovecots *.subscriptions*-Datei. Benennen Sie diese um und ersetzen darin die INBOX-Präfixe. Die Datei courierimapuiddb ist ebenfalls kompatibel zu Dovecot; Sie müssen sie lediglich in *dovecot-uidlist* umbenennen. Inkompatibel hingegen sind Couriers Nachrichten-Keywords, und es gibt auch keine einfache Migrationsmöglichkeit.



Konverter: Mit dem kleinen Tool cyrus2courier von Alexander Marx kann man Cyrus-Mailboxen ins Maildir-Format übertragen.

Mailboxen von Cyrus können mithilfe des Tools cyrus2courier (http://madness.at/projects/) einzeln ins Maildir-Format übertragen werden und sind damit Dovecot-kompatibel.

2.1.8 Pfade in Mutt und Pine einstellen

Mutt ist einer der beliebtesten Mail-Clients für die Konsole. Das Programm kann mit IMAP umgehen, es müssen lediglich die folgenden zwei Anweisungen in die versteckte Datei .muttrc geschrieben werden:

```
set spoolfile=imap://hostname/INBOX
set folder=imap://hostname/
```

```
## You probably don't really care to know about deleted attachments.
attachments   -A message/external-body
attachments   -I message/external-body

# enable mime lookup by extension
mime_lookup application/octet-stream

##
# See /usr/share/doc/mutt/README.Debian for details.
source /usr/lib/mutt/source-muttrc.d

# IMAP-Zugang
set spoolfile=imap://imapserver.net/INBOX
set folder=imap://imapserver.net/
~
```

Kommunikativ: Nur zwei Änderungen an der Konfigurationsdatei von Mutt sind notwendig, damit der Konsolen-Mail-Client mit einem IMAP-Server kommunizieren kann.

Passen Sie *hostname* entsprechend an. Anschließend können Sie Mutt neu starten und auf die IMAP-Mail-Ordner zugreifen.

Wer den Mail-Client Pine einsetzt und den Pfad zur Inbox auf entfernten Servern setzen will, muss das in der versteckten Datei .pinerc erledigen. Die Kommentare darin schlagen folgende Schreibweise vor:

```
inbox-path={imapserver.tld}INBOX
```

Passen Sie den Domainnamen und die Toplevel-Domain an. Wenn Ihr IMAP-Server SSL oder TLS unterstützt, fügen Sie */ssl* oder */tls* an den Servernamen an, etwa *imapserver.tld/tls*. Sie können auch gleich noch den Benutzer mit übergeben: *imapserver.tld/tls/user=toni*.

Thomas Hümmler

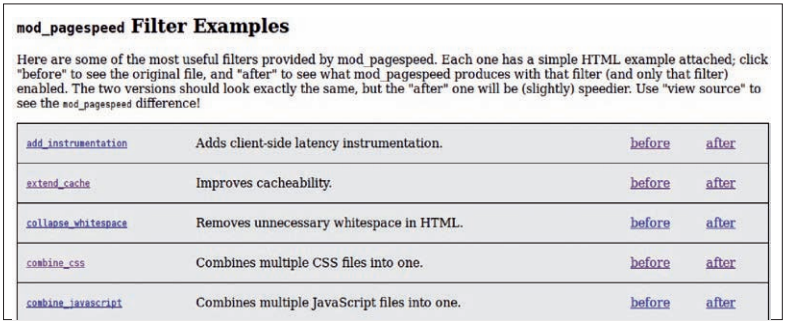
Thomas Hümmler ist freiberuflicher Journalist und beschäftige sich mit Betriebssystemen, Office-Anwendungen, freier Software, dem Internet und anderen IT- und Technik-Themen.

TecChannel-Links zum Thema	Webcode	Compact
Workshop – IMAP-Server Dovecot installieren und konfigurieren	2036025	S.49
Workshop – Apache HTTP-Server beschleunigen	2035748	S.58
Workshop – Thin Clients im Netzwerk einrichten	2035848	S.66
Workshop – Debian 6 übers Netzwerk installieren und einrichten	2035240	S.74
Workshop – Debian 6 übers Netzwerk installieren und einrichten	2033715	S.81
Versteckte Funktionen in der Fritz!Box nutzen	2035528	S.88

2.2 Workshop – Apache HTTP-Server beschleunigen

Cloud-Dienstanbieter haben ein enormes Interesse an schnellem Internet. Das ist aber nicht nur abhängig von der Leitung und der sogenannten letzten Meile, sondern auch von der Konfiguration des HTTP-Servers, der die Anfragen entgegennimmt, an interne Mail-Server oder Datenbanken weiterleitet und die Antworten an den Browser des Benutzers ausliefert. Dabei ist es egal, ob die Anfragen aus dem internen Netzwerk oder von außerhalb kommen.

Was extern für Geschwindigkeit sorgt, kann intern nicht verkehrt sein – eigentlich. Wenn aber eine Site im Inter- oder Intranet extrem langsam ist, kann das auch an der Konfiguration des HTTP-Servers liegen. Das wird umso ärgerlicher, je mehr Programme einen HTTP-Server in Anspruch nehmen: Telefonanlagensoftware und Streaming-Programme bis hin zum Virtualisierungs-Hypervisor laufen im internen Netz darüber – ganz zu schweigen von SaaS-Produkten (Software-as-a-Service) und jeder weiteren webbasierten Software.



mod_pagespeed Filter Examples

Here are some of the most useful filters provided by mod_pagespeed. Each one has a simple HTML example attached; click "before" to see the original file, and "after" to see what mod_pagespeed produces with that filter (and only that filter) enabled. The two versions should look exactly the same, but the "after" one will be (slightly) speedier. Use "view source" to see the mod_pagespeed difference!

add_instrumentation	Adds client-side latency instrumentation.	before	after
extend_cache	Improves cacheability.	before	after
collapse_whitespace	Removes unnecessary whitespace in HTML.	before	after
combine_css	Combines multiple CSS files into one.	before	after
combine_javascript	Combines multiple JavaScript files into one.	before	after

Vorher und nachher: Wie sich die Filter auf die Geschwindigkeit auswirken, zeigen die Beispiele auf der Seite www.modpagespeed.com.

Um Apache flotter zu machen, hat Google vor gut einem halben Jahr das Open-Source-Modul „mod_pagespeed“ veröffentlicht. Es soll Webseiten so beschleunigen, dass sie mit bis zu doppelter Geschwindigkeit im Browser des Benutzers ankommen – auf http://code.google.com/p/modpagespeed/ ist ein Video zu sehen, das den beschleunigten Seitenaufbau verdeutlichen soll.

Dabei nutzt das Modul verschiedene Filter, um die auszuliefernden Daten zu minimieren: Das Caching werde verbessert, CSS- und Javaskript-Daten würden reduziert, HTML-Header zusammengefasst und Bilder abermals komprimiert – unter http://www.modpagespeed.com/ sind zahlreiche Beispiele für die unterschiedlichen Filter zu finden.

2.2.1 mod_pagespeed-Filter beschleunigt den Datenverkehr

Das *mod_pagespeed*-Modul gibt auf der Seite http://code.google.com/intl/de-DE/speed/page-speed/download.html zum Download. Es ist für den Apache 2.2 programmiert und derzeit für Debian, Ubuntu und CentOS beziehungsweise Fedora (jeweils als 32- und 64-Bit-Version) verfügbar. Unter Debian und Ubuntu wird es auf einer Konsole mit dem Befehl:

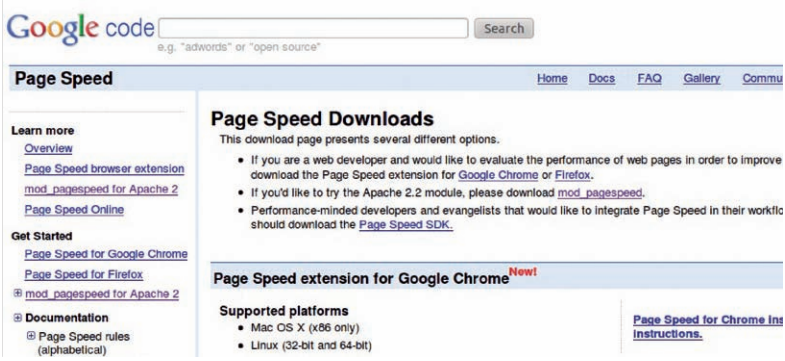
```
dpkg -i mod-pagespeed-*.deb
apt-get -f install
```

installiert (in Ubuntu müssen Sie ein „*sudo*“ voranstellen). In CentOS und Fedora führen Sie folgende Befehle als root aus:

```
yum install at
rpm -U mod-pagespeed-*.rpm
```

Die erste Zeile ist nur erforderlich, wenn Sie den Befehl „at“ noch nicht installiert haben. Insgesamt werden damit vier Dateien installiert:

- das Apache-Modul */usr/lib/apache2/modules/mod_pagespeed.so*,
- die Cron-Datei */etc/cron.daily/mod-pagespeed*,
- die Datei */etc/apache2/mods-available/pagespeed.load* und
- die Datei */etc/apache2/mods-available/pagespeed.conf*.



Download: Auf der Projektseite findet man das Modul fertig zum Herunterladen für Debian, Ubuntu, CentOS und Fedora.

Nach der Installation muss der HTTP-Server einmal neu gestartet werden mit dem Befehl */etc/init.d/apache2 restart* (*sudo* in Ubuntu voranstellen). Danach arbeitet das pagespeed-Modul bereits. Das Apache-Modul macht die eigentliche Arbeit. Es speichert die Daten, die der HTTP-Server ausliefert, in den Verzeichnissen

/var/mod_pagespeed/cache und */var/mod_pagespeed/files* zwischen. Die Cron-Datei */etc/cron.daily/mod-pagespeed* richtet das Google-Repository für eventuelle Paket-Updates ein. Diese Funktion kann der Debian-Benutzer zudem selbst kontrollieren, indem er die Datei */etc/default/mod-pagespeed* erzeugt. Hier kann er zwei Variablen verwenden: *repo_add_once* und *repo_reenable_on_distupgrade*. Diese sind für ein Distributions-Update gedacht, bei dem die Repositories auf Debian-Standards gesetzt werden. Setzt er beide Parameter auf *true*, wird das Google-Repository automatisch wieder als Datenquelle eingerichtet.

2.2.2 Weniger Daten ausliefern mit dem Deflate-Modul

Die Datei */etc/apache2/mods-available/pagespeed.load* lädt das Apache-Module *mod_deflate.so*, falls dies noch nicht geschehen ist. Das Deflate-Modul komprimiert Serverdaten mithilfe der Programmbibliothek zlib, bevor sie über das Netzwerk an den Client gesendet werden. Es kann in der Serverkonfiguration oder auch in Konfigurationsabschnitten für virtuelle Hosts eingerichtet werden. Insgesamt gibt es für das Deflate-Modul fünf sogenannte Direktiven:

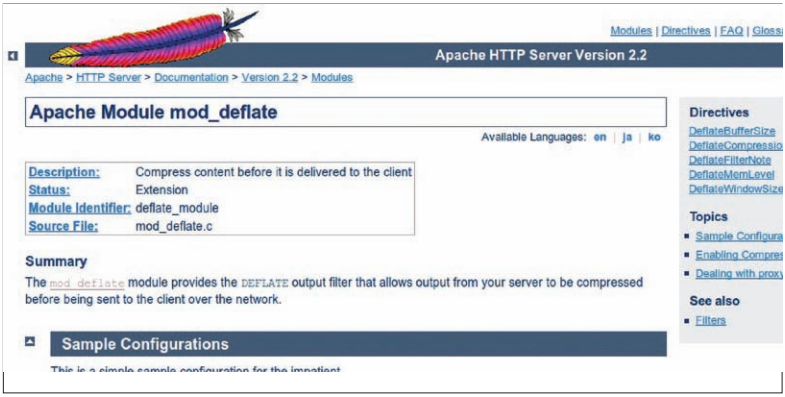
- **DeflateBufferSize:** Mit dieser Direktive wird die Größe der Fragmente bestimmt, die zlib auf einmal komprimiert. Die Vorgabe ist 8096.
- **DeflateCompressionLevel:** Hier wird festgelegt, wie hoch die zlib-Kompression sein soll. Voreingestellt ist die zlib-Standardkompression. Es können Werte zwischen 1 (geringe Kompression) und 9 (höchste Kompression) gewählt werden. Beachten Sie, dass eine höhere Kompression auch mehr Rechenzeit beansprucht. Die Direktive kann ab der Apache-Version 2.0.45 verwendet werden.
- **DeflateFilterNote:** Mit dieser Direktive kann der Administrator sehen, wie hoch die Kompressionsrate ist. Denn das Ergebnis wird mit in die Logdateien des HTTP-Servers geschrieben und kann statistisch ausgewertet werden.
- **DeflateMemLevel:** Diese Direktive legt fest, wie viel Speicher von zlib für die Kompression genutzt werden soll. Möglich sind Werte von 1 bis 9, die Vorgabe ist 9.
- **DeflateWindowSize:** Für diese Direktive sind Werte von 1 bis 15 möglich. Die Vorgabe ist 15. Generell gilt laut Apache-Dokumentation: Je höher der Wert, desto höher ist die zu erwartende Kompressionsrate.

2.2.3 Deflate-Modul konfigurieren

Nicht jeder Browser kann mit komprimierten Inhalten umgehen. Darüber hinaus ist es nicht sinnvoll, komprimierte Daten wie etwa Bilder noch weiter zu komprimieren. Diesem kann man mit der Konfiguration des Deflate-Moduls Rechnung tragen. Die Zeile:

```
AddOutputFilterByType DEFLATE text/html text/plain text/xml
```

etwa sorgt dafür, dass nur die MIME-Typen *text/html*, *text/plain* und *text/xml* komprimiert werden.



Luft rauslassen: Mit Hilfe des Deflate-Moduls wird Platz in HTML-Dateien geschaffen. Die Dokumentation steht unter http://httpd.apache.org/docs/2.2/mod/mod_deflate.html.

Die folgende Konfiguration aus der Apache-Dokumentation komprimiert hingegen alles außer Bilder.

```
<Location />
# Insert filter
SetOutputFilter DEFLATE

# Netscape 4.x has some problems...
BrowserMatch ^Mozilla/4 gzip-only-text/html

# Netscape 4.06-4.08 have some more problems
BrowserMatch ^Mozilla/4\.0[678] no-gzip

# MSIE masquerades as Netscape, but it is fine
# BrowserMatch \bMSIE !no-gzip !gzip-only-text/html

# NOTE: Due to a bug in mod_setenvif up to Apache 2.0.48
# the above regex won't work. You can use the following
# workaround to get the desired effect:
BrowserMatch \bMSI[E] !no-gzip !gzip-only-text/html

# Don't compress images
SetEnvIfNoCase Request_URI \
\.(?:gif|jpe?g|png)$ no-gzip dont-vary
```

```
# Make sure proxies don't deliver the wrong content
Header append Vary User-Agent env=!dont-vary
</Location>
```

In der Zeile mit *SetOutputFilter DEFLATE* wird die Kompression aktiviert. Fordert nun ein Netscape-4.x-Browser Daten an, werden nur solche vom Typ *text/html* komprimiert. An die Netscape-Browser 4.06, 4.07 und 4.08 werden überhaupt keine komprimierten Daten ausgeliefert. In der zweitletzten Anweisung steht schließlich, dass Daten mit den Endungen *.gif*, *.jpg*, *.jpeg* und *.png* nicht komprimiert werden sollen. Wer darüber hinaus noch einen Proxyserver einsetzt, benötigt auch die letzte Anweisung, damit keine falschen Daten ausgeliefert werden. Sie können die Kompression auch einfach für bestimmte MIME-Typen vorgeben. Die Zeilen

```
<Directory "/your-server-root">
AddOutputFilterByType DEFLATE text/html
</Directory>
```

beispielsweise komprimieren im Server-Root-Verzeichnis und den darunterliegenden Verzeichnissen alle HTML-Dateien, lassen aber die anderen wie Bilder und Dokumente unberücksichtigt.

2.2.4 Kompressionsrate mitloggen

Wie oben erwähnt, dient die Direktive DeflateFilterNote dazu, die Kompressionsrate in die Logdateien zu schreiben. Apache gibt in der Serverdokumentation ein Beispiel dafür:

```
DeflateFilterNote ratio
LogFormat '"%r" %b (%{ratio}n) "%{User-agent}i"' deflate
CustomLog logs/deflate_log deflate
```

Wer noch akkurater protokollieren möchte, kann mithilfe der Parameter *Input* und *Output* in der Konfigurationsdatei auch die Byteanzahl vor und nach dem Komprimieren mitschreiben lassen:

```
DeflateFilterNote Input instream
DeflateFilterNote Output outstream
DeflateFilterNote Ratio ratio
LogFormat '"%r" %{outstream}n/%{instream}n
➥ (%{ratio}n%%)' deflate
CustomLog logs/deflate_log deflate
```

Damit erhält der Administrator einen guten Überblick, welche Daten wie hoch komprimiert ausgeliefert werden. Übrigens: Der Parameter *Ratio* ist der Vorgabewert und muss aus dem Grund im ersten Beispiel nicht angegeben werden.

2.2.5 Pagespeed-Modul konfigurieren

In der Datei */etc/apache2/mods-available/pagespeed.conf* wird das Google-Pagespeed-Modul konfiguriert. Es wird zwischen eine IfModule-Direktive gestellt. Innerhalb der If-Abfrage können zwei Routinen aufgerufen werden, die Statistiken liefern: *mod_pagespeed_statistics* und *mod_pagespeed_beacon*. Die erste Routine zeigt Serverstatistiken, aus denen man die Latenzzeit berechnen kann, um so die Effizienz verschiedener Beschleunigungsmethoden zu messen. Will man auf diese Statistiken verzichten, ist das Kommentarzeichen in der Zeile

```
# ModPagespeedStatistics off
```

zu löschen.

```
    # Uncomment the following line if you want to disable statistics entirely.
    #
    # ModPagespeedStatistics off

    # This page lets you view statistics about the mod_pagespeed module.
    <Location /mod_pagespeed_statistics>
        Order allow,deny
        # You may insert other "Allow from" lines to add hosts you want to
        # allow to look at generated statistics.  Another possibility is
        # to comment out the "Order" and "Allow" options from the config
        # file, to allow any client that can reach your server to examine
        # statistics.  This might be appropriate in an experimental setup or
        # if the Apache server is protected by a reverse proxy that will
        # filter URLs in some fashion.
        Allow from localhost
        SetHandler mod_pagespeed_statistics
```

Keine Statistik, bitte! Um die Auswertung abzuschalten, entfernen Sie hier das Kommentarzeichen.

Ein wichtiger Teil der Konfiguration ist die Anweisung *ModPagespeedRewriteLevel*. In der Voreinstellung sind hier die sogenannten Core-Filter eingeschaltet, also die folgenden neun der insgesamt 21 Filter:

- **add_head:** Fügt ein head-Tag im HTML-Code hinzu, falls es vor einem body-Tag keinen findet (der Filter bereitet nach Entwickleraussagen keine Probleme).
- **combine_css:** Kombiniert unter bestimmten Voraussetzungen mehrere CSS-Dateien zu einer (Javaskript in Kombination mit link-Einträgen kann sich fehlerhaft verhalten).
- **extend_cache:** Fügt in URL-Referenzen einen Hash-Wert ein, sodass sich die URL ändert, sobald die Ressource geändert wird. So wird alter Inhalt im Browser-Cache nicht erneut referenziert (Javaskript-Code, der bestimmte Dateinamen erwartet, kann zu anderen Ergebnissen führen).
- **inline_css:** Fügt kleine externe CSS-Daten direkt in den HTML-Code ein (kann mit link- oder style-Tags Probleme bereiten).

- **inline_javascript:** Fügt kleine externe Javaskript-Daten direkt in den HTML-Code ein (kann mit script-Tags Probleme bereiten, die sowohl src-Attribute als auch Inline-Daten enthalten).
- **rewrite_css:** Checkt verlinkte und Inline-CSS-Daten und minimiert das CSS in style-Blöcken und link-Referenzen (kann zu Problemen mit schlecht kodierten CSS führen, auch mit Javaskript-Code, der exakte URLs verlangt).
- **rewrite_images:** Entfernt unter anderem Metadaten wie Copyright-Informationen aus den Bildern (der Filter bereitet nach Entwickleraussagen keine Probleme). rewrite_images ruft auch noch die Filter insert_image_dimensions (fügt width- und height-Attribute hinzu), inline_images (ersetzt kleinere Bilder durch data-URLs), recompress_images (entfernt Metadaten und wandelt gif- in png-Dateien um) und resize_image (ändert die Bildgröße, wenn im img-Tag kleinere Werte für width und height stehen) auf.
- **rewrite_javascript:** Minimiert Javascript-Code, indem Leerzeichen, Tabulatoren und Kommentare entfernt werden (dieser Filter wird als riskant betrachtet und ist daher standardmäßig nicht eingeschaltet).
- **trim_urls:** Kürzt URLs aus scr- oder href-Attributen relativ zur Basis (der Filter bereitet nach Entwickleraussagen keine Probleme).

2.2.6 Filterfunktionen nutzen

Wollen Sie einen der Filter nicht nutzen, schalten Sie ihn mithilfe der Anweisung *ModPagespeedDisableFilters* aus. Als Argumente geben Sie hier einen oder – mit Kommata getrennt – mehrere Filter an:

```
ModPagespeedDisableFilters
➥ rewrite_javascript,inline_javascript
```

```
<IfModule pagespeed_module>
    # Turn on mod_pagespeed. To completely disable mod_pagespeed, you
    # can set this to "off".
    ModPagespeed on

    # Direct Apache to send all HTML output to the mod_pagespeed
    # output handler.
    AddOutputFilterByType MOD_PAGESPEED_OUTPUT_FILTER text/html

    # The ModPagespeedFileCachePath and
    # ModPagespeedGeneratedFilePrefix directories must exist and be
    # writable by the apache user (as specified by the User
    # directive).
    ModPagespeedFileCachePath           "/var/mod_pagespeed/cache/"
    ModPagespeedGeneratedFilePrefix     "/var/mod_pagespeed/files/"

    # Override the mod_pagespeed 'rewrite level'. The default level
```

Handarbeit: Wollen Sie das Pagespeed-Modul abschalten, genügt es, hier ein „off“ zu setzen.

Möchten Sie umgekehrt weitere Filter zuschalten, nutzen Sie die Anweisung *ModPagespeedEnableFilters*. Die Beschreibung der übrigen Filter finden Sie in der Dokumentation unter http://code.google.com/intl/de-DE/speed/page-speed/docs/filters.html. Bevor Sie einen Filter einschalten, lesen Sie die dortige Dokumentation unbedingt. Denn es wird beispielsweise standardmäßig der resize_image-Filter eingeschaltet, was zu extrem hohen CPU-Lasten führen kann. Wird es zu viel, reduzieren Sie den Wert in der Anweisung *ModPagespeedImageMaxRewritesAtOnce* auf einen Voreinstellungswert unter acht, etwa:

```
ModPagespeedImageMaxRewritesAtOnce 4
```

Wer das Pagespeed-Modul nicht mehr nutzen und abschalten möchte, muss das Paket übrigens nicht löschen. Es genügt, die Anweisung

```
ModPagespeed on
```

zu Anfang der Konfiguration auf *off* zu setzen. Tipp: Das Pagespeed-Modul können Sie auch über Directory-Direktiven oder mithilfe von *.htaccess*-Dateien auf bestimmte Verzeichnisse eingrenzen. Denken Sie aber immer daran, nach Änderungen der Konfiguration diese neu zu laden oder den Apache neu zu starten

Thomas Hümmler

Thomas Hümmler ist freiberuflicher Journalist und beschäftige sich mit Betriebssystemen, Office-Anwendungen, freier Software, dem Internet und anderen IT- und Technik-Themen.

TecChannel-Links zum Thema	Webcode	Compact
Workshop – Apache HTTP-Server beschleunigen	2035748	S.58
Workshop – IMAP-Server Dovecot installieren und konfigurieren	2036025	S.49
Workshop – Thin Clients im Netzwerk einrichten	2035848	S.66
Workshop – Debian 6 übers Netzwerk installieren und einrichten	2035240	S.74
Workshop – Debian 6 übers Netzwerk installieren und einrichten	2033715	S.81
Versteckte Funktionen in der Fritz!Box nutzen	2035528	S.88

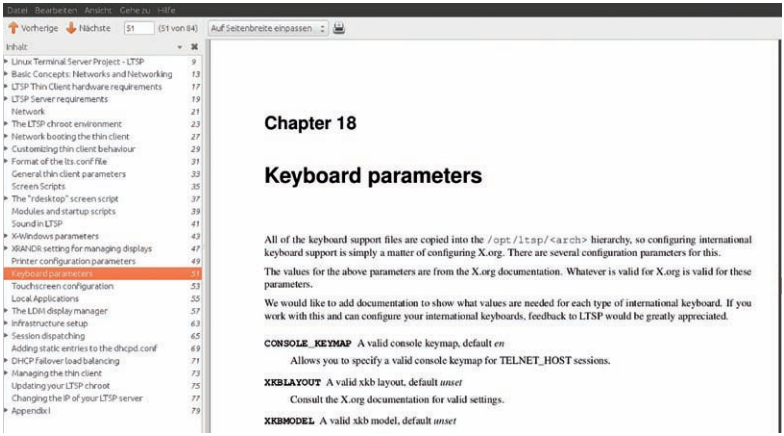
Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

2.3 Workshop – Thin Clients im Netzwerk einrichten

Ein Terminal-Server, etwa in Form des Linux Terminal Server Projects, ist für Administratoren eine feine Sache. Denn alle Anwendungen laufen intern auf dem Server. LTSP nutzt dazu die Fähigkeiten des grafischen X-Servers, ein Linux-Programm in die Programmausführung und die Anzeige zu trennen. Die am Server per Netzwerk angeschlossenen Clients benötigen deshalb auch keine Festplatten; sie zeigen im Prinzip nur, was auf dem Server passiert. Alle Daten werden daher auch direkt auf dem Server gespeichert und nicht über das Netzwerk an die einzelnen Clients verteilt. Dementsprechend sollte der Server als Grundvoraussetzung über genügend Systemleistung verfügen.

Dabei ist die Server-CPU gar nicht so wichtig, vielmehr kommt es auf schnelle und ausreichend große Festplatten sowie genügend Arbeitsspeicher an. Wer IDE oder langsame SATA-Platten einsetzt, sollte maximal zehn Clients bedienen. Sind mehr Clients vorgesehen, greift man besser zu schnellen SATA- oder SAS-Festplatten, denn diese sollten mit 20 Clients fertig werden.

Der Arbeitsspeicher des Servers sollte aber möglichst groß sein. Hierbei werden allgemein (Ubuntu-Users-Wiki) 256 MByte für den Server und 128 MByte pro Client empfohlen; ein Server für 20 Clients benötige dementsprechend 1 GByte Arbeitsspeicher. Realistischer scheinen die Angaben im LTSP-Manual zu sein: 256 MByte plus 192 MByte pro Client – macht insgesamt 4 GByte für 20 Clients. Bei den Festplatten empfiehlt das Manual schnelle SATA-Disks, außerdem ein RAID vom Typ 1 für den schmalen und vom Typ 10 für den größeren Geldbeutel.



Wichtige Hilfe: das 84-seitige Handbuch „Administrator's Reference", das Sie auf https://sourceforge.net/projects/ltsp/files/Docs-Admin-Guide/LTSPManual.pdf/download herunterladen können.

Als Server-CPU für ein Netzwerk mit bis zu 20 Clients ist ein 3-GHz-Prozessor ausreichend, so das Manual. Für größere Netzwerke liefert eine Dual-Core-CPU die erforderliche Performance. Aufseiten der Clients sind die Anforderungen wesentlich geringer. Hier tun es bereits eine 533-MHz-CPU sowie 256 MByte Arbeitsspeicher – mehr ist hier natürlich in beiden Fällen besser. Wichtig ist, dass die Netzwerkkarte per PXE – beziehungsweise mit Yaboot für Macintosh-PowerPC-Rechner – übers Netzwerk booten kann. LTSP ist in allen gängigen Linux-Distributionen von CentOS bis openSUSE enthalten. Auch in Debian und Ubuntu ist es dabei. Es gibt sogar zwei Ubuntu-Versionen, mit denen Sie schon während der Installation einen LTSP-Server aufsetzen können: Die eine ist Edubuntu (www.edubuntu.org), eine Ubuntu-Distribution für den Einsatz in Schulen. Die andere ist die sogenannte Alternate-Installations-CD (http://releases.ubuntu.com/releases/11.04/). Wer Ubuntu von dieser anstelle der sonst üblichen Desktop-CD installiert, kann sofort eine LTSP-Umgebung aufsetzen, indem er im Installationsbildschirm die Funktionstaste *F4* drückt und anschließend *Install an LTSP Server* wählt. Wer LTSP nachträglich installieren will, ist damit auch schnell durch. Man benötigt lediglich eines der beiden Serverpakete ltsp-server oder ltsp-server-standalone. Das erste Paket erzeugt eine minimale Serverumgebung, das andere eine vollständige. Die Minimalvariante verzichtet auf Openssh- und DHCP-Server und überlässt den Bootstrap der Clients einem externen DHCP-Server.

2.3.1 Schritt 1: Grundinstallation

Doch auch mit einem andernorts vorhandenen DHCP-Server, etwa einer Fritz!-Box, kann man den vollständigen LTSP-Server aufsetzen. Sie benötigen dazu die folgenden Pakete:

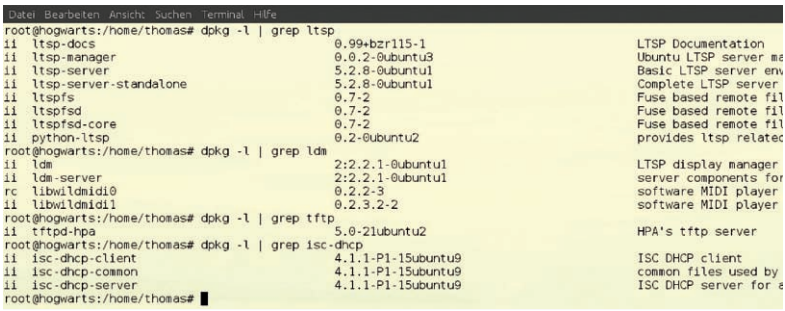
- **ltsp-server-standalone:** den LTSP-Server mit Open-SSH- und nbd-server
- **ltspfsd, ltspfs und ltspfsd-core:** ein entferntes Dateisystem, um zum Beispiel USB-Sticks und DVD-Laufwerke an den Thin Clients nutzen zu können
- **ltsp-manager:** ein GUI-Werkzeug, um einen LTSP-Server aufzusetzen, zu modifizieren und zu verwalten (nicht zwingend erforderlich)
- **ltsp-docs:** die Dokumentation für LTSP (nicht zwingend erforderlich)
- **ldm und ldm-server:** den LTSP-Displaymanager und die Serverkomponenten für den LTSP-Displaymanager
- **tftpd-hpa:** das Trivial-File-Transfer-Protokoll TFTP, das dafür sorgt, dass den Thin Clients das entsprechende Bootimage übers Netzwerk angeboten wird
- **isc-dhcp-server und isc-dhcp-client:** den DHCP-Server und -Client des Internet Software Consortiums

Installieren Sie die Pakete mithilfe des Befehls apt-get, also etwa:

```
sudo apt-get install ltsp-server-standalone
```

Wenn Sie unter Debian installieren, brauchen Sie den *sudo*-Befehl nicht voranstellen. Manche Pakete installieren einige der genannten bereits mit, sodass diese Pakete bereits auf dem Server vorhanden sein können. Welche das sind, überprüfen Sie mit dem Befehl *dpkg* wie folgt:

```
dpkg -l | grep ltsp
```



Alles installiert: Mithilfe des dpkg-Kommandos stellen Sie fest, was vorhanden ist und was noch fehlt.

Der Befehl listet alle Pakete auf, in deren Namen oder Beschreibung die Zeichenfolge *ltsp* auftaucht. Dass die Pakete installiert sind, erkennen Sie an den beiden *ii* zu Anfang einer Zeile. Wichtig: Schreiben Sie *ltsp* und nicht *LTSP*, denn *grep* arbeitet kontextsensitiv mit regulären Ausdrücken und unterscheidet zwischen Groß- und Kleinschreibung.

Sind alle Pakete installiert, wird die LTSP-Netzwerk-Umgebung auf dem Server erzeugt. Dazu starten Sie in einer Konsole den Befehl

```
sudo ltsp-build-client
```

Damit erzeugen Sie je nach Serverarchitektur die Umgebung entweder im Verzeichnis */opt/ltsp/i386 oder /opt/ltsp/amd64*; Sie finden in diesen Ordnern die erforderliche Linux-Dateistruktur sowie alle benötigten Befehle und Einstellungen. Wichtig: Beachten Sie, dass viele Thin Clients 32-Bit-Rechner sind und Sie daher die entsprechende Umgebung benötigen. Ist Ihr Server selbst ein 64-Bit-Rechner etwa mit einem Dual- oder Quad-Core-Prozessor, müssen Sie die gewünschte Architektur für die LTSP-Umgebung noch mit angeben:

```
sudo ltsp-build-client --arch i386
```

Nun wird eine Verbindung zu den Repositories hergestellt, und die für die LTSP-Umgebung erforderlichen Pakete werden heruntergeladen und anschließend installiert. Jetzt müssen Sie nur noch mit dem Befehl

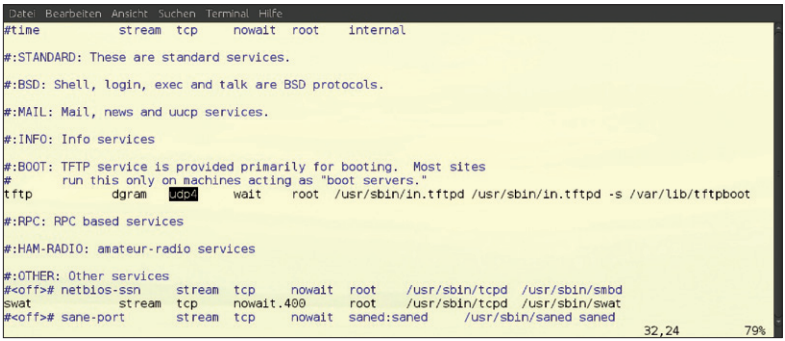
```
sudo ltsp-update-sshkeys
```

die aktuellen LTSP-Serverkeys in die Chroot-Umgebung des Clients installieren. Übrigens: Diesen Befehl wird auch dann benötigt, wenn sich später einmal die IP-Adresse des Servers ändern sollte.

Hinweis: Wollen Sie eine grafische Desktop-Umgebung wie Gnome, KDE oder XFCE nutzen, müssen Sie diese auf dem LTSP-Server installieren – sonst startet später auf den Thin Clients keine grafische Umgebung.

2.3.2 Schritt 2: Trivial-File-Transfer-Protokoll (TFTP)

Das Trivial-File-Transfer-Protokoll – kurz TFPT – wird in Ubuntu über den sogenannten Inet-Superserver gestartet. Es dient hauptsächlich dazu, Kernel-Images über das Netzwerk anderen Maschinen zur Verfügung zu stellen. Der in Ubuntu benutzte tftpd-hpa-Server basiert auf dem BSD-TFTP-Server, hat aber gegenüber dem Original einige Verbesserungen und Bugfixes erfahren.



Ganz wichtig: In der Konfiguration des Internet-Superservers muss udp4 beim TFTP-Service stehen.

Damit der TFTP-Server funktioniert, müssen Sie zwei Dinge kontrollieren und gegebenenfalls ändern: In der Konfigurationsdatei */etc/inetd.conf* des Inet-Superservers muss der Eintrag

```
tftp dgram udp4 wait root /usr/sbin/in.tftpd /usr/sbin/in.
➥ tftpd -s /var/lib/tftpboot
```

vorhanden sein. Achten Sie in Ihrer Installation besonders auf die *4* hinter *upd* – die muss dort stehen. Des Weiteren benötigen Sie die Datei */etc/default/tftpd-hpa* mit folgendem Inhalt:

```
TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/var/lib/tftpboot"
TFTP_ADDRESS="0.0.0.0:69" TFTP_OPTIONS="-l -s"
```

Die Variable *TFTP_DIRECTORY* weist auf das Verzeichnis mit dem Kernel-Image der LTSP-Umgebung hin. Nach den Änderungen müssen Sie den TFTP-Server neu starten mit

```
service tftpd-hpa restart
```

Der einfache Weg zur korrekten Konfigurationsdatei: Ändern Sie die /etc/default/tftpd-hpa mit dem Kommando dpkg-reconfigure.

Tipp: Anstatt die Datei direkt zu editieren, können Sie auch Debians Paketkonfiguration nutzen mit dem Befehl:

```
sudo dpkg-reconfigure -plow tftpd-hpa
```

2.3.3 Schritt 3: DHCP konfigurieren

Ein DHCP-Server verteilt IP-Adressen an die angeschlossenen Clients. Über diese sind die Rechner eines Netzwerks zu erreichen. Wer beispielsweise einen Internet-Router wie die Fritz!Box einsetzt, bekommt den DHCP-Server schon einsatzbereit mitgeliefert. Der hauptsächliche Vorteil: Man muss sich um die Konfiguration des Netzwerkadapters nicht mehr kümmern, das geschieht automatisch.

Es können auch mehrere DHCP-Server innerhalb eines Netzwerks genutzt werden: etwa einer, der nur die IP-Adressen verteilt, und einer, der die Informationen vorhält, wo Clients das Boot-Image für die LTSP-Umgebung finden. Das Gute dabei: Man muss die Konfiguration des ersten DHCP-Servers nicht ändern und nur den neuen für LTSP anpassen. Zuerst stellen Sie in der Datei */etc/default/isc-dhcp-server* ein, über welchen Netzwerkadapter der DHCP-Server seine Dienste anbietet. Dazu passen Sie lediglich die *INTERFACES*-Zeile an, etwa:

```
INTERFACES="eth1"
```

Die Konfiguration des DHCP-Servers für LTSP passen Sie in der Datei */etc/ltsp/dhcpd.conf* an. Diese hat beispielsweise folgenden Inhalt:

```
authoritative;
subnet 192.168.178.0 netmask 255.255.255.0 {
```

```
range 192.168.178.20 192.168.178.200;

option domain-name "hogwarts.huemmler.de";
option domain-name-servers 192.168.178.1;
option broadcast-address 192.168.178.255;
option routers 192.168.178.1;

next-server 192.168.178.52;

option subnet-mask 255.255.255.0;
option root-path "/opt/ltsp/i386";

if substring( option vendor-class-identifier, 0, 9 ) =
➥ "PXEClient" {
filename "/ltsp/i386/pxelinux.0";
} else {
filename "/ltsp/i386/nbi.img";
}
}
```

Für Ihr Netzwerk müssen Sie zumeist nur die folgenden Parameter anpassen:

- **subnet:** Hier steht die Adresse des Netzwerk, häufig etwa 192.168.178.0 oder 192.168.1.0.
- **range:** die kleinste und die höchste IP-Adresse innerhalb eines Subnetzes, die zugewiesen werden kann
- **option domain-name:** Hier tragen Sie den Namen Ihres Netzwerks ein.
- **option domain-name-servers:** der DNS-Server im Netzwerk (meist wie das Subnetz, nur mit „1“ am Ende)
- **option broadcast-address:** die Broadcast-Adresse (meist wie das Subnetz, nur mit „255“ am Ende)
- **option routers:** die Adresse des Routers (oft die IP-Adresse mit „1“ am Ende)
- **next-server:** Hier tragen Sie die IP-Adresse des LTSP-Servers ein.
- **option root-path:** der Pfad zur LTSP-Umgebung

Haben Sie gemischte Umgebungen mit 32- und 64-Bit-Clients, muss die DHCP-Konfiguration entsprechend erweitert werden, etwa so:

```
group {
next-server 192.168.1.1;
server-name "192.168.1.1";
use-host-decl-names on;

host alice {
option root-path "/opt/ltsp/i386";
filename "/ltsp/i386/pxelinux.0";

# MAC-Adresse des Client-Rechners
```

```
hardware ethernet 00:e0:4c:c8:de:ad;

# IP-Adresse, welche zugewiesen wird
fixed-address 192.168.1.32;
}

host bob {
option root-path "/opt/ltsp/amd64";
filename "/ltsp/amd64/pxelinux.0";
hardware ethernet 00:16:36:10:b3:61;
fixed-address 192.168.1.33;
}
}
```

```
# Der Server hat die IP 192.168.1.1, und und legt ausserdem den DNS,
# den Router und das TFTP- und das LTSP-Verzeichnis fest.

option domain-name "domainname.net";
option domain-name-servers dns.com;
option broadcast-address 192.168.1.255;
option routers 192.168.1.1;
option subnet-mask 255.255.255.0;
authoritative;
allow booting;
allow bootp;

group {
  next-server 192.168.1.1;
  server-name "192.168.1.1";
  use-host-decl-names on;
  host alice {
    # Pfad zum Wurzelverzeichnis des zu bootenden Systems
    option root-path "/opt/ltsp/i386";
    # Pfad zum TFTP-Verzeichnis (relativ zur TFTP-Konfiguration)
    filename "/ltsp/i386/pxelinux.0";
    # MAC-Adresse des Client-Rechners
    hardware ethernet 00:e0:4c:c8:de:ad;
    # IP-Adresse, welche zugewiesen wird
    fixed-address 192.168.1.32;
    }
  host bob {
    option root-path "/opt/ltsp/amd64";
    filename "/ltsp/amd64/pxelinux.0";
```

Hilfreich: Im Ubuntu-Users-Wiki steht beschrieben, wie man die DHCP-Server an verschiedene Client-Architekturen anpassen kann.

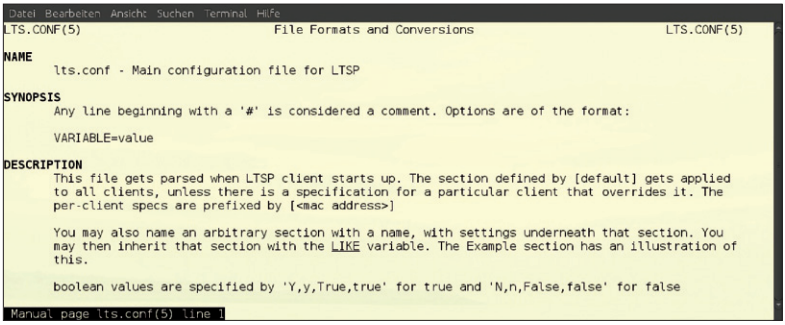
In diesem Beispiel aus dem Ubuntu-Wiki werden zwei Rechner – *alice* und *bob* – definiert und zu einer Gruppe zusammengefasst. Beide Rechner erhalten außerdem eine feste IP-Adresse und werden über die MAC-Adresse des Netzwerkadapters eindeutig erkannt; das sorgt dafür, dass nur diese sich mit dem LTSP-Server verbinden können. Ist der DHCP-Server konfiguriert, starten Sie ihn anschließend neu mit dem Kommando

```
sudo /etc/init.d/isc-dhcp-server restart
```

2.3.4 Thin Clients im Netzwerk starten

Nun können Sie die Thin Clients starten. Festplattenlose Thin Clients booten zumeist per PXE-Boot direkt über das Netzwerk und greifen auf das Boot-fähige Image auf dem LTSP-Server zu. Achten Sie deshalb darauf, dass im BIOS der Clients das Booten per Netzwerk eingestellt ist. Danach sollte der grafische Login erscheinen – falls nicht, achten Sie auf die Meldungen in der Datei */var/log/syslog*.

Ein etwas kurioses Problem kann es beim Login geben. Wenn Sie zum Beispiel einen falschen Benutzernamen oder ein falsches Passwort eingeben, meldet der Login-Screen „Antwort des Servers", aber es passiert nichts weiter, und Sie erhalten keinen Zugang. Das liegt daran, dass die Meldung nicht vollständig angezeigt wird: Sie lautet nämlich normalerweise „Keine Antwort des Servers" und soll Sie auf eine falsche Eingabe hinweisen. Haben Sie Name und Passwort korrekt eingegeben, erhalten aber trotzdem keinen Zugriff? Dann benutzen Sie eventuell deutsche Umlaute oder andere Sonderzeichen im Passwort. Der grafische Anmeldeschirm am Thin Client nutzt zunächst die englische Tastaturbelegung. Dort befinden sich die meisten Sonderzeichen an anderen Stellen.



Weitere Arbeiten: In der ausführlich gehaltenen Manpage lts.conf wird gut erklärt, etwa wie man verschiedene Thin Clients konfiguriert.

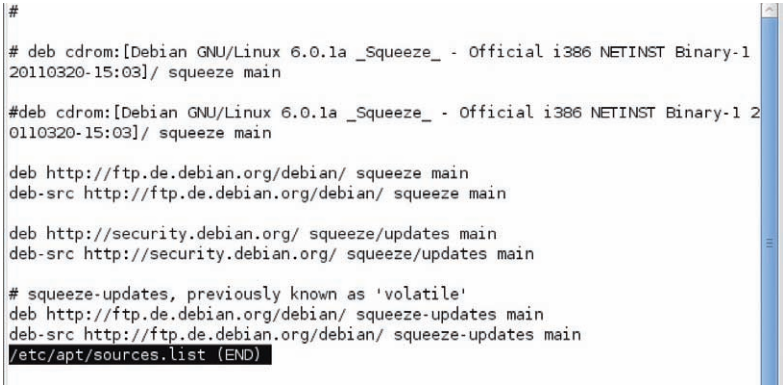
Läuft so weit alles, können Sie die Thin Clients noch weiter speziell an Ihre Anforderungen beziehungsweise Netzwerkumgebung anpassen. Das machen Sie in der Datei */var/lib/tftpboot/ltsp/i386/lts.conf* beziehungsweise */var/lib/tftpboot/ltsp/amd64/lts.conf*. Welche Parameter erlaubt sind, steht in der Manpage *lts.conf*.

Auf diese greifen Sie zu, wenn Sie das Paket *ltsp-docs* installiert haben. Um Fehler zu vermeiden, passen Sie die Konfiguration aber nur schrittweise an. Damit ist unsere Basisinstallation zum Betreiben von Thin-Clients im Netzwerk abgeschlossen. Weitere Informationen zur LTSP-Installation finden Sie auf der LTSP-Homepage und im Ubuntu-Wiki.

Thomas Hümmler

2.4 Workshop – Debian 6 übers Netzwerk installieren und einrichten

Jede neue Version eines Betriebssystems sollte man erst einmal die anderen installieren lassen. Das gilt für Windows genauso wie für Linux. Denn anfangs werden schnell noch Fehler gefunden, manchmal gravierende. Davor ist auch Debian GNU/Linux 6 nicht gefeit, obwohl es als eine der stabilsten Linux-Distributionen gilt. Seit Ende März gibt es nun die fehlerbereinigte Version 6.0.1a – und damit endlich auch eine gesunde Basis für ein Debian-Serversystem. Debian 6 – auch „Debian Squeeze" benannt nach den dreiäugigen Gummi-Aliens aus dem Film „Toy Story" – bietet dem Nutzer mehr als 29.000 freie Softwarepakete.



Auswahl: In die Datei /etc/apt/sources.list tragen Sie die Non-free-Bereiche als Paketquellen ein.

Zum ersten Mal liefert das Projekt nun auch einen vollständig freien Linux-Kernel 2.6.32 aus – das bedeutet, proprietäre Linux-Firmware-Dateien wurden in separate Pakete ausgelagert. Der Benutzer findet sie nun auch nicht mehr im „Debian-main-Archiv"; stattdessen haben die Entwickler die nicht quelloffenen Pakete in den non-free-Bereich verlagert. Der muss, um genutzt zu werden, nachträglich als Archiv aktiviert werden. Dazu editiert der Administrator die Datei */etc/apt/sources-list* und fügt den *non-free*-Bereich in die Zeilen

deb http://ftp.de.debian.org/debian/ squeeze main non-free,

deb http://security.debian.org/ squeeze/updates main non-free oder

deb http://ftp.de.debian.org/debian/ squeeze-updates main non-free

ein. Falls bereits während der Installation Firmware-Dateien benötigt werden, können diese, wie aus früheren Versionen gewohnt, nachgeladen werden. In diesem Workshop zeigen wir, wie Sie die aktuelle Debian-6.0.1a-Distribution mittels der Netzwerkinstallationsversion schnell und problemlos einrichten.

2.4.1 Freie Auswahl für unterschiedliche Einsatzzwecke

Das Debian-Betriebssystem gibt es derzeit für neun verschiedene Rechnerarchitekturen vom Palmtop bis zum Supercomputer. Debian 6 bietet darüber hinaus zwei Portierungen als sogenannte Technologievorschau mit einem FreeBSD-Kernel an. Dies sind die ersten Portierungen innerhalb einer Debian-Veröffentlichung, die nicht auf dem Linux-Kernel basieren. Die Entwickler haben sich dafür entschieden, weil FreeBSD allgemeine Serversoftware „sehr stark" unterstütze und die Debian-Funktionalitäten „mit einzigartigen Merkmalen aus der BSD-Welt" kombiniere. Allerdings werden in dieser ersten BSD-Portierung zum Beispiel einige erweiterte Desktop-Funktionen noch nicht unterstützt.

Wer hingegen weiterhin auf den Linux-Kernel setzt, hat auch auf den Clients eine reiche Auswahl an GUIs: Debian 6 enthält den KDE-Plasma-Desktop in der Version 4.4.5 ebenso wie GNOME 2.30, Xfce 4.6 und LXDE 0.5.0. Für die tägliche Office-Arbeit sind OpenOffice.org 3.2.1, GIMP 2.6.11, Iceweasel 3.5.16 (markenfreie Version von Mozilla Firefox) und Icedove 3.0.11 (markenfreie Version von Mozilla Thunderbird) enthalten. Entwickler können nun mit GNU Compiler Collection 4.4.5, OpenJDK 6b18, Perl 5.10.1, PHP 5.3.3 oder Python 2.6.6, 2.5.5 und 3.1.3 programmieren. Serveradministratoren finden eine reiche Auswahl für unterschiedliche Einsatzzwecke, unter anderem:

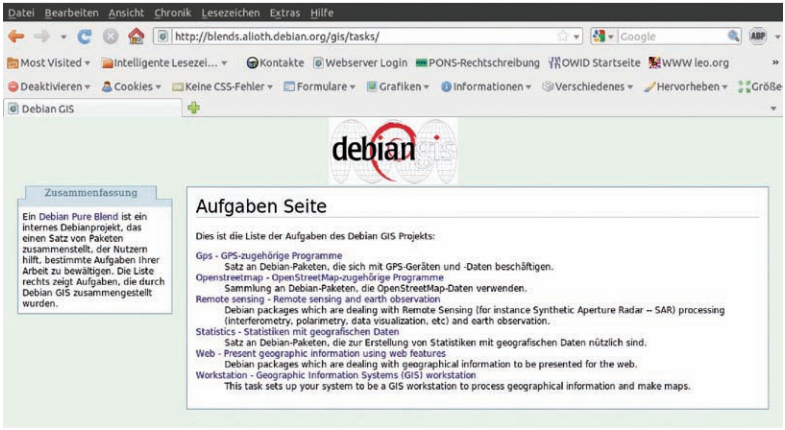
- die Datenbanken PostgreSQL 8.4.6 und MySQL 5.1.49,
- den Webserver Apache 2.2.16,
- den Windows-Share-Server Samba 3.5.6,
- den Kommunikationsserver Asterisk 1.6.2.9,
- das Monitoring-Tool Nagios 3.2.3,
- den Xen Hypervisor 4.0.1 und
- den Java-Servlet-Container Tomcat 6.0.18.

Ähnlich wie schon Ubuntu bootet nun auch Debian schneller. Dank eines abhängigkeitsbasierten Boot-Systems läuft der Systemstart schneller ab – und auch robuster, wie die Projektverantwortlichen mitteilen. Möglich wird das aufgrund paralleler Ausführung von Boot-Skripten und korrekt festgelegter Abhängigkeiten zwischen diesen Skripten.

2.4.2 Angepasste Debian-Distributionen

Pure Blends heißen ab der neuen Debian-Version die angepassten Debian-Distributionen. Zu den bisherigen Spezialdistributionen Debian Edu, Debian Med und Debian Science sind weitere hinzugekommen wie Debian Multimedia für die speziellen Anforderungen an Multimedia-Rechner. Die neuen Blends sind aus vorhandenen Projekten entstanden, wie etwa Debian GIS, an dem schon seit 2004 gearbeitet wird. Debian GIS – GIS steht für Geographic Information Systems – enthält

unter anderem vorbereitete Installationsgruppen (sogenannte Tasks) mit Debian-Paketen für GPS-Geräte und -Daten, OpenStreetMap, SAR und Erdbeobachtung.



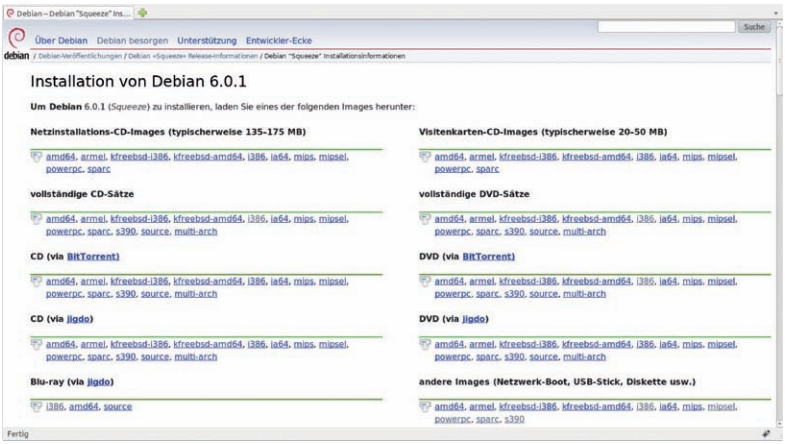
Die Mischung macht's: Debian GIS (Geographic Information System) ist eine eigenständige Distribution mit Software für Geoinformationsdatenverarbeitung.

Außer mit den Pure-Blend-Distributionen glänzt Debian auch in der neuen Version wieder mit Multi-Architektur-CDs und -DVDs für die Architekturen amd64 und i386. Diese ermöglichen von nur einem Medium die Installation auf sämtlichen x86-Rechnern sowie allen 64-Bit-PCs mit AMD-CPUs mit AMD64-Erweiterung und allen Intel-CPUs mit EM64T-Erweiterung und einer gemeinsamen 64-Bit-Benutzerumgebung. Darüber hinaus gibt es nun auch Live-Images für CDs, USB-Sticks und Netz-Boot-Installationen. Diese Images können – wie in anderen Distributionen auch – für die reguläre Installation von Debian GNU/Linux verwendet werden. Als Dateisysteme werden mit Debian 6 nun auch ext4 und Btrfs unterstützt. Die Variante mit FreeBSD-Kernel nutzt ZFS, das Zettabyte-Dateisystem. Upgrades laufen zumeist reibungslos, und die meisten Konfigurationen werden automatisch vom apt-get-Paketverwaltungs-Tool abgewickelt. Wo es Schwierigkeiten geben könnte, ist im Installationshandbuch unter www.debian.org/releases/squeeze/installmanual festgehalten.

2.4.3 Einfache Netzwerkinstallation

Wer zum ersten Mal Debian installieren will, ist nach dem ersten Besuch der Seite www.debian.org/releases/stable/debian-installer/ zunächst vielleicht verwirrt ob der verschiedenen Installationsarten: Es gibt vollständige Sätze für CD (52 Medien), DVD (acht Medien) und Blu-ray (zwei Medien), es gibt Images für Netzwerk-Boot, USB-Stick oder CD, es gibt die kleinen Images mit 20 bis 50 MByte für visi-

tenkartengroße CDs, und es gibt Images mit 135 bis 180 MByte Größe für die Installation via Internet. Wer zum Beispiel eine IBM S/390 mit Debian bestücken will, macht das entweder mit CD- oder DVD-Medien oder von einem IPL-Tape (IPL = Initial Program Load) aus. Alle anderen sollten nach Möglichkeit die Netzinstallation nutzen. Denn die ist je nach Architektur nur zwischen 135 und 180 MByte groß und enthält lediglich das Wichtigste für ein funktionierendes Basissystem; der Rest an Software wird über das Internet nachgeladen.



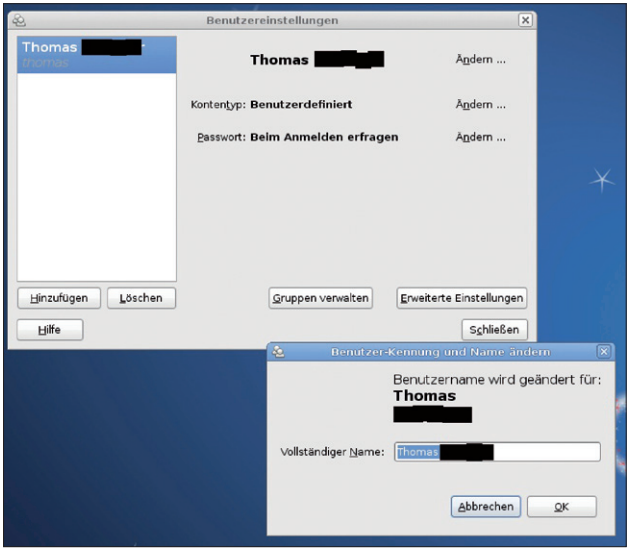
Das soll erst mal einer nachmachen: Es gibt kaum eine Distribution, die für so viele Rechnerarchitekturen ausgelegt ist wie Debian GNU/Linux.

Falls noch nicht entsprechend vorbereitet, muss im Rechner-Bios das Booten von CD/DVD vor dem Booten von Festplatte stehen. Anschließend wird der Rechner von der Netzinstallations-CD gestartet. Das Installationsmenü ist mit vier Einträgen sehr übersichtlich – die Installation gibt es einmal im Text-, einmal im Grafikmodus. Über die *Advanced options* kann der Expertenmodus gestartet oder eine andere Desktop-Umgebung ausgewählt werden. Im Normalfall sollte der *Install*-Befehl gute Dienste leisten.

In der geführten Installation muss der Anwender zunächst Sprache, Standort und Tastaturbelegung auswählen. Anschließend werden das CD- oder DVD-Laufwerk eingebunden, die Komponenten des Installationsprogramms geladen sowie die Netzwerkkarten und -hardware wie zum Beispiel ein DHCP-Server erkannt. Danach will der Installer das Netzwerk einrichten. Geben Sie zuerst einen Namen ein, mit dem der Computer im Netzwerk identifiziert werden soll. Im folgenden Dialog nennen Sie den Domainnamen, also den Teil einer E-Mail-Adresse nach dem @-Zeichen. Haben Sie keinen DHCP-Server im Netz, müssen Sie IP-Adresse, Netzmaske, Gateway und DNS-Server angeben. Diese Angaben schreibt die Setup-Routine in die Datei */etc/network/interfaces*.

2.4.4 Benutzer anlegen

Nach dem Netzwerk werden Benutzer und Passwörter angelegt. Als Erstes geben Sie ein Passwort für den Administrator Root ein. Dieses Passwort sollte schwer zu erraten sein, weil ein Benutzer mit Root-Rechten das gesamte System zerstören kann. Das Installationsprogramm empfiehlt, keine Wörter aus einem Wörterbuch zu nutzen und Buchstaben, Zahlen und Sonderzeichen zu mischen. Wechselnde Klein- und Großschreibung erschwert zusätzlich das Erraten des Passworts.



Kann später geändert werden: Das erste Benutzerkonto, das Sie während der Installation einrichten, können Sie später über die Systemverwaltung in Gnome leicht ändern.

Jetzt wird ein Benutzer angelegt. Auch *Root* sollte möglichst immer als normaler Benutzer arbeiten, so kann er nicht versehentlich wichtige Systemdateien ändern oder löschen. Zuerst müssen Sie den vollständigen Namen eingeben – Sonderzeichen und Umlaute erkennt das Setup-Programm. Der Name wird übrigens auch für E-Mail-Konten oder in Programmen verwendet, die den Benutzernamen anzeigen. Danach schlägt Debian einen Namen für das neue Benutzerkonto vor; abschließend müssen Sie für diesen Benutzer ein Passwort vergeben.

2.4.5 Festplatte partitionieren und LVM konfigurieren

Das Partitionieren der Festplatten erfolgte in früheren Versionen vor dem Anlegen eines Benutzers, ist nun aber im Anschluss zu erledigen. Das Partitionieren kann geführt oder manuell erfolgen; das Partitionsprogramm bietet folgende Optionen:

- *Geführt – vollständige Festplatte verwenden:* löscht alle anderen Betriebssysteme auf der Platte;
- *Geführt – gesamte Platte verwenden und LVM einrichten*: wie zuvor, nur wird auch der Logical Volume Manager eingerichtet, mit dem man Partitionen einfach erweitern kann;
- *Geführt – gesamte Platte mit verschlüsseltem LVM:* wie zuvor, nur mit verschlüsseltem Logical Volume Manager;
- *Manuell:* die Option für Experten, die wissen, was sie tun.

In vielen Fällen wählt man eine geführte Partitionierung. Der Benutzer muss dann lediglich die richtige Festplatte wählen und kurz darauf einen von drei Partitionierungsvorschlägen aussuchen:

- *Alle Dateien auf eine Partition, für Anfänger empfohlen*;
- *Separate /home-Partition*: sinnvoll, wenn man öfter das Betriebssystem ändert;
- *Separate /home-, /usr-, /var- und tmp-Partitionen*: empfehlenswert für den Serverbetrieb, um etwa das Überlaufen der Festplatte durch vollgeschriebene Log-Dateien zu verhindern.

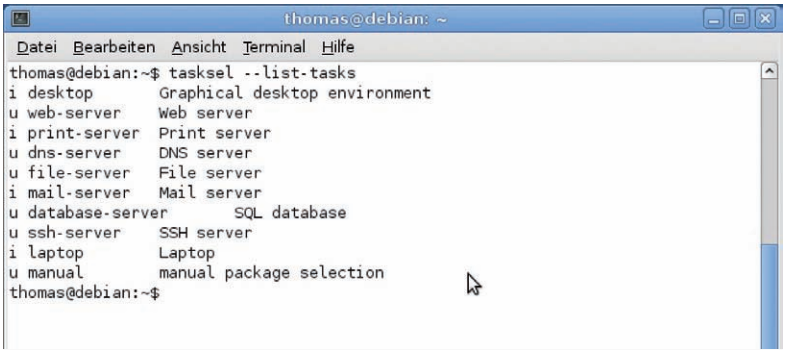
Nach dem Partitionieren wird der Logical Volume Manager konfiguriert. Das geht ähnlich leicht von der Hand wie zuvor das Partitionieren der Festplatte. Es wird eine Startpartition mit dem Verzeichnis */boot* eingerichtet, ferner eine lvm-Partition, in die der Auslagerungsspeicher und die Systempartition gemappt werden. Haben Sie alles zu Ihrer Zufriedenheit eingestellt, übernehmen Sie die Änderungen und lassen den Installer die Partitionen formatieren, bevor dann automatisch das Grundsystem installiert wird.

2.4.6 Paketmanager und Softwareauswahl

Wählen Sie im nächsten Bildschirm ein Land mit dem Spiegelserver und dann einen Server. Standardmäßig wird hier zunächst ein FTP-Server von debian.org ausgewählt, der im jeweils gewählten Land steht. Ein Text im Installationsprogramm weist aber darauf hin, dass ein Server im eigenen oder benachbarten Land nicht unbedingt die schnellste Verbindung garantiert. Das soll im Moment aber nicht weiter stören. Um später nach der Installation einen schnelleren Server zu finden, verwenden Sie das Paket *apt-spy*.

Wenn das Paketverwaltungs-Tool *apt* konfiguriert ist, kommt der Hauptteil: Sie wählen Software aus und installieren diese. Im ersten Schritt legen Sie fest, welche Software installiert werden soll. Voreingestellt sind hier *Desktop-Umgebung* und *Standard-Systemwerkzeuge*; diese Kombination erzeugt ein System mit insgesamt etwa 1100 Programmpaketen inklusive GNOME und OpenOffice. Die werden je nach Geschwindigkeit des Internetzugangs in einigen Minuten oder mehreren Stunden heruntergeladen und anschließend installiert und konfiguriert.

Wollen Sie Debian als Serversystem nutzen, haben Sie ebenfalls reichlich Auswahl: vom *Web-Server* über *Druck-Server*, *DNS-Server*, *Datei-Server* und *Mail-Server* bis hin zum *SSH-Server*. Je nachdem, welchen Task Sie markieren, werden die entsprechenden Pakete mitinstalliert und -konfiguriert. Fürs Erste sollten Sie aber die beiden voreingestellten Standard-Tasks übernehmen und installieren. Sobald Sie auf *Weiter* drücken, werden die Pakete auf den Computer kopiert, die Installation vorbereitet und dann alle Pakete installiert und konfiguriert. Abschließend wird noch der Bootloader installiert; danach kann das neue System gestartet werden. Die CD-Schublade wird geöffnet, damit Sie das Installationsmedium entfernen können. Wenn Sie danach *Weiter* drücken, fährt Debian hoch, und Sie können sich am GNOME Display Manager anmelden.



Nach der Installation ist vor der Installation: Nachdem das Grundsystem läuft, können Sie mit tasksel Ihre Serveranwendungen ins System einspielen.

Nun können Sie auf einer Konsole mit dem Befehl

```
tasksel --list-tasks
```

die Server-Tasks noch einmal auflisten, mit

```
tasksel --task-packages TASKNAME
```

die Pakete eines Tasks abfragen und mit

```
tasksel install TASKNAME
```

einen gewünschten Task installieren, etwa *file-server* für NFS und Samba, *print-server* für CUPS und *mail-server* für Exim sowie Spamassassin.

Thomas Hümmler

2.5 Workshop – Drucken in heterogenen Systemumgebungen

Druckdienste auf PCs funktionieren nach dem Warteschlangenprinzip. Hierbei stellen die Benutzer ein auszudruckendes Dokument per Klick auf eine Schaltfläche oder mittels kurzem Befehl in die Warteschlange. Was anschließend im Hintergrund passiert, bis das Dokument schwarz auf weiß oder bunt auf Papier aus dem Drucker kommt, darum kümmert sich der Druckdienst.

In Linux-Distributionen wie openSUSE (www.opensuse.org) oder Ubuntu (www.ubuntu.com) wird default-mäßig CUPS (www.cups.org) installiert, das Common-Unix-Printing-System. CUPS ist ein Druckserver, der unter Linux genauso arbeitet wie auf Mac OS, das ebenfalls auf Unix basiert. Insofern können Sie unter Linux sofort mit dem Einrichten Ihres Druckers loslegen. Darüber hinaus kann CUPS in heterogenen Umgebungen genutzt werden, sodass auch Windows-basierte Computer den Druckerserver einsetzen können. Somit lassen sich mit einer zentralen Anlaufstelle für Druckaufträge das Management von Druckanforderungen vereinfachen und Kosten sparen. In unserem Workshop zeigen wir, wie Sie CUPS schnell und problemlos einrichten und anschließend nutzen können.

2.5.1 CUPS in Ubuntu einrichten

In Ubuntu etwa finden Sie das Konfigurationsprogramm für die Drucker unter *System / Systemverwaltung / Drucken*. Mit *Hinzufügen* öffnen Sie einen Assistenten zum Einrichten eines Druckers. Der Assistent sucht nach vorhandenen Druckern. Findet er welche, bietet er diese zur Auswahl an. Anderenfalls wählen Sie den Anschluss, dann das Modell und den Treiber.

Druckeroptionen: Je nach gewähltem Drucker und Treiber bietet die Druckerkonfiguration von Ubuntu unterschiedliche Einstellmöglichkeiten.

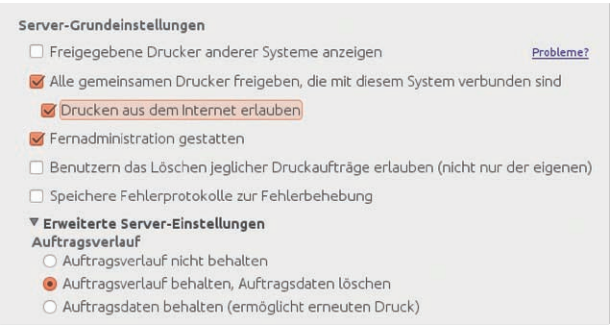
Viele Drucker haben mehr als einen Treiber, etwa sogenannte Foomatic- (www.linuxfoundation.org/collaborate/workgroups/openprinting) oder Gutenprint-Treiber (http://gutenprint.sourceforge.net/) mit zum Teil anderen Funktionen. Welchen Sie letztlich wählen, sollten Sie mit einer Testseite ausprobieren. Ihre Auswahl hängt

unter anderem auch von Ihren genutzten Anwendungen ab. Sie können stattdessen einen Drucker auch mehrmals einrichten – jeweils mit anderen Treibern. Eingerichtete Drucker werden danach im Druckerkonfigurationsprogramm angezeigt. Über das Druckermenü definieren Sie weitere Gerätefunktionen:

- Mit dem Befehl *Eigenschaften* etwa legen Sie die Einstellungen für jeden Drucker fest.
- Über *Duplizieren* erzeugen Sie eine Kopie der Druckerkonfiguration. Diese können Sie *Umbenennen* und mit anderen Eigenschaften hinterlegen – vielleicht wollen Sie einen anderen Treiber wählen oder auch nur einen anderen Papierschacht, etwa für DIN-A3-Papier. Haben Sie die Konfiguration aus Versehen kopiert, *Löschen* Sie sie ebenfalls im Druckermenü.
- *Aktiviert* sind die Drucker, auf die zugegriffen werden kann. Ist ein Drucker *Freigegeben*, kann er auch im Netzwerk benutzt werden.
- Verwenden Sie mehrere Drucker, sollten Sie mit dem Befehl *Als Standard setzen* einen davon als den Standarddrucker definieren.

2.5.2 Drucken im reinen Linux-Netzwerk

CUPS nutzt Avahi, um Drucker im Netzwerk automatisch zu erkennen. Rechner, die CUPS verwenden, können dementsprechend einfach auf Drucker zugreifen, die an anderen Netzwerkrechnern angeschlossen und freigegeben sind.



Druckservereinstellungen: Mit diesen Optionen stellen Sie das Verhalten des Druckservers ein. Ist Ihr Rechner ein Client, stellen Sie hingegen die erste Option ein, um Drucker im Netzwerk zu finden.

Über Avahi gibt ein Rechner seine Präsenz und seine angebotenen Dienste innerhalb des lokalen Netzwerks bekannt. Dazu muss Avahi nicht einmal extra konfiguriert werden, es funktioniert „Out-of-the-box". Wenn Sie mehrere Linux-Rechner innerhalb eines Netzwerkes betreiben, sind auch die Drucker innerhalb dieser Netzwerkumgebung dank Avahi schnell und komfortabel konfiguriert. Sie müssen nur auf allen Netzwerkrechnern die CUPS-Servereinstellungen anpassen. Das geschieht in Ubuntu über *Server / Einstellungen*:

- *Freigegebene Drucker anderer Systeme anzeigen* zeigt im Druckerkonfigurationsprogramm auch die Drucker an, die an anderen Linux-Computern mit *Drucker / Freigegeben* öffentlich nutzbar sind. Diese Einstellung müssen Sie auf jedem Linux-Client einschalten, anderenfalls werden die Drucker des Servers nicht erkannt und angezeigt. Anschließend können Sie die Drucker des Servers nutzen, als wären sie am eigenen Computer angeschlossen.
- *Alle gemeinsamen Drucker freigeben, die mit diesem System verbunden sind* muss eingeschaltet sein, sonst funktioniert der Rechner nicht als Druckserver. Mit *Drucken aus dem Internet erlauben* können Sie sogar per HTTP- oder IPP-Protokoll übers Web ausdrucken. Dazu sollte der Rechner allerdings eine feste und dauerhafte IP-Adresse haben.
- Für *Fernadministration gestatten* gilt Ähnliches: Wenn Sie auf CUPS per HTTP zugreifen wollen, dann benötigen Sie am besten eine dauerhafte, feste IP-Adresse. Über einen Internet-Browser greifen Sie anschließend über *http://IP-Adresse-des-CUPS-Servers:631* auf den Druckserver zu.
- Die Option *Benutzern das Löschen jeglicher Druckaufträge erlauben (nicht nur der eigenen)* sollten Sie nicht einschalten, denn damit ist Ärger im Büro programmiert.
- Spätestens wenn alle Drucker richtig angeschlossen sind und der Druckserver reibungslos arbeitet, können Sie auch die Funktion *Speichere Fehlerprotokolle zur Fehlerbehebung* abschalten.
- Unter *Erweiterte Server-Einstellungen* legen Sie fest, was nach dem Ausdruck mit den Druckaufträgen geschehen soll: Sie können den *Auftragsverlauf nicht behalten*, also löschen lassen. Vielleicht wollen Sie den *Auftragsverlauf behalten, Auftragsdaten löschen* oder auch – speicherintensiv – alle *Auftragsdaten behalten*. Mit letztgenannter Option können Sie Druckaufträge zu einem beliebigen Zeitpunkt wiederholen.

2.5.3 Drucker in openSUSE einrichten

Wenn Sie Ubuntu als Druckserver nutzen, ist Gnome der Standard-Desktop. Auf dem kann CUPS wie zuvor beschrieben konfiguriert werden. Wenn Sie openSUSE mit dem KDE-Desktop einsetzen, ist die Vorgehensweise eine andere: Wählen Sie im Konfigurationswerkzeug Yast im Bereich *Hardware* das Applet *Drucker*. In der *Druckerkonfiguration* wählen Sie *Hinzufügen*. Dann sucht Yast Drucker und den passenden Treiber. Mit *OK* aktualisieren und beenden Sie die Konfiguration.

2.5.4 CUPS in Debian installieren

Während im Debian-Abkömmling Ubuntu CUPS üblicherweise mit installiert wird, ist das in Debian GNU/Linux nicht immer der Fall. Falls Sie den Druckserver

dort installieren wollen, erledigen Sie das als Root in einer Konsole mithilfe des *apt-get*-Befehls:

```
apt-get install cups
```

Auf Debian-Clients installieren Sie das Paket *cups-client*:

```
apt-get install cups-client
```

Falls Sie in einem heterogenen Netzwerk über den Samba-Dienst auf den CUPS-Server zugreifen wollen, installieren Sie auf dem Debian-Server noch Samba:

```
apt-get install samba
```

Wollen Sie jedoch mit Debian-Clients auf Windows-Druckfreigaben zugreifen, installieren Sie den Samba-Client mit

```
apt-get install smbclient
```

```
Datei  Bearbeiten  Ansicht  Suchen  Terminal  Hilfe
webserver:/home/thomas# apt-get install cups
Paketlisten werden gelesen... Fertig
Abhängigkeitsbaum wird aufgebaut
Lese Status-Informationen ein... Fertig
Die folgenden zusätzlichen Pakete werden installiert:
  avahi-utils cups-client cups-common foomatic-db foomatic-db-engine
  foomatic-filters libavahi-client3 libavahi-compat-libdnssd1 libslp1 netcat
  netcat-traditional smbclient
Vorgeschlagene Pakete:
  cups-bsd cups-driver-gutenprint hplip xpdf-korean xpdf-japanese
  xpdf-chinese-traditional xpdf-chinese-simplified cups-pdf kdeprint gtklp
  cups-pt xpp foomatic-db-hpijs foomatic-db-gutenprint foo2zjs cupsys
  foomatic-gui slpd openslp-doc
Die folgenden Pakete werden ENTFERNT:
  lprng
Die folgenden NEUEN Pakete werden installiert:
  avahi-utils cups cups-client cups-common foomatic-db foomatic-db-engine
  foomatic-filters libavahi-client3 libavahi-compat-libdnssd1 libslp1 netcat
  netcat-traditional smbclient
0 aktualisiert, 13 neu installiert, 1 zu entfernen und 0 nicht aktualisiert.
Es müssen 29,0MB an Archiven heruntergeladen werden.
Nach dieser Operation werden 69,5MB Plattenplatz zusätzlich benutzt.
Möchten Sie fortfahren [J/n]? ■
```

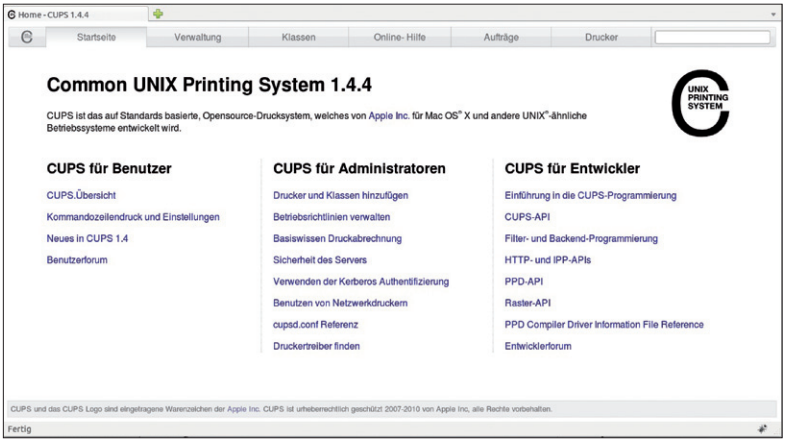
Schnell erledigt: Mit einen einfachen apt-get-Befehl wird CUPS auf einem Debian-Server installiert; insgesamt benötigt der Druckdienst etwa 70 MByte Festplattenplatz.

Der Samba-Client ist eine Implementation des SMB-Protokolls für Linux. Damit erkennt ein Linux-Rechner auch Windows-Datei- und Druckerfreigaben. Man kann damit in einem gemischten Netzwerk von Linux-Clients Drucker benutzen, die an einem Windows-Rechner angeschlossen sind. Für den Fall, dass Sie den Samba-Client installieren, verlangt die Debian-Paketverwaltung nach dem Installieren einige Konfigurationsdaten. So müssen Sie den Namen der Arbeitsgruppe oder Domäne angeben und ob die Passwörter für das SMB-Protokoll verschlüsselt

über das Netz gehen sollen. Während unter Windows 98 noch unverschlüsselte Passwörter übertragen wurden, setzen neuere Betriebssystemversionen von Windows nur noch auf verschlüsselte.

2.5.5 CUPS per Webbrowser steuern

CUPS kann auch in gemischten Umgebungen mit Macintosh- und Windows-PCs als Druckserver dienen. Man kann den Server sogar von diesen Rechnern aus steuern. Dazu benötigen Sie nur einen Webbrowser, über den CUPS bedient werden kann. Geben Sie im Browser die Adresse *http://IP-Adresse-des-CUPS-Servers:631* ein



Leicht zu handhaben: Der CUPS-Server lässt sich über einen Webbrowser gestesteuern; so kann man auf unterschiedliche Programme in den verschiedenen Linux-Distributionen verzichten.

Die webbasierte Konfiguration funktioniert natürlich auch direkt am Druckserver vor Ort; dann lautet die Adresse in der Eingabezeile des Browsers *http://localhost:631*. Dabei handelt es sich um die Port-Adresse des CUPS-Webservers. Über diese rufen Sie dedizierte Statusinformationen vom Drucker und über Druckaufträge ab oder richten neue Drucker ein. Damit erhalten Sie die volle Kontrolle über die oder den angeschlossenen Netzwerkdrucker.

Für die Konfiguration wichtig sind hier vor allem die folgenden drei Untermenüs:

- Im Menü *Verwaltung* legen Sie neue Drucker an und konfigurieren die grundsätzlichen Einstellungen des CUPS-Servers.
- Unter *Aufträge* sehen Sie die aktuellen Aufträge, können diese beide Bedarf anhalten oder löschen.
- Im Menü *Drucker* verwalten Sie die Drucker oder ändern deren Einstel-

lungen. Außerdem kontrollieren Sie mit *Aktive Aufträge anzeigen*, ob der Drucker gerade verwendet wird. Sie können in diesem Menü etwa auch Druckaufträge ablehnen oder verschieben. Klicken Sie dazu auf den Druckernamen, um die weiteren Möglichkeiten zu sehen: Dort können Sie in der Dropdown-Liste *Wartung* auch eine *Testseite drucken* oder unter *Administration* mehrere *Erlaubte Benutzer festlegen*, die den Drucker verwenden dürfen.

2.5.6 Druckerklassen definieren

In der Druckerkonfiguration wie auch auf der Weboberfläche des CUPS-Servers können Sie Druckerklassen verwalten und neue hinzufügen. Das ist dann sinnvoll, wenn Sie ein sehr großes Netzwerk betreuen – in kleinen Netzwerken sind Klassen meist überflüssig, denn in einer Klasse werden mehrere ähnliche Drucker zusammengefasst. Das kann nach Stockwerken geschehen oder nach bestimmten Druckmöglichkeiten, etwa alle Drucker mit Briefpapier. Dokumente werden dann nicht mehr an einen Drucker, sondern an eine Druckerklasse geschickt. CUPS führt den Auftrag dann am ersten verfügbaren Drucker der entsprechenden Klasse aus.

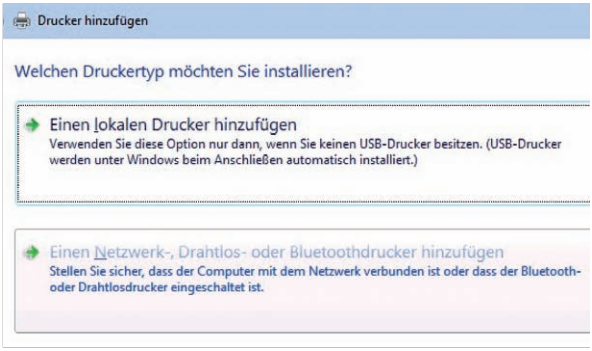
2.5.7 Windows-Clients am CUPS-Server einrichten

Während Unix-Rechner problemlos und einfach mit einem CUPS-Server verbunden werden können, ist es mit Windows-Clients leider alles andere als einfach, und in verschiedenen Windows-Versionen werden die Verbindungen zum Druckserver anders eingerichtet. CUPS unterstützt das Internet Printing Protocol (IPP). Windows beherrscht IPP ab XP und Windows 2000 ebenfalls. Damit ist es ohne allzu viel Konfigurationsaufwand möglich, eine Verbindung zum CUPS-Server herzustellen. Für ältere Windows-Versionen wie Windows 95, 98 oder ME muss auf dem Linux-Server zusätzlich Samba mit Druckfreigaben eingerichtet werden, die dann von Windows aus genutzt werden können. Unter Windows XP und 2000 passen Sie zunächst noch die hosts-Datei an, unter Windows 7 ist das nicht nötig. Die hosts-Datei enthält die Zuordnungen der IP-Adressen zu Host-Namen und steht im Verzeichnis *C:\WNDOWS\system32\drivers\etc*. Fügen Sie eine Zeile mit der IP-Adresse des CUPS-Servers und dessen Host-Namen hinzu, also beispielsweise:

```
192.168.178.2 cupsido
```

Anschließend richten Sie den Drucker ein. Fügen Sie über die Systemsteuerung und *Drucker* einen neuen Netzwerkdrucker hinzu. Für Windows XP und 2000 wählen Sie die Option *Verbindung mit einem Drucker im Internet oder Heim-/Firmennetzwerk herstellen*; als URL tragen Sie *http://cupsido:631/printers/Name_des_Druckers* ein. Im nächsten Fenster suchen Sie den Hersteller und das Druckermodell aus. Abschließend können Sie diesen noch als Standarddrucker festlegen und den Assistenten beenden.

Seit Windows 7 wird es wieder komplizierter. Hier muss in der Systemsteuerung zunächst die Datei- und Druckfreigabe eingeschaltet werden. Damit sollte eine Verbindung zum CUPS-Server möglich sein. Allerdings gibt es den dafür benötigten Datei- und Druckdienst erst ab Windows 7 Home Premium. Unverständlich, denn damit schließt Microsoft sämtliche Netbooks vom Drucken übers Internet aus. Netbooks haben nur die Windows 7 Starter, in dem dieser Druckdienst fehlt.



Windows 7 Home Premium: Hier schalten Sie zunächst den Internetdruckdienst ein und wählen dann als Netzwerkdrucker den CUPS-Drucker.

Zwar gibt es im Netz eine ganze Reihe von Berichten, die Lösungen vorhalten. Auf der CUPS-Projektseite etwa finden sich Ansätze mit Samba über den CUPS-Treiber für Windows. In Microsofts Technet-Forum erhält man den Tipp, erst einen lokalen Windows-Drucker und dann den CUPS-Drucker einzurichten. Beide Vorschläge führen unter Windows 7 Starter nicht zum erwünschten Erfolg.

Eine dritte Lösung wäre schließlich der Apple-Bonjour-Druckdienst für Windows. Den kann man kostenlos von der Apple-Homepage (www.apple.com) herunterladen. Doch leider funktioniert auch dieser im Test mit Windows 7 Starter nicht.

2.5.8 Dedizierter Netzwerkdrucker als Alternative

In gemischten Umgebungen mit Windows 7 Starter bleibt als Alternative nur ein echter Netzwerkdrucker, der ohne Druckserver direkt über seine TCP/IP-Adresse angesprochen wird. Diese haben allerdings den Nachteil, dass sie nicht so dediziert konfiguriert werden können, sodass der Anwender unter Umständen auf verschiedene Komfortfunktionen verzichten muss, die er sonst gewohnt ist.

So ist beispielsweise keine Nutzereinschränkung möglich, ebenso wenig funktioniert eine zentrale Druckauftragsverwaltung. Wer jedoch darauf verzichten kann, für den ist ein Netzwerkdrucker eine Alternative – auch wenn diese Geräte immer noch um einiges teurer sind als herkömmliche Drucker.

Thomas Hümmler

2.6 Versteckte Funktionen in der Fritz!Box nutzen

In unserem ersten Tipp rund um Fritz!Box-Einstellungen geht es um das manuelle Trennen und Wiederherstellen der Internet-Verbindung. Das ist praktisch bei Diensten, die pro IP-Adresse und Tag nur eine begrenzte Nutzung zulassen. Denn bei der erneuten Einwahl weist Ihr Internet-Anbieter der Fritz!Box eine neue IP-Adresse zu. Erst seit der neuesten Firmware findet sich bei der der aktuellen Fritz!Box-Generation in den Fritzbox-Einstellungen im Abschnitt *Internet* eine Schaltfläche mit der Bezeichnung *Neu verbinden*. Damit sie angezeigt wird, muss unter *System -/ Ansicht* die *Expertenansicht* aktiviert sein. Falls Ihre Fritz!Box schon etwas älter ist und die aktuelle Firmwareversion die Option *Neu verbinden* nicht bietet, können Sie alternativ eine spezielle Befehlszeile mit Hilfe des kostenlosen Kommandozeilen-Tools Curl an die FritzBox schicken.

Viele Funktionen: Die Fritz!Box von AVM besitzt eine Fülle an Optionen, die teils undokumentiert sind.

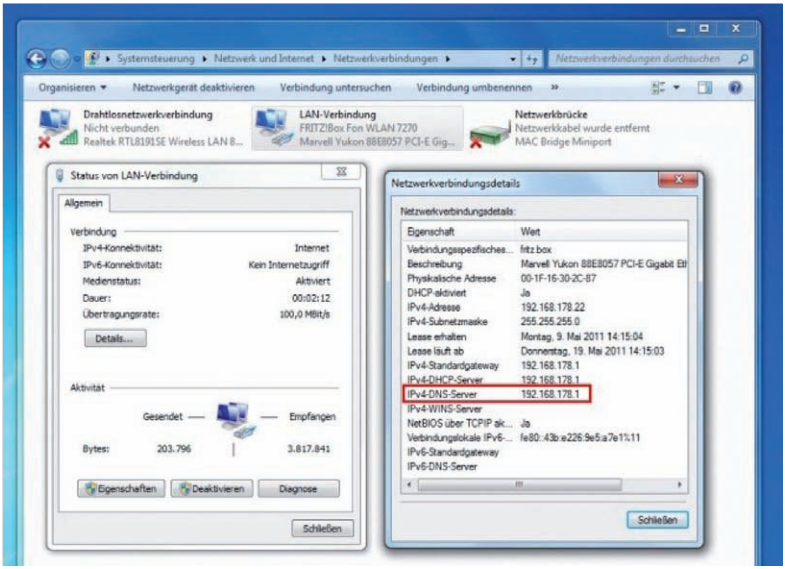
In dem Archiv pcwFBDisconnect (www.pcwelt.de/downloads/pcwFBDisconnect-590571.html) haben wir alle benötigten Komponenten zusammengepackt. Ein Doppelklick auf die darin enthaltene „FB-disconnect.bat“ genügt, um die Verbindung der FritzBox zu trennen.

Voraussetzung dafür, dass die Verbindungstrennung über pcwFBDisconnect funktioniert: In den Einstellungen der Fritz!Box muss unter *Heimnetz* auf der Registerkarte *Programme* der Punkt *Statusinformationen über UPnP übertragen* aktiviert sein. Auch dieser Menüpunkt wird nur angezeigt, wenn die „Expertenansicht“ der FritzBox-Einstellungen aktiviert ist.

Dieses Vorgehen ist auch dann sinnvoll, wenn Sie nur die Verbindung trennen möchten. Denn im Gegensatz zur neuen Fritz!Box-Funktion *Neu verbinden* wird erst dann eine neue Verbindung aufgebaut, wenn ein Programm Daten ins Internet senden will.

2.6.1 DNS-Server in der Fritz!Box

DNS-Server übersetzen Web-Adressen wie www.pcwelt.de in die dazugehörige IP-Adresse, zum Beispiel 62.146.91.230. Das ist nötig, weil Internet-Datenpakete nur anhand der numerischen IP-Adresse zugeordnet und transportiert werden können. Sie bekommen davon normalerweise gar nichts mit, da sich das Betriebssystem darum kümmert, den DNS-Server zu befragen. Auf welchen es dabei zugreifen soll, erfährt es vom Router, in unserem Beispiel der Fritz!Box. Der Router erhält seinerseits die Adresse eines DNS-Servers bei der Einwahl vom Provider zugewiesen. Es steht Ihnen aber frei, einen beliebigen anderen DNS-Server zu nutzen. Gründe dafür gibt es einige. Zum Beispiel stand lange Zeit im Raum, dass die Bundesregierung die Provider zwingen wollte, den Zugang zu bestimmten Web-Seiten zu blocken. Diese Sperre sollte über DNS-Sperrlisten umgesetzt werden. Die Funktionsweise: Wer eine Web-Adresse eintippt, die auf einer schwarzen Liste steht, wird protokolliert und erhält eine falsche IP-Adresse zurückgeliefert. Über ausländische DNS-Server lassen sich solche Sperren umgehen.



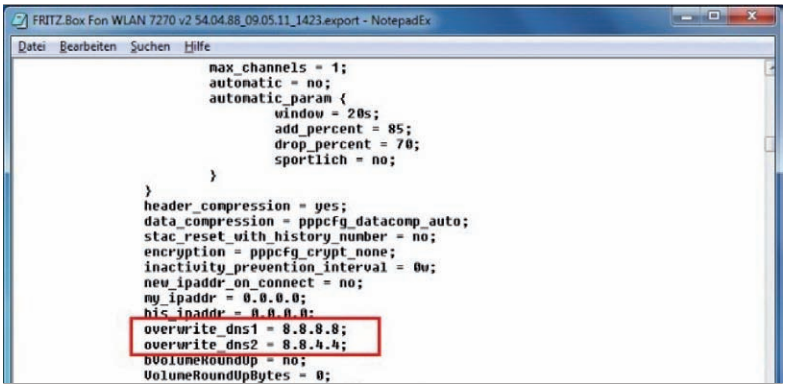
Details: Anzeige des DNS-Servers unter Windows 7.

Hin und wieder kommt es auch vor, dass DNS-Server der Provider überlastet sind und zu lange benötigen, um eine Antwort zu liefern. Gerade bei umfangreichen Websites, bei denen der Browser die Inhalte von mehreren Web-Servern abrufen muss, verzögert sich in einem solchen Fall der Seitenaufbau spürbar. Der nächste Grund betrifft die Sicherheit. Nicht jeder DNS-Server ist ausreichend gegen Angriffe geschützt. Sollte ein Angreifer eine Schwachstelle entdecken, könnte er beliebte Web-Adressen auf gefährliche Malware-Seiten oder auf nachgebaute Online-Banking-Seiten, die Zugangsdaten abfischen, umleiten.

Für solche und ähnliche Fälle gibt es öffentliche DNS-Server. Der von OpenDNS.com hört zum Beispiel auf die IP-Adressen 208.67.222.222 und 208.67.220.220. Auch Google betreibt öffentliche DNS-Server – und zwar unter den Adressen 8.8.8.8 und 8.8.4.4. Google wirbt damit, dass sein DNS-System besonders sicher, also besonders gut gegen Angriffe geschützt sei. Auf der anderen Seite könnte Google mit seinem DNS-Angebot aber auch die Absicht verfolgen, zu protokollieren, welche Web-Seiten besonders häufig aufgerufen werden.

2.6.2 DNS-Server in der Fritz!Box ändern

Es ist etwas umständlich, den DNS-Server in der Fritz!Box zu ändern: Klicken Sie auf *System / Einstellungen sichern / Sichern*. Daraufhin öffnet sich eine Download-Dialogbox für die Konfigurationsdatei, die Sie auf der Festplatte Ihres PCs speichern. Öffnen Sie die Datei anschließend in einem Editor wie Notepad++. Der Editor, der Windows beiliegt, ist dazu nicht geeignet.



Gewusst wie: DNS-Server in der Fritz!Box ändern.

In der Datei gibt es zwei Stellen, die mit *overwrite_dns1* beginnen und zwei, die mit *overwrite_dns2* beginnen. Um den DNS-Server in der FritzBox zu ändern, tragen Sie an beiden Stellen hinter *overwrite_dns1* statt 0.0.0.0 die Nummer des ge-

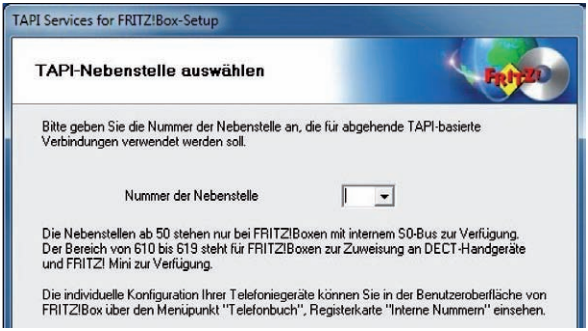
wünschten ersten DNS-Servers ein, zum Beispiel 8.8.8.8. Hinter *overwrite_dns2* schreiben Sie statt 0.0.0.0 die Nummer des gewünschten zweiten DNS-Servers, zum Beispiel 8.8.4.4. Achten Sie in allen Fällen darauf, nicht versehentlich das dahinter stehende Semikolon zu löschen. Der zweite DNS-Server wird immer dann verwendet, wenn der erste nicht oder nicht schnell genug reagiert. Um maximale Ausfallsicherheit zu erzielen, können Sie die Adressen von OpenDNS und Google kombinieren – also 8.8.8.8 bei *overwrite_dns1* und 208.67.220.220 bei *overwrite_dns2* eintragen – oder genau umgekehrt.

Damit die FritzBox die geänderte Konfigurationsdatei akzeptiert und Sie damit den DNS-Server in der FritzBox ändern können, fügen Sie oberhalb von **** *CFGFILE:ar7.cfg* eine neue Zeile ein und schreiben dort *NoChecks=yes* hinein. Nun speichern Sie die Datei und klicken in der FritzBox auf *System / Einstellungen sichern*, wechseln auf die Registerkarte *Wiederherstellen*, laden über *Durchsuchen…* die Konfigurationsdatei in die FritzBox und klicken unten auf die Schaltfläche *Wiederherstellen*. Im Anschluss wird die FritzBox neu gestartet. Dadurch haben Sie den DNS-Server in der FritzBox geändert.

2.6.3 Fritz!Box als Wählhilfe nutzen

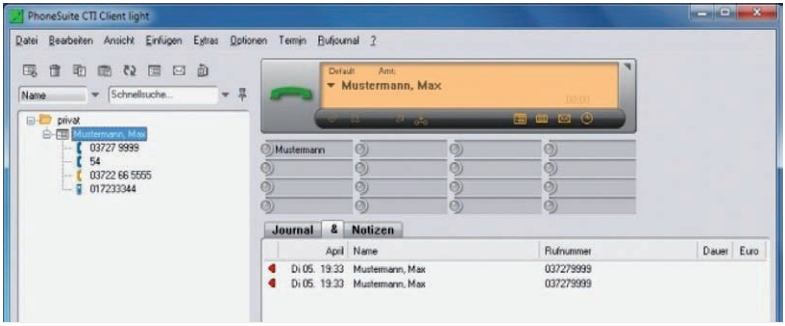
Sie können Ihren PC in Verbindung mit der Fritz!Box als Wählhilfe nutzen, wenn Sie ein Telefon daran angeschlossen haben: Künftig genügt ein Klick auf einen Namen im Adressverzeichnis Ihres PCs und schon klingelt das Telefon. Sobald sie es abheben, wird automatisch eine Verbindung zu der Person hergestellt. Dies funktioniert mit allen Anwendungen, die die Windows-Schnittstelle TAPI (Telephony API) unterstützen. Hier wäre insbesondere Outlook zu nennen. Alternativ nutzen Sie eine Freeware wie PhoneSuite CTI Client light (www.phonesuite.de).

TAPI Services konfigurieren: AVM TAPI Services for FRITZ!Box ist ein Tool, um die Wählhilfe der Fritz!Box nutzen zu können.



Bevor Sie die Fritz!Box-Wählhilfe nutzen können, müssen Sie den Treiber „AVM TAPI Services for FRITZ!Box“ herunterladen. Es gibt ihn in einer 32-Bit-Version und in einer 64-Bit-Version, jeweils für Windows 7, Vista und XP. Bei der Installa-

tion legen Sie fest, welche Nebenstelle der Treiber benutzen soll. Wenn Sie sich unsicher sind, schauen Sie in der Konfiguration der FritzBox unter *Telefonie / Telefoniegeräte* nach, welcher Nebenstellennummer das gewünschte Telefon zugeordnet ist. Um die Einstellung später zu ändern, installieren Sie den Treiber erneut.



So geht es: PhoneSuite CTI Client Light hilft bei der Telefonie.

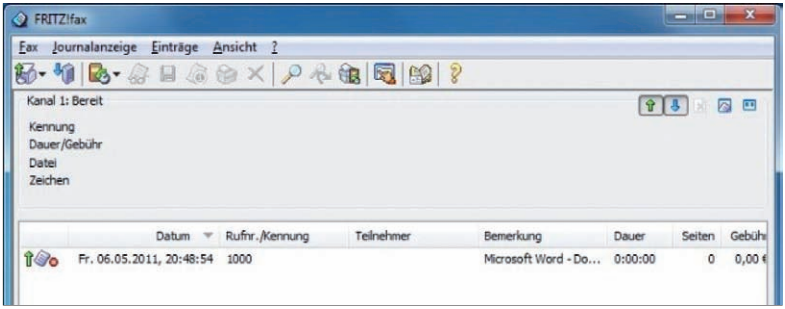
Im Anschluss legen Sie in Ihrer TAPI-fähigen Adressverwaltung fest, dass sie die „AVM TAPI Services for FRITZ!Box" als „TAPI-Gerät" nutzen soll. In PhoneSuite CTI Client light erledigen Sie das indem Sie unter *Optionen / Optionen / TAPI-Geräte* auf *Hinzufügen* klicken und aus der angezeigten Liste *AVM TAPI Services for FRITZ!Box* auswählen.

Tipp: Um eine Rufnummer zu wählen, die Sie auf einer Internet-Seite gefunden haben, markieren Sie diese, drücken Sie *Strg-C*, klicken Sie in PhoneSuite CTI Client light auf das orange Feld, drücken Sie *Strg-V* und anschließend die Eingabetaste *Return*. Viele TAPI-fähigen Programme (Outlook allerdings nicht) zeigen auch eingehende Anrufe an, inklusive der Nummer des Anrufers.

2.6.4 Faxe auf der Fritz!Box versenden

Mit der Fritz!Box können Sie auch faxen – und zwar aus jedem Programm heraus, das eine Druckfunktion bietet. Auch wenn heutzutage E-Mails mehr und mehr das Fax ablösen, so hat ein Fax doch eine höhere Rechtsverbindlichkeit als eine (unsignierte) E-Mail. Um mit der Fritz!Box zu faxen, benötigen Sie das kostenlose Tool FRITZ!fax für FRITZ!Box für Windows 7, Vista und XP (32-Bit und 64-Bit). Falls Sie eine Desktop-Firewall nutzen haben, müssen Sie dem Treiber die Kommunikation mit dem lokalen Netzwerk gestatten.

Nachdem Sie Fritz!fax installiert haben, finden Sie auf dem Desktop ein neues Symbol mit dem Namen *Fritz!fax*, das Sie doppelt anklicken. Beim ersten Programmstart fragt Fritz!fax Ihre Faxrufnummer ab und den Absender, der auf ausgehenden Faxen ganz oben erscheinen soll (*Teilnehmerkennung* und *Kopfzeile*).



Funktionserweiterung: Fritz!Box als Faxgerät nutzen.

Um mit Fritz!fax ein Fax zu versenden, starten Sie aus einer beliebigen Anwendung heraus einen Druckvorgang und wählen Sie als Drucker *FRITZ!Fax Drucker* aus. In dem folgenden Dialogfeld, in das Sie die Faxnummer des Empfängers eintragen und auf *OK* klicken.

Über den Sendestatus informieren Sie sich, indem Sie erneut das Tool „FRITZ!fax" über sein Desktop-Symbol aufrufen. Es archiviert auch Ihre Faxe: Durch Doppelklick auf einen Eintrag sehen Sie den Inhalt des gesendeten Dokuments.

Daniel Behrens

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation PC-Welt.

TecChannel-Links zum Thema	Webcode	Compact
Versteckte Funktionen in der Fritz!Box nutzen	2035528	S.88
Workshop – IMAP-Server Dovecot installieren und konfigurieren	2036025	S.49
Workshop – Apache HTTP-Server beschleunigen	2035748	S.58
Workshop – Thin Clients im Netzwerk einrichten	2035848	S.66
Workshop – Debian 6 übers Netzwerk installieren und einrichten	2035240	S.74
Workshop – Debian 6 übers Netzwerk installieren und einrichten	2033715	S.81

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

3 Sicherheit

Umfragen belegen eine bedrohlich steigende Zahl von Angriffen auf Unternehmensnetze. Dennoch bleibt den Verantwortlichen im Praxisalltag immer weniger Zeit für die Absicherung sowie das Auditing der eigenen IT. Auf den folgenden Seiten steht, wie ein sinnvoller Netzwerkzugriffschutz mit Windows Server 2008 R2 funktioniert, wie man WLANs sicher macht und einen Radius Server einrichtet.

3.1 Praxis: Netzwerkzugriffsschutz (NAP) in Windows-Umgebungen

Dabei kann man überprüfen, ob aktuelle Patches installiert, die Firewall aktiviert und weitere Sicherheitskonfigurationen gesetzt sind. Entspricht ein Client nicht den Bedingungen für das Netzwerk, wird diesem nur ein eingeschränkter Zugriff zum Netzwerk oder überhaupt kein Zugriff gewährt. Durch diese Funktion können Unternehmen vor allem Gefahren vermeiden, die von Heim-PCs und Notebooks ausgehen. Fremdsysteme, Internet-Cafés und unsichere Heimarbeitsplätze lassen sich so effizient vom Netzwerk ausschließen und bei der VPN-Einwahl blockieren, auch wenn der Anwender über entsprechende Einwahlrechte verfügt.

NAP (www.microsoft.com/germany/technet/sicherheit/newsletter/nap.mspx) stellt sicher, dass die Endpunkte in einem Netzwerk, also die PCs, einem fest definierten Sicherheitsstandard entsprechen. Damit der Zugriff eines PCs überprüft werden kann, findet folgender Vorgang statt:

1. Ein Client will sich mit dem Netzwerk verbinden.
2. Als Nächstes generiert der Client ein Statement of Health (http://technet.microsoft.com/de-de/library/bb680833.aspx). Der NAP-Client weiß, wie er das System untersuchen muss, und kann einen Bericht erstellen, den er an den Netzwerkrichtlinienserver übergibt.

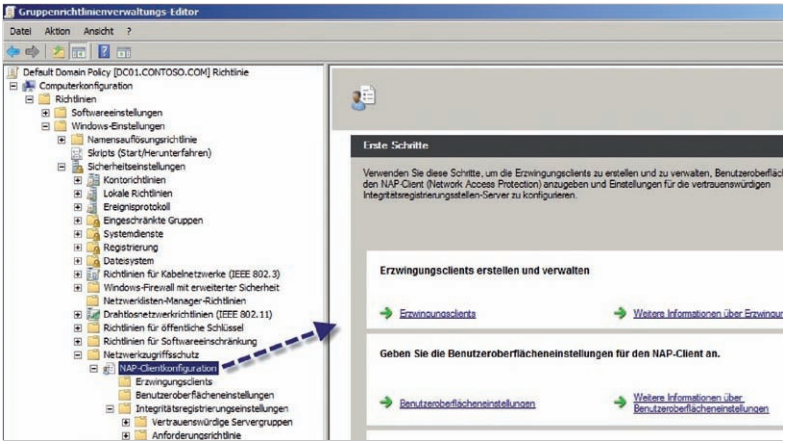
Erkennbar: Der Netzwerkzugriffschutz ist direkt in das Windows-7-Wartungscenter integriert.

3. Dieser entscheidet auf Basis der zentralen Richtlinie, ob das Statement of Health gültig ist oder nicht.
4. Auf Basis dieses Ergebnisses wendet der Server eine Richtlinie an, die den Zugriff gestattet oder nicht.

In Windows 7 ist der Netzwerkzugriffschutz direkt in das Wartungscenter integriert, was für Administratoren und Endanwender den Überblick deutlich erhöht.

3.1.1 Erste Schritte mit NAP

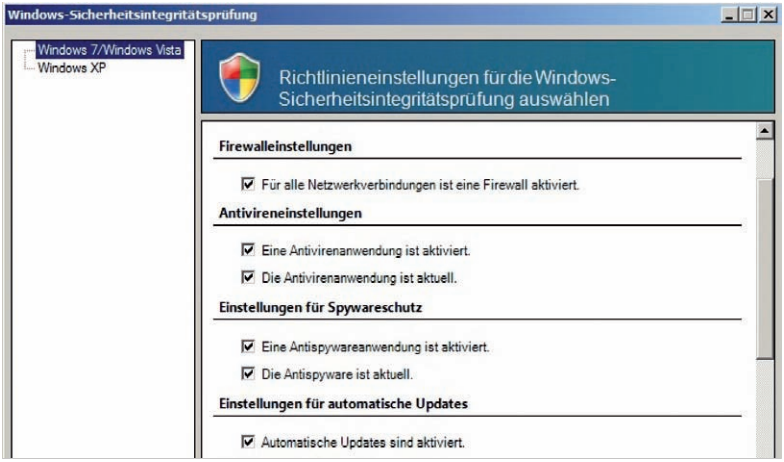
Die Client-seitige Konfiguration von NAP führen Sie am besten über Gruppenrichtlinien durch. Die Einstellungen hierfür finden Sie in der Gruppenrichtlinienverwaltung unter *Computerkonfiguration/(Richtlinien)/Windows-Einstellungen/Sicherheitseinstellungen/Netzwerkzugriffschutz*.



Regelgerecht: Die Konfiguration der NAP-Clients führen Sie über Gruppenrichtlinien durch.

Über diese Einstellungen können Sie das Verhalten der Client-Computer konfigurieren. Hier können Sie zum Beispiel die einzelnen Clients für NAP für die einzelnen Funktionen aktivieren oder deaktivieren. Die Servereinstellungen von NAP führen Sie über den Servermanager durch. Sie finden die Konfiguration des Netzwerkrichtlinienservers über *Rollen/Netzwerkrichtlinien- und Zugriffsdienste*. Die Verwaltung baut zunächst auf die Sicherheitsintegritätsprüfung auf. Diese ruft von den Clients das Statement of Health (SoH) ab. Diese Einstellungen finden Sie in der Verwaltungskonsole über *NPS/Netzwerkzugriffsschutz/Systemintegritätsprüfungen/Windows-Sicherheitsintegritätsverifizierung*.

Rufen Sie in der Mitte diese Eigenschaften der Verifizierungsmethode auf, zum Beispiel von der standardmäßigen vorhandenen Windows-Sicherheitsintegritätsverifizierung. Hier können Sie über die Schaltfläche *Konfigurieren* die Einstellungen festlegen, die die Clients erfüllen müssen, um mit NAP in Ihrem Netzwerk konform zu sein. Diese Systemintegritätsprüfungen bezeichnet Microsoft auch als *Security Health Agents (SHA)*.



Einstellungsfrage: Hier können Sie den Netzwerkzugriffsschutz konfigurieren.

Über den Konsoleneintrag *NPS/Richtlinien/Integritätsrichtlinien* legen Sie Richtlinien fest, auf deren Basis bestimmt wird, was mit Clients passieren soll, die die Sicherheitsverifizierung bestehen oder nicht.

Aufbauarbeit: Auf Basis der Integritätsrichtlinie können Sie die Netzwerkrichtlinie konfigurieren.

Nachdem Sie die Einstellungen in der jeweiligen Systemintegritätsprüfung definiert haben, die ein Computer erfolgreich übermitteln muss, legen Sie eine Integritätsrichtlinie fest, die entscheidet, auf welcher Systemintegritätsüberprüfung festgemacht wird, ob ein Client konform oder nicht konform ist. Clients werden also einer dieser Richtlinien zugewiesen.

Als Nächstes erstellen Sie eine Netzwerkrichtlinie, die auf der Integritätsrichtlinie basiert. In ihr steuern Sie schließlich, was mit den konformen, beziehungsweise nicht konformen, Clients passieren soll.

3.1.2 Netzwerkzugriffsschutz (NAP) mit DHCP einsetzen

Microsoft empfiehlt, den grundlegenden NAP-Schutz in einem Unternehmen über den DHCP-Server einzuführen. Über diese Möglichkeit erlangen Unternehmen den Vorteil der NAP ohne umfangreiche Änderungen in der Infrastruktur. Der NAP-Schutz in DHCP ist zwar die unsicherste Variante des NAP-Schutzes (Clients könnten sich auch manuell eine IP-Adresse zuteilen), dafür aber auch die am schnellsten einführbare.

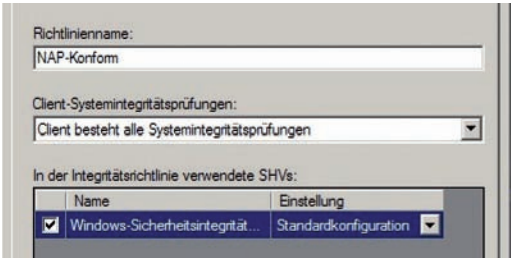
1. Klicken Sie dazu in der NAP-Konsole auf *Netzwerkzugriffsschutz/Systemintegritätsprüfungen/ Windows-Sicherheitsintegritätsverifizierung.*
2. Klicken Sie in der Mitte der Konsole auf *Einstellungen.*
3. Rufen Sie die Eigenschaften der *Standardkonfiguration* auf.
4. Hier legen Sie fest, welche Bedingungen eine Arbeitsstation erfüllen muss, damit diese mit dem Netzwerk kommunizieren darf.

Wartungsserver (Remediation Server) sind Server, auf die Clients zugreifen können, wenn sie nicht NAP-konform sind. Hier tragen Sie die DNS-Namen oder IP-Adressen von Servern ein, mit denen nicht-konforme Clients kommunizieren dürfen. Das kann entweder ein WSUS-Server oder ein FTP-Server sein, auf dem Sie Virensignaturen bereitstellen.

3.1.3 Integritätsrichtlinie erstellen

Der nächste Schritt besteht darin, dass Sie eine Integritätsrichtlinie (Health Policy) erstellen, die als Grundlage die konfigurierte Systemintegritätsprüfung verwendet.

Schritt für Schritt: Es gilt eine neue Integritätsrichtlinie zu erstellen.



Integritätsrichtlinien haben die Aufgabe, Clients in konforme und nicht-konforme NAP-Clients zu unterscheiden. Clients, die die Systemintegritätsprüfung bestehen, sind konform, Clients, die diese Prüfung nicht bestehen, sind nicht-konform:

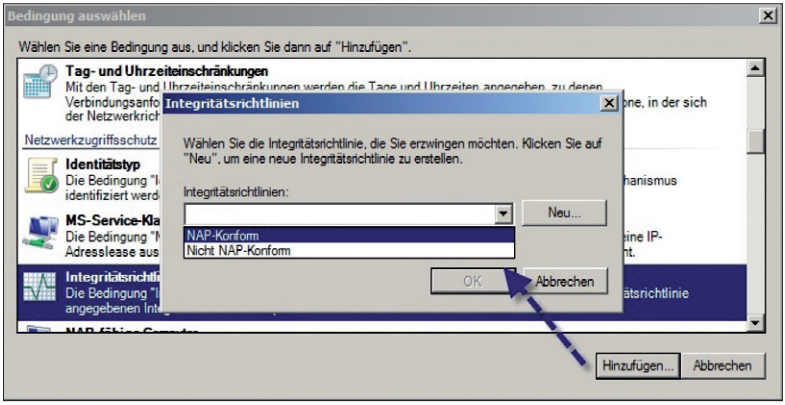
1. Klicken Sie zum Erstellen einer Integritätsrichtlinie mit der rechten Maustaste auf *Richtlinien/Integritätsrichtlinien* und wählen Sie im Kontextmenü den Befehl *Neu.*

2. Geben Sie der Richtlinie die Bezeichnung *NAP-Konform*.
3. Stellen Sie sicher, dass im Listenfeld *Client-Systemintegritätsprüfen* der Eintrag *Client besteht alle Systemintegritätsprüfungen* ausgewählt ist.
4. Aktivieren Sie das Kontrollkästchen *Windows-Sicherheitsintegritätsverifizierung*.
5. Erstellen Sie eine weitere Integritätsrichtlinie.
6. Geben Sie dieser die Bezeichnung *Nicht-NAP-Konform*.
7. Wählen Sie im Listenfeld den Eintrag *Client besteht mindestens eine Systemintegritätsprüfung* nicht aus.
8. Aktivieren Sie das Kontrollkästchen *Windows-Sicherheitsintegritätsverifizierung*.

Im Anschluss legen Sie fest, welchen Netzwerkzugriff die Clients bekommen, die der jeweiligen Integritätsrichtlinie zugewiesen sind. Diese Aufgabe erledigen Sie mit Netzwerkrichtlinien. Einfach ausgedrückt bauen Netzwerkrichtlinien auf Integritätsrichtlinien auf, die wiederum auf Systemintegritätsprüfungen beruhen.

3.1.4 Netzwerkrichtlinien erstellen

Nachdem Sie die Systemintegritätsprüfung festgelegt haben, in denen konfiguriert ist, welche Bedingungen ein NAP-konformer-Client erfüllen muss, wird mit den Integritätsrichtlinien festgelegt, ob ein Client NAP-konform oder nicht-NAP-konform ist. Die Netzwerkrichtlinien steuern wiederum, was mit NAP-konformen beziehungsweise nicht-NAP-konformen Clients im Netzwerk passieren soll und welchen Zugriff diese erhalten dürfen.



Netzwerkrichtline: Es gilt für die Netzwerkrichtlinie die erstellte Integritätsrichtlinie festzulegen.

Die NAP-Infrastruktur basiert daher auf folgenden drei Pfeilern:

- Systemintegritätsprüfungen (System Health Validators) und System Health Agents (SHA)
- Integritätsrichtlinien (Health Policies)
- Netzwerkrichtlinien (Network Policies)

Bevor Sie neue Richtlinien erstellen, sollten Sie zunächst die standardmäßig angelegten Richtlinien deaktivieren. Klicken Sie diese dazu mit der rechten Maustaste an und wählen im Kontextmenü den Eintrag *Deaktivieren* aus, wenn diese noch nicht deaktiviert sind.

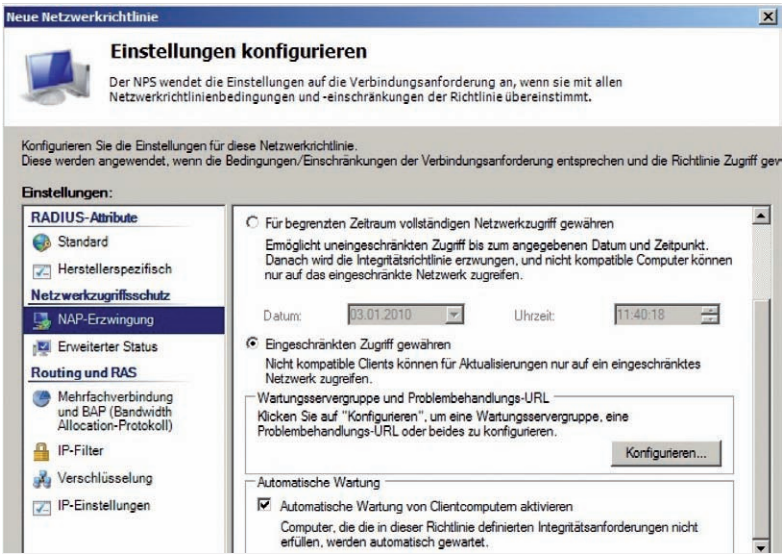
Im ersten Schritt erstellen Sie die Netzwerkrichtlinie für konforme Clients:

1. Klicken Sie dazu mit der rechten Maustaste auf den Konsoleneintrag *Richtlinien/Netzwerkrichtlinien* und wählen im Kontextmenü den Befehl Neu aus.
2. Geben Sie der Richtlinie eine Bezeichnung wie etwa *Vollzugriff für NAP-Konforme Clients* und klicken auf *Weiter*.
3. Klicken Sie auf der nächsten Seite *Bedingungen angeben* auf *Hinzufügen*.
4. Wählen Sie als Option *Integritätsrichtlinien* aus. Hier sehen Sie, dass Ihnen, abgesehen den Integritätsrichtlinien, noch zahlreiche weitere Methoden zur Verfügung stehen, um Richtlinien für den Netzwerkzugriff der Clients festzulegen. Es besteht dabei auch die Möglichkeit, dass Sie mehrere Bedingungen festlegen, die für verschiedene Netzwerkzugriffe notwendig sind.
5. Klicken Sie auf *Hinzufügen*.
6. Wählen Sie die Richtlinie *NAP-Konform* aus.
7. Auf der nächsten Seite des Fensters legen Sie den Netzwerkzugriff der Richtlinie fest. Wählen Sie hier *Zugriff gewährt* aus.
8. Klicken Sie auf *Weiter*, um zum Fenster *Authentifizierungsmethoden konfigurieren* zu gelangen.
9. Deaktivieren Sie die Standardeinstellungen und aktivieren noch die Option *Nur Integritätsprüfung für Computer durchführen*.
10. Klicken Sie auf *Weiter* und belassen im nächsten Fenster alle Einstellungen, wie sie sind. Auf diesem Fenster legen Sie die Einschränkungen fest.
11. Klicken Sie im Fenster *Einschränkungen konfigurieren* ebenfalls auf *Weiter*. Sie gelangen zum Fenster *Einstellungen konfigurieren*.
12. Klicken Sie hier auf *NAP-Erzwingung* und stellen Sie sicher, dass die Option *Vollständigen Netzwerkzugriff gewähren* aktiviert ist.
13. Klicken Sie nach der Einstellung auf *Weiter* und schließen das Erstellen der Richtlinie ab.

3.1.5 Netzwerkrichtlinie für nicht-konforme NAP-Clients erstellen

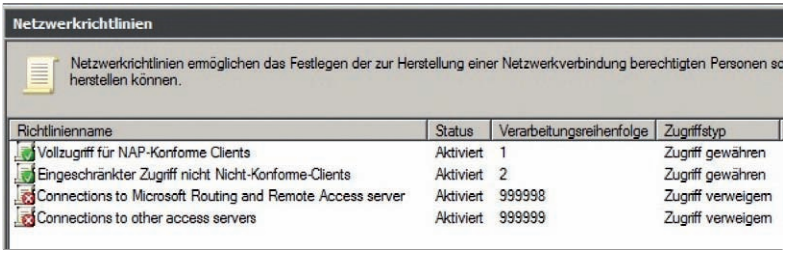
Nachdem Sie die Richtlinie für konforme NAP-Clients erstellt haben, müssen Sie als Nächstes eine Netzwerkrichtlinie erstellen, die den Netzwerkzugriff für nicht-konforme Clients steuert:

1. Gehen Sie analog zum vorhergehenden Abschnitt vor und weisen der Richtlinie eine passende Bezeichnung zu.
2. Wählen Sie diesmal als Integritätsrichtlinie die Richtlinie *Nicht-NAP-Konform* aus.



Einschränkung: Der nicht-konforme Client bekommt nur einen begrenzten Zugriff gewährt.

3. Auf der Seite *Zugriffsberechtigungen angeben* wählen Sie auch hier *Zugriff gewähren*. Der Zugriff wird später noch eingeschränkt. Natürlich könnten Sie für sich auch die Option *Zugriff verweigert* auswählen, um den Clients die komplette Kommunikation zu untersagen. Allerdings würden Sie in diesem Fall die Clients völlig aus dem Netzwerk aussperren.
4. Klicken Sie auf *Weiter*, um zum Fenster *Authentifizierungsmethoden konfigurieren* zu gelangen.
5. Deaktivieren Sie die Standardeinstellungen und aktivieren noch das Kontrollkästchen *Nur Integritätsprüfung für Computer durchführen*.



Wer darf was?: Sie können sich die Netzwerkrichtlinien anzeigen lassen.

6. Klicken Sie auf *Weiter*, um zur Seite *Einschränkungen konfigurieren* zu gelangen. Klicken Sie auch hier auf *Weiter*, um zur Seite *Einstellungen konfigurieren* zu gelangen.
7. Klicken Sie auf *NAP-Erzwingung*.
8. Aktivieren Sie die Option *Eingeschränkten Zugriff gewähren*.
9. Aktivieren Sie das Kontrollkästchen *Automatische Wartung von Clientcomputern aktivieren*.

Schließen Sie das Erstellen der Netzwerkrichtlinien ab. Diese werden anschließend in der NPS-Konsole angezeigt. Alle anderen Richtlinien sollten als deaktiviert angezeigt werden.

3.1.6 DHCP-Server für NAP konfigurieren

Im nächsten Schritt müssen Sie den DHCP-Server unter Windows Server 2008 R2 konfigurieren, damit dieser NAP nutzen kann. Rufen Sie die Verwaltungskonsole des DHCP-Servers auf. Sie finden die Konsole über *Start/Verwaltung/DHCP* oder im Servermanager. Auch über *Start/Ausführen/dhcpmgmt.msc* können Sie die Konsole aufrufen.

Um DHCP für NAP zu konfigurieren, gehen Sie folgendermaßen vor:

1. Rufen Sie die Eigenschaften des Bereiches auf.
2. Wechseln Sie auf die Registerkarte *Netzwerkzugriffsschutz*.
3. Aktivieren Sie die Option *Für diesen Bereich aktivieren*.
4. Aktivieren Sie die Option *Netzwerkzugriffsschutz-Standardprofil verwenden*.

Im nächsten Schritt konfigurieren Sie den DHCP-Server so, dass NAP-konforme Clients eine IP-Adresse vom Server erhalten. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf den Konsoleneintrag Bereichsoptionen unterhalb des von Ihnen erstellten Bereiches und wählen Sie *Optionen konfigurieren* aus.
2. Wechseln Sie auf die Registerkarte *Erweitert*.

3. Wählen Sie im Dropdownlistenfeld *Benutzerklasse* die Option *Standardbenutzerklasse* aus.
4. Jetzt können Sie die Optionen auswählen, die Ihren standardmäßigen NAP-konformen Clients zugewiesen werden sollen, zum Beispiel *DNS-Server*, *WINS* und *DNS-Domäne*.

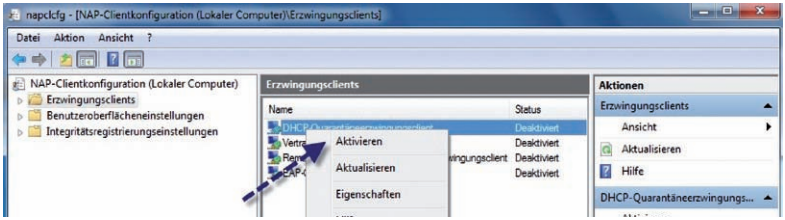
DHCP-Konfiguration für nicht-konforme Clients

Im nächsten Schritt müssen Sie den DHCP-Server so konfigurieren, dass nicht-konforme NAP-Clients entsprechende IP-Adressen erhalten, und zwar so, dass die Clients sich mit den Wartungsservern verbinden beziehungsweise nur teilweise mit dem Netzwerk kommunizieren können. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf den Konsoleneintrag Bereichsoptionen unterhalb des von Ihnen erstellten Bereiches und wählen *Optionen konfigurieren* aus.
2. Wechseln Sie auf die Registerkarte *Erweitert*.
3. Wählen Sie im Dropdownlistenfeld Benutzerklasse die Option *Standardmäßige Netzwerkzugriffsschutz-Klasse* aus.
4. Wählen Sie die Option *006 DNS-Server* aus und hinterlegen die IP-Adresse Ihres DNS-Servers.
5. Wählen Sie die Option *015 DNS-Domänenname* aus und hinterlegen als Namen einen DNS-Namen, zum Beispiel restricted.contoso.com.
6. Durch diese Konfiguration haben Sie sichergestellt, dass die konformen NAP-Clients vollständig an das Netzwerk angebunden werden und die nicht-konformen eingeschränkten Zugriff erhalten.

3.1.7 NAP-Clients konfigurieren

Damit die Windows-Sicherheitsintegritätsverifizierung unter Windows Server 2008 R2 Daten empfangen kann, muss in Windows das Wartungscenter aktiviert sein. Das Sicherheitscenter oder das Wartungscenter fragt die entsprechenden Daten auf dem PC ab und sendet diese zum NPS-Server.



Konfiguration: Aktivieren Sie den DHCP-Quarantäneerzwingungs-Clients unter Windows 7 oder Vista.

Auf Windows-Vista-Computern, die Mitglied einer Domäne sind, ist das Sicherheitscenter deaktiviert, bei Windows 7 ist das Wartungscenter auch bei einer Domänenmitgliedschaft aktiv. Der beste Weg dazu ist die Aktivierung über Gruppenrichtlinien. Gehen Sie dazu folgendermaßen vor:

1. Geben Sie über *Start/Ausführen/gpedit.msc* ein.
2. Navigieren Sie zu *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Sicherheitscenter*.
3. Aktivieren Sie die Richtlinie *Sicherheitscenter aktivieren (nur Domänencomputer)*

Die nächste Aufgabe, die Sie durchführen müssen, ist die Aktivierung der DHCP-NAP-Unterstützung:

1. Starten Sie dazu auf dem Windows-Vista- und Windows-7-PC über *Start/Ausführen/napclcfg.msc* die Verwaltungskonsole des NAP-Clients.
2. Klicken Sie in der Konsolenstruktur auf den Eintrag *Erzwingungsclients*.
3. Aktivieren Sie den *DHCP-Quarantäneerzwingungsclient*.

Alternativ können Sie Erzwingungsclients für den Netzwerkzugriffsschutz auch über Gruppenrichtlinien aktivieren. Diese Einstellung finden Sie unter *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Netzwerkzugriffschutz/NAP-Clientkonfiguration/Erzwingungsclients*.

3.1.8 Clients anbinden

Der nächste Schritt zur Anbindung von Windows Vista und Windows 7 an eine NAP-Infrastruktur besteht darin, den Systemdienst NAP-Agent (Network Access Protection) zu aktivieren. Setzen Sie nach Aufruf der Dienste-Konsole über *Services.msc* den Starttyp dieses Dienstes auf Automatisch und starten diesen.

Aufmerksam: Windows 7 erkennt, wenn ein Computer nicht dem Zugriffsschutz im Netzwerk entspricht.

Durch die Einstellung in der Netzwerkrichtlinie, derzufolge sich die angebundenen Windows-Vista- und Windows 7-PCs automatisch warten sollen, wenn diese nicht NAP-konform sind, wird die Windows-Firewall immer wieder in Echtzeit automatisch aktiviert, wenn Sie diese deaktivieren.

Dadurch ist sichergestellt, dass auch auf PCs, an denen Benutzer mit Administratorrechten sitzen, die Firewall immer aktiv ist. In regelmäßigen Abständen, vor allem bei der Anmeldung, erscheint im Info-Bereich der Taskleiste ein Hinweis, ob

der Client den Netzwerkrichtlinien entspricht. Nur wenn Sie die automatische Wartung aktiviert haben, startet Windows die Firewall neu. Ansonsten erhalten Sie lediglich eine Fehlermeldung, und Windows schränkt den Zugriff auf Basis der hinterlegten Regeln ein. Wenn Sie auf die Meldung oder das dazugehörige Symbol doppelklicken, erhalten Sie eine ausführliche Statusangabe anzeigt für den Fall, dass der Zugriffschutz nicht mehr hergestellt werden kann. Außerdem zeigt der Netzwerkzugriffschutz Fehler bei der Verbindung im Wartungscenter von Windows 7 an. Damit erhalten Anwender auch hier Informationen und eine Lösung und werden nicht einfach nur blockiert.

Alle Ereignisse der NAP-Konfiguration finden Sie in der Ereignisanzeige. Die Ereignisse auf dem Client erhalten Sie in der Ereignisanzeige über *Anwendungs- und Dienstprotokolle/Microsoft/Windows/Network Access Protection*. Auf dem Server sind die Fehler im Systemprotokoll vermerkt.

Thomas Joos

Thomas Joos ist freiberuflicher IT-Consultant und seit 20 Jahren in der IT tätig. Er schreibt praxisnahe Fachbücher und veröffentlicht in zahlreichen IT-Publikationen wie TecChannel.de und PC Welt. Das Blog von Thomas Joos finden Sie unter thomasjoos.wordpress.com.

TecChannel-Links zum Thema	Webcode	Compact
Praxis: Netzwerkzugriffsschutz (NAP) in Windows-Umgebungen	2035833	S.94
Tipps und Tricks – WLANs sicher konfigurieren	2035470	S.105
Workshop – Freeradius für Linux einrichten	2036067	S.115

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

3.2 Tipps und Tricks – WLANs sicher konfigurieren

Drahtlose Netze, so prophetisch kann man heute durchaus sein, dürften über kurz oder lang in jedem Kleinbüro, Home-Office oder halbwegs technikaffinen Haushalt zu finden sein. Allein die rasante Verbreitung von drahtlosen Endgeräten wie Notebooks, Smartphones und – ganz wichtig – Tablet-PCs wird WLAN allgegenwärtig machen. Der Sicherheit der drahtlosen Zugriffsmöglichkeiten kommt damit noch mehr Bedeutung zu. Auch wenn Deutschland den Schutz der WLANs ernster nimmt als andere Länder, zeigte bereits eine lokal stark eingeschränkte Analyse im Dezember 2010, dass immer noch etwa 4 Prozent der Wireless Local Area Networks komplett ungesichert und mehr als 15 Prozent lediglich mit dem veralteten Verschlüsselungsstandard WEP geschützt waren. Diese Werte sind deutlich besser als noch vor zwölf Monaten. Das Thema Sicherheit ist also bei den Benutzern angekommen. Trotzdem gehören ungesicherte oder nur mit WEP geschützte WLANs im Jahr 2011 aus dem Verkehr gezogen. Dafür sollte schon das Urteil des Bundesgerichtshofs vom 12.05.2010 (Az. I ZR 121/08) sorgen. Das Urteil stellte klar, dass der Betreiber eines WLANs den Anschluss vor dem unbefugten Zugriff Dritter sichern muss. Versäumt er dies und begehen Dritte über den WLAN-Anschluss Rechtsverstöße, beispielsweise durch illegale Musiktauschbörsen, dann kann man auf Unterlassung der Rechtsverstöße in Anspruch genommen und abgemahnt werden. Dem Bundesgerichtshof zufolge muss das WLAN mit den zum Zeitpunkt der Installation marktüblichen Sicherungen geschützt werden.

Als Privatperson ist man nicht verpflichtet, den WLAN-Schutz ständig auf den neuesten Stand zu bringen, eine einmalige gute Sicherung bei der Installation reicht aus. Doch schon um die eigenen Computer und anderen WLAN-fähigen Endgeräte zu schützen, sollte der Schutz des WLANs ernst genommen und regelmäßig nachgebessert werden. Schließlich war auch WEP noch vor nicht allzu langer Zeit ein adäquates Mittel zum Absichern des drahtlosen Datenverkehrs.

Wie üblich kann es keine absolute Sicherheit geben, ein Schlupfloch wird sich immer auftun, wenn man nur lange und ausdauernd genug sucht. Aber es ist wichtig, zum einen die rechtlichen Anforderungen zu erfüllen und zum anderen den unbedarften Drive-by-Angreifer auszusperren. Natürlich ist es schade, dass auf diese Weise harmlose Nutzer, die einfach nur einen WLAN-Zugang für einen schnellen E-Mail-Check benötigen, außen vor bleiben. Aber für die gibt es in Deutschland etwa 15.000 Hotspots.

3.2.1 Keine SSIDs senden

Der erste Schritt muss immer sein, sein eigenes WLAN so gut wie möglich zu verstecken. Wenn niemand weiß, dass ein Funknetzwerk existiert, wird es auch keine Angriffe geben. Dazu erlauben alle aktuellen und fast alle älteren Access Points, die

Ausstrahlung des Service Set Identifiers (SSID) zu unterbinden. Zugang zum Netz gibt es dann nur, wenn man den SSID explizit in den Client einträgt. Bei einer nicht-trivialen Buchstaben- und Zahlenkombination ist das zufällige Erraten ausgeschlossen. Man sollte also auch den Default-Namen, häufig der Name des Herstellers wie „Netgear“ oder „Zyxel“, tunlichst verändern, um Rückschlüsse auf die verwendete Hardware und den Einsatzort wie „Charlys Cafe“ zu vermeiden.

Tarnmodus: Ein Klick auf diese Funktion schaltet den SSID Broadcast ab.

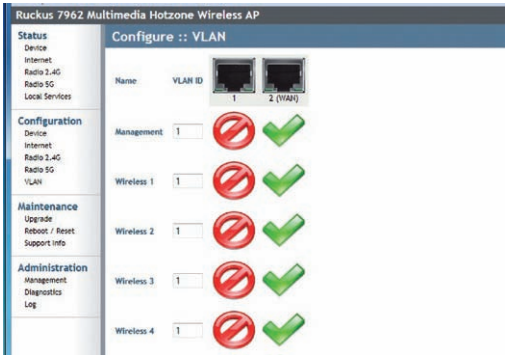
Der SSID dient bei der Anmeldung an einem WLAN und beim Handover zwischen zwei benachbarten Funkzellen dazu, den nächsten Access Point zu finden. Die maximale Länge eines SSID beträgt 32 Byte, seine Übertragung geschieht auf Layer-2 als Parameter in einem speziellen, in regelmäßigen Abständen übertragenen Paket, dem sogenannten Beacon Frame. Dieser Mechanismus, der SSID Broadcast, lässt sich über die Benutzeroberfläche des Access Points abstellen.

Allerdings hilft diese Maßnahme nur gegen flüchtige Beobachter. Wer sich mit drahtlosen Netzwerken auskennt und in der Lage ist, einen Protokoll-Analyzer zu bedienen, kann aus mitgeschnittenen Paketen die SSID extrahieren. Zudem sollte man sich auf mögliche Probleme mit bestimmten Endgeräten einstellen. So konnte Windows XP SP2 keine Verbindung zu WLANs aufbauen, bei denen der SSID Broadcast abgeschaltet war.

3.2.2 Gezielt getrennte SSIDs einrichten

Sehr einfache Access Points, wie sie oft Bestandteil von Routern sind, erlauben nur eine SSID für das komplette Gerät. Etwas hochwertigere Systeme können hingegen mehrere SSIDs gleichzeitig verwalten. So lassen sich virtuelle drahtlose Zonen einrichten, was beim ambitionierten Privatanwender durchaus sinnvoll sein kann. Wer partout einen Zugang zum Internet freigeben möchte und das auch entsprechend mit Firewall, Virenscanner und Content-Filter absichern kann, kann dafür einen Public-SSID reservieren. Der ist dann auch ohne Verschlüsselung zugänglich, was ansonsten nicht ratsam ist. Der private Datenverkehr läuft hingegen über eine SSID mit schärferen Zugangsbeschränkungen.

VLANs verwalten: Mehrere SSIDs werden meist in Verbindung mit VLANs genutzt. Hier legt Ruckus fest, welche Ports und SSIDs zu welcher VLAN-ID gehören.



Bei komplexeren Netzwerken werden die SSIDs in der Regel mit virtuellen LANs (VLAN) gekoppelt. So sind auch die Daten, die vom drahtlosen Netz in das drahtgebundene Netzwerk übergehen, verschlüsselt und vor dem Zugriff durch andere WLAN-Teilnehmer geschützt.

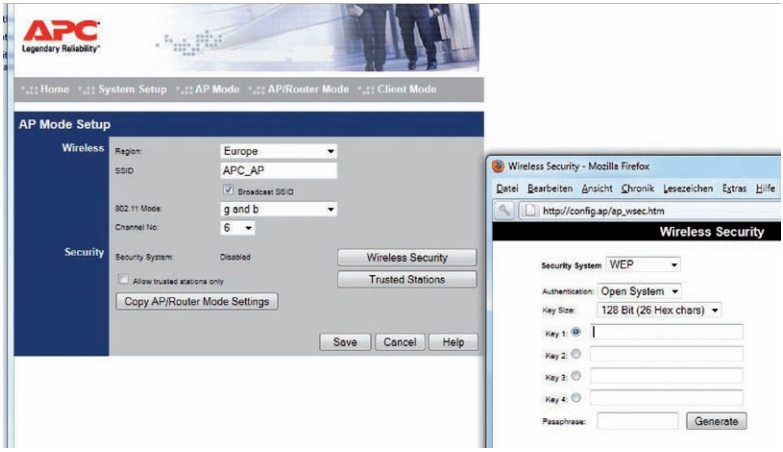
3.2.3 WLAN Teilnehmer per IP Isolation kontrollieren

Nicht alle Access Points oder DSL-Router bieten diese Funktion, aber in der Oberklasse ist sie mittlerweile üblich: IP-Isolation. Während normalerweise alle Teilnehmer der drahtlosen Netzkommunikation mit den anderen Teilnehmern Kontakt aufnehmen, also beispielsweise deren IP-Adressen per Ping testen können, ist das mit IP-Isolation nicht möglich. Der Gedanke dahinter ist, dass drahtlose Clients keine Ressourcen auf den PCs der anderen drahtlosen Clients in Anspruch nehmen müssen. Sobald beispielsweise ein drahtloser Drucker am WLAN teilnimmt, ist dieser Ansatz nicht mehr möglich. Wer hingegen nur Clients per WLAN ins Netz holt, die auf Ressourcen hinter dem Access Point zugreifen wollen, kann mit einem Haken an diesem Feature die Sicherheit innerhalb des WLANs erhöhen

3.2.4 WEP: trügerische Sicherheit

Die Verschlüsselung ist mit Sicherheit das wichtigste Sicherheits-Feature bei drahtlosen Netzwerken. Schon in den ersten WLAN-Produkten war sie fester Bestandteil, allerdings nutzte man damals noch das Wired-Equivalent-Privacy (WEP)-Verfahren. WEP basiert auf der Stromchiffre RC4, mit der Klardaten paketweise abhängig von einem Schlüssel und einem Initialisierungsvektor (IV) in Chiffratdaten umgewandelt werden. Der Schlüssel ist dabei eine Zeichenkette von wahlweise 40 oder 104 Bit; er muss den am WLAN beteiligten Endgeräten sowie dem Access Point vorab zur Verfügung gestellt werden. Für das gesamte WLAN wird ein gemeinsamer Schlüssel verwendet, alle Access Points und Clients müssen

den Schlüssel kennen und in ihren Einstellungen hinterlegen. Das macht das Schlüsselmanagement schwierig und schon ab einer zweistelligen Zahl von teilnehmenden Computern sehr umständlich.



Schlüsselbund: Bei WEP konnte man mehrere Schlüssel eingeben, um einfacher zwischen den Einträgen wechseln zu können.

In Verbindung mit der WEP-Verschlüsselung kann auch zwischen zwei Authentisierungsmodi gewählt werden. Im Modus „Open" findet keine Authentisierung statt, bei „Shared Key" kommt ein Challenge-Response-Verfahren zum Einsatz: Der Access Point generiert 128 zufällige Bytes und sendet diese als Challenge in einem Datenpaket unverschlüsselt an einen Client. Der Client verschlüsselt das Datenpaket und sendet diese Response zurück zum Access Point. Wenn der Access Point die Response erfolgreich entschlüsseln kann, wird der Client authentisiert. Das erste Problem dabei ist, dass der Vorgang nur einseitig abläuft. Der Access Point muss sich gegenüber den Clients nicht authentisieren.

Zudem ist die Implementierung des Initialisierungsvektors fehlerbehaftet, was die Verschlüsselung selbst angreifbar macht. In einem viel beachteten Grundlagenpapier zeigten Fluhrer, Mantin und Shamir, dass aufgrund der schwachen IVs prinzipiell erfolgreiche Angriffe auf die Verschlüsselung durchgeführt werden können. Die ersten Tools wie Aircrack und Airsnort folgten bald nach, sodass WEP binnen kürzester Zeit als nicht mehr sicher anzusehen war, unabhängig von Länge und Komplexität des Schlüssels.

Zwar musste dazu eine große Zahl von Paketen (> 500.000) mitgeschnitten werden, doch weitere Tools erlaubten es bald, die Access Points dazu zu bringen, ausreichend Daten für einen erfolgreichen Angriff zu generieren. Dazu werden ARP-Pakete anhand bestimmter Signaturen gezielt abgefangen und – ohne ihren

entschlüsselten Inhalt zu kennen – wieder verschlüsselt in das WLAN eingespeist. Für einen Angriff sind zwar immer noch handfeste Netzwerk- und Computerkenntnisse erforderlich, aber zahlreiche Tools erlauben heute jedem, der sich eine Weile mit dem Thema beschäftigt, WEP zu knacken. WEP ist also keine Option mehr; Access Points und Clients, die keine moderneren Verschlüsselungsverfahren unterstützen, sollte man ausmustern.

3.2.5 WPA TKIP: Die Industrie bessert nach

Wi-Fi Protected Access (WPA) ist ein 2003 veröffentlichter Industriestandard der Wi-Fi Alliance, der auf einem Draft zu IEEE 802.11i basiert und aufwärtskompatibel zu IEEE 802.11i ist. Nachdem sich die Verabschiedung des neuen Sicherheitsstandards IEEE 802.11i verzögerte, wurde durch die Wi-Fi Alliance eine Teilmenge von IEEE 802.11i vorweggenommen und unter dem Begriff WPA als Pseudostandard etabliert. Bereits seit Ende August 2003 war WPA Bestandteil der Wi-Fi-Interoperabilitätstests. Für einen Anwender ändert sich bei WPA gegenüber WEP wenig: Die Sicherung des WLANs erfolgt durch die Eingabe eines Schlüssels in Client und Access Point, der nun aber mit 63 Zeichen deutlich länger sein darf. Diese Methode mit den sogenannten Pre-Shared Keys (PSK) ist – wie bei WEP – durch die Logistik beim Verwalten des Schlüssels in den Endgeräten nur in kleineren Netzwerken praktikabel. Der Schlüssel dient zur Authentisierung der Teilnehmer im WLAN, für größere Netzwerke bietet WPA das Extensible Authentication Protocol (EAP) über IEEE 802.1x (RADIUS) an. Die Verschlüsselung der Datenpaket erfolgt in der Regel über TKIP (Temporal Key Integrity Protocol). Für WPA wurde TKIP zwingend vorausgesetzt, die Implementierung der Variante mit Advanced-Encryption-Standard (AES)-Verschlüsselung (AES) über CCMP war optional.

Alles auf einen Blick: Bei Ruckus ist die WLAN-Sicherheit eine einfache Angelegenheit.

In TKIP wird pro Paket ein neuer Schlüssel erzeugt, um die bisher statischen WEP-Schlüssel zu vermeiden. Ein solcher Schlüssel entsteht durch Anwendung einer Hash-Funktion auf einen geheimen symmetrischen Sitzungsschlüssel, den Initialisierungsvektor und eine Paketsequenznummer. Der Sitzungsschlüssel wiederum wird aus einem gemeinsamen Schlüssel abgeleitet: dem Pre-Shared Key, der in allen Endgeräten eingetragen ist oder im Rahmen der Authentisierung über IEEE 802.1x übermittelt wird.

Ältere Betriebssysteme und Treiber sind meist nicht ohne Änderungen oder Updates in der Lage, WPA zu nutzen. Windows XP benötigt beispielsweise einen Patch, um als Client WPA anzubieten. Weil WPA auch höhere Anforderungen an die Rechenleistung der WLAN-Hardware stellt, ließen sich einige Netzwerkkarten und Access Points selbst mit Firmware-Updates nicht zur Zusammenarbeit mit WPA bewegen. Allerdings sind bei aktuellen Produkten keine Schwierigkeiten mehr bekannt. Dafür ist es Angreifern inzwischen gelungen, auch in WPA-TKIP-geschützte Funknetzwerke einzudringen. Die Täter verwenden hierzu unter anderem Wörterbuch-Attacken, anders als bei WEP kommt es also auf die Qualität des verwendeten PSK an. Er sollte möglichst lang sein und nicht aus natürlicher Sprache bestehen, sondern Kombinationen von möglichst kryptischen Zahlen-, Buchstaben- und Sonderzeichen enthalten. Befürchtungen über eine Schwachstelle in WPA gibt es schon seit 2004, in den folgenden Jahren tauchten immer mehr Tools auf, mit denen sich der Angriff automatisieren und vor allem beschleunigen ließ. Allerdings erfordert eine solche Attacke weit mehr Wissen und Fähigkeiten als ein Angriff auf WEP und wird daher nicht so oft vorkommen.

Trotzdem wird mittelfristig der Umstieg von WPA nach WPA2 empfohlen. Aktuelle WLAN-Produkte bieten ausnahmslos beide Verfahren an, in der entsprechenden Auswahlliste tauchen sie direkt untereinander auf. Windows XP erfordert einen Patch, Windows 7 beherrscht WPA2 bereits im Auslieferungszustand.

3.2.6 Sicher im WLAN mit WPA2 und AES

Im Jahr 2004 wurde WPA2, die Folgeversion von WPA, verabschiedet und im Sommer 2004 mit dem Zertifizierungsprozess begonnen. Seit Herbst 2006 ist eine WPA2-Zertifizierung zwingender Bestandteil einer Wi-Fi-Zertifizierung. WPA2 deckt alle zwingenden Anforderungen von IEEE 802.11i ab, inklusive des AES-Modus CCMP. Auch bei WPA2 gibt es einen Pre-Shared Key (PSK) zum Einsatz in kleineren Netzwerken sowie die Möglichkeit, über 802.1X (RADIUS) eine zentralisierte Authentisierung vorzunehmen. WPA2 nutzt für die Verschlüsselung den Advanced Encryption Standard (AES) und gilt per Stand heute bei einem ausreichend komplexen Schlüssel als nicht mit vernünftigem Aufwand knackbar.

Zwar existieren in der theoretischen Mathematik erste Ansätze, die auch bei diesem Verfahren ein Berechnen der Schlüssel erlauben sollen, doch die Rechenleistung derzeitiger Computer ist dafür noch zu gering. Ältere Access Points und Netzwerkkarten lassen sich selten auf WPA2 aufrüsten, die Prozessoren schaffen

die höhere Rechenleistung nicht, die für den Einsatz von AES benötigt wird. Auch die Anwendung von WPA2 ist in der Praxis für den Benutzer einfach: In den Sicherheitseinstellungen des WLANs wird WPA2 mit der Variante „TKIP+AES“ gewählt, und ein ausreichend sicherer Schlüssel wird in das Feld für den Pre-Shared Key eingetragen.

3.2.7 Der richtige Aufstellort: Gewusst wo

Kleine Ursache, große Wirkung – wer sich ein paar Gedanken über den richtigen Aufstellort seines DSL-Routers oder Access Points macht, kann Angriffen schon physikalisch einen Riegel vorschieben. Je nach Qualität des Funkmoduls im Access Point sendet er seine Datenpakete mehr oder weniger weit aus. Abhängig von der Umgebung, in der er aufgestellt ist, decken die Funksignale nach einem kaum vorhersagbaren Muster die Räume der eigenen Wohnung oder des Hauses ab. Stahlbetonwände wirken stark dämpfend, Reflektionen durch Möbel können die Reichweite erhöhen. Normalerweise kennt man eher das Problem, dass der Access Point nicht in alle benötigten Räume hineinreicht, doch die Wahl des richtigen Aufstellorts kann auch dafür sorgen, dass das eigene WLAN nicht auf der Straße oder dem Parkplatz gegenüber empfangen werden kann.

Generell ist die Aufstellung in der Mitte des Büros oder der Wohnung ein guter Startpunkt, dann kann man je nach gewünschter Ausleuchtung der Räume die Position des Access Points oder auch nur der Antennen verändern. Um die Ausbreitung zu messen, ist ein Tool wie Netstumbler (www.netstumbler.com) hilfreich, das alle WLANs im Umkreis kontinuierlich mit ihrer Signalstärke anzeigt. Natürlich können Angreifer durch den Einsatz von Richtantennen mehr Reichweite erzielen, aber das setzt eine bessere Vorbereitung und einen gezielten Angriff voraus.

3.2.8 Basisregeln: Updates machen und Standardpasswörter ändern

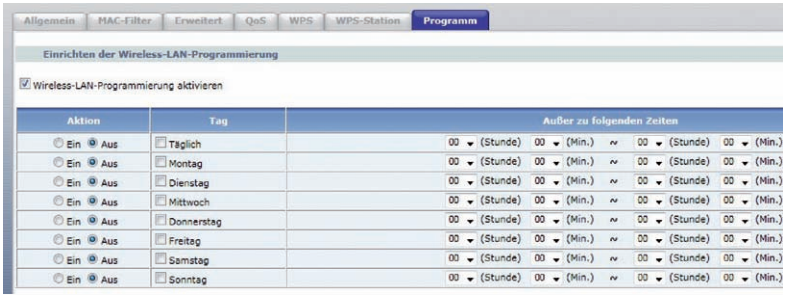
Zu den ersten Dingen, die man mit seinem neuen Access Point tun sollte, gehört das Ändern der Standardpasswörter für den Managementzugang. Fast alle Hersteller nutzen dafür eine gut dokumentierte Zahlen- oder Buchstabenkombination wie „1234“ oder „Admin“. Auch der Name des Herstellers wird gern verwendet. Bekommt ein Angreifer Zugriff auf den Access Point oder Router, wird er als Erstes versuchen, den rechtmäßigen Besitzer auszusperren, indem er das Standardpasswort ändert, sofern es noch eingetragen ist.

Natürlich lassen sich Access Points auf den Auslieferungszustand zurücksetzen, aber das dauert und ist umständlich, und bis man erkannt hat, dass ein Angriff stattfindet und man nicht nur das Passwort vergessen hat, kann viel Zeit vergehen. Besser ist es, das Passwort sofort zu ändern. Ebenfalls wichtig ist das Updaten der Firmware. Für die meisten Access Points und Router mit WLAN-Funktion gibt es

schon zum Zeitpunkt der Auslieferung neuere Firmware-Dateien, die Fehler beheben oder weitere Funktionen hinzufügen. Daher sollte, sobald die Internetverbindung steht, ein Update der Firmware durchgeführt werden.

3.2.9 Netzwerk einfach mal abschalten

Im Zuge der Green-Ethernet-Welle haben viele der neuen Access Points und Router Zeit- oder manuelle Schalter eingebaut, mit denen das WLAN abgeschaltet werden kann. Der Zeitschalter lässt sich meist pro Wochentag konfigurieren, sodass man unter der Woche, wenn ohnehin niemand zu Hause ist, das WLAN erst ab dem späten Nachmittag aktivieren kann. Das spart Strom und beugt Angriffen sehr wirkungsvoll vor.



Abschalten hilft immer: Eine Zeitsteuerung für das WLAN sorgt zu den deaktivierten Zeiten für absolute Sicherheit und spart darüber hinaus Strom.

3.2.10 Zugang nur auf Einladung: Access-Control-Listen

Selbst ganz alte WLAN-Hardware beherrscht die Zugangssicherung per Access Control List (ACL). Dabei wird die eindeutige MAC-Adresse eines Clients in eine Liste eingetragen; fortan können nur diese Clients Verbindung mit dem Access Point aufnehmen.

Nur wer drin ist, darf ins WLAN: eine Access-Control Liste bei Ruckus.

Das Verfahren ist aufgrund der manuellen Verwaltung relativ umständlich und wird schon ab mehr als fünf Clients unpraktisch. Zudem ist es sehr leicht möglich, eine MAC-Adresse zu fälschen, wenn man die korrekte MAC vorher mit einem Protokoll-Analyzer abgehört hat. Dennoch, wer nur einen oder zwei Computer im WLAN nutzt und auch keinen Freunden oder Besuchern regelmäßig den Zugang zum Internet gestatten will, kann über die ACL eine zusätzliche Hürde aufbauen.

Schützt nur rudimentär: keine DHCP-Funktion bei einem APC Access Point.

Ebenfalls möglich ist der Verzicht auf die automatische Zuteilung von IP-Adressen per DHCP. Selbst wenn ein unberechtigter Nutzer eine Verbindung zum WLAN aufbauen kann, muss er immer noch eine korrekte IP-Adresse herausfinden. Weil der Standardadressbereich für Consumer-Produkte fast immer 192.168.0.x ist, sollte man diesen ebenfalls ändern. Kein DHCP zu nutzen ist allerdings nur in sehr statischen Umgebungen praktikabel, in denen auch keine Endgeräte in anderen Netzwerken wie am Arbeitsplatz genutzt werden.

3.2.11 VPN: sicherer Tunnel inklusive

Ein Virtual Private Network ist für den Zugang zu einem WLAN im privaten Bereich eine reichlich extreme Maßnahme. Der verschlüsselte Tunnel verhindert, dass ein Angreifer selbst nach einem erfolgreichen Angriff auf das WLAN Zugang zum Netz bekommen oder die Datenpakete der anderen Teilnehmer im LAN belauschen kann. Allerdings ist dazu ein VPN-Server im eigenen Netz notwendig, der als Gateway die Schnittstelle zwischen WLAN und LAN regelt. Eine kostenlose Variante ist die Open-Source-Lösung OpenVPN. Der Aufwand für die Konfiguration ist jedoch nicht zu unterschätzen und nur etwas für fortgeschrittene Benutzer.

Ein VPN kann jedoch sinnvoll sein, wenn man häufig öffentliche Hotspots benutzt und dort die Sicherheit seiner übertragenen Daten erhöhen möchte. Dazu installiert man den Client auf seinem PC und verbindet sich, nachdem der Zugang zum WLAN steht, als Erstes mit dem VPN-Server. Nachdem sich Client und Server gegenseitig authentisiert haben, erfolgt die weitere Kommunikation verschlüsselt. Es gibt zahlreiche Anbieter von VPN-Lösungen speziell für den Einsatz am Hotspot wie Boingo, AnchorFree oder Hotspot Shield. Oft haben auch die Betreiber der

Hotspots wie T-Mobile (www.t-mobile.de) speziell für ihre Umgebungen zugeschnittene Software im Angebot.

3.2.12 RADIUS: Zugang nur nach Anmeldung

RADIUS (Remote Authentication Dial-In User Service) oder auch 802.1x ist ein zentraler Authentifizierungsserver, an den sich Services für die Authentisierung von Clients in einem physischen oder virtuellen Netzwerk (VPN) wenden. Der RADIUS-Server übernimmt dabei die Überprüfung von Benutzername und Kennwort. Die dabei verwendeten Daten entnimmt der RADIUS-Server entweder eigenen Konfigurationsdatenbanken oder zieht die Informationen aus Verzeichnisdiensten wie Microsoft Active Directory oder Novells eDirectory (www.novell.com/de-de/products/edirectory/).

RADIUS verwaltet generell den Zugang zum Netz, das kann ein physikalischer Port an einem Switch sein oder ein virtueller Port an einem Access Point. Durch das zentrale Management können auch große Netzwerke mit vielen Benutzern einfach verwaltet werden. Der Client heißt im 802.1x Umfeld „Supplicant", das Gerät, das den Netzwerkzugang herstellt, trägt den Namen „Authenticator". Im WLAN wird diese Funktion vom Access Point beziehungsweise WLAN Controller wahrgenommen. Der Authentication Server ist der eigentliche RADIUS-Server.

Die Authentisierung geschieht über das Extensible Authentication Protocol (EAP). Dabei läuft die Kommunikation über die LAN- beziehungsweise WLAN-Schnittstelle zwischen Supplicant und Authenticator mit der Variante EAP over LAN (EAPOL). EAPOL gestattet die Übertragung von EAP-Nachrichten auf Layer-2. Auf diese Weise wird eine Authentisierung am Netzzugangspunkt ermöglicht, bevor eine Kommunikation auf IP-Ebene und auf höheren Protokollebenen stattfinden kann. Die Kommunikation zwischen Authenticator und Authentication Server geschieht über RADIUS, wobei die EAP-Nachrichten als RADIUS-Attribute übertragen werden.

Ein kostenloser RADIUS-Server ist FreeRadius (www.freeradius.org), allerdings erfordert er den Einsatz von Linux als Plattform, da der Windows-Port veraltet ist und nicht mehr gepflegt wird. Auch einige Access Points enthalten RADIUS-Server, darunter die Geräte von Lancom (www.lancom-systems.de) oder Access Points die auf die Open-Source-Firmware DD-WRT umgerüstet wurden. Ein einfach zu bedienender RADIUS-Server für Windows ist WinRadius (www.itconsult2000.com), allerdings ist die Software auf fünf Nutzer beschränkt

Elmar Török

Elmar Török arbeitet seit 1993 als Autor und Fachjournalist im Bereich Netzwerke und Telekommunikation. Mittlerweile hat er neben zwei Büchern einige Hundert Artikel für zahlreiche Medien – online wie offline – geschrieben, darunter PC Professionell, LANline, c't, IT-Administrator, sueddeutsche.de. und TecChannel.

3.3 Workshop – Freeradius unter Linux einrichten

Insgesamt 35 unterschiedliche RADIUS-Server listet die englische Wikipedia-Enzyklopädie auf. Hersteller wie Microsoft und Cisco bieten Server an oder integrieren diese in ihre Geräte. Einer der bekanntesten RADIUS-Vertreter ist Freeradius. Diesen Open-Source-Server gibt es sowohl für Linux als auch für Windows. Die Windows-Version nutzt Cygwin, um unter dem Microsoft-Betriebssystem laufen zu können. Als Download steht auf der Homepage die Version 1.1.7 zur Verfügung (www.freeradius.net/Downloads.html). Die Linux-Variante hat schon weitere Entwicklungsschritte hinter sich gebracht zurzeit ist Version 2.1.10 zu haben. Hiervon existiert keine Windows-Variante; die Betreiber von freeradius.net haben es bislang nur geschafft, 2.0.x und ältere Pakete auf Windows XP zu kompilieren.

RADIUS wird für die Authentifizierung, die Autorisierung und die Zugangssteuerung benutzt. Sehr passend wird es im Entwicklernetzwerk von Microsoft erklärt: „Ein RADIUS-Client (normalerweise ein DFÜ-Server, VPN-Server oder drahtloser Zugriffspunkt) sendet Benutzeranmeldeinformationen und Verbindungsparameter in Form einer RADIUS-Meldung an einen RADIUS-Server. Der RADIUS-Server authentifiziert und autorisiert die Anfrage des RADIUS-Clients und sendet eine RADIUS-Antwortmeldung zurück."

RADIUS-Clients senden darüber hinaus Kontoführungsmeldungen an einen RADIUS-Server. Sogenannte RADIUS-Proxys werden ebenfalls verwendet. Dieser Proxy schickt RADIUS-Meldungen zwischen RADIUS-kompatiblen Computern hin und her. Authentifizierungen im RADIUS-Protokoll werden über den UDP-Port 1812 gesendet (einige senden über den Port 1645). Der folgende UDP-Port 1813 (oder 1646) wird für die RADIUS-Kontoführungsmeldungen benutzt. Jedes Datenpaket enthält jeweils nur eine einzige RADIUS-Meldung.

3.3.1 RADIUS-Protokoll für Benutzer und Geräte

Das RADIUS-Protokoll existiert schon seit 1991. Es wurde von Livingston Enterprises entwickelt und zunächst an der Universität Michigan und verbundenen Instituten eingesetzt. 1997 wurde das Protokoll zu einem Internetstandard erklärt; es ist in den RFCs 2039, 2865 und 2866 beschrieben. Das Entwicklungsunternehmen hat den Quellcode veröffentlicht, und heutzutage wird RADIUS als typische Implementation für 802.1X-Netzwerkzugänge genutzt.

Eingesetzt werden RADIUS-Server daher häufig von Internet-Service-Providern oder von Hochschulen. Dort können dann mithilfe eines Authentifizierungsservers auch lokal unbekannte Teilnehmer den Netzzugang nutzen. Doch nicht nur Benutzer, auch Geräte können sich per RADIUS im Netzwerk identifizieren. Benutzer wie Geräte werden in der Fachsprache als *Supplicant* tituliert, die über einen *Authenticator* – quasi einen Türsteher – eine Verbindung mit dem Netzwerk

oder Einlass begehren. Der Authenticator ist oft ein 802.1X-fähiger Netzwerk-Switch, ein Router oder ein WLAN-Access-Point. Er erfragt mithilfe von PAP-, CHAP- oder EAP-Authentikation die Legitimation bei einem Authentication -erver, in diesem Fall einem RADIUS-Server. Der sendet als Antwort zurück: Zugang gewährt, Zugang verboten oder „Weitere Daten erforderlich". Wird der Zugriff gewährt, prüft der RADIUS-Server oft noch, auf welche Ressourcen ein Benutzer zugreifen darf – etwa das VPN oder nur das interne WLAN. Passwörter werden dabei nicht im Klartext übertragen, sondern mittels eines MD5-Hash-Algorithmus. Allerdings wird das nicht als starker Schutz betrachtet, weshalb zusätzliche Methoden wie beispielsweise IPsec-Tunnel benutzt werden. RADIUS-Server prüfen die Benutzerdaten zum Beispiel mithilfe von Textdateien, LDAP-Servern oder SQL-Datenbanken. Wie lange RADIUS allerdings noch das Protokoll der Wahl ist, ist fraglich. Mit Diameter steht schon der Nachfolger fest. Als Transport-Layer nutzt es das Stream Control Transmission Protocol (SCTP) oder das ähnliche TCP.

3.3.2 Freeradius unter Linux installieren

Von Freeradius gibt es für verschiedene Linux-Derivate bereits vorgefertigte Pakete, ebenso für Mac OS, BSD und Windows. In den verschiedenen Linux-Versionen sind meist mehrere Pakete für unterschiedliche Aufgaben enthalten: In Ubuntu etwa wird das eigentliche Paket freeradius flankiert von Paketen mit Modulen für iODBC, LDAP, PostgreSQL, MySQL und Kerberos; standardmäßig unterstützt Freeradius bereits das Systempasswort, PAM und Textdateien mit Anmeldeinformationen.

Im Paket *freeradius-dialupadmin* stehen PHP-Skripte mit einer web-basierten Schnittstelle, um einen Freeradius-Server zu administrieren, der die Anmeldeinformationen entweder in SQL oder in LDAP speichert. Das Paket freeradius-utils schließlich enthält verschiedene Programme für RADIUS-Clients wie radclient und radeapclient , radsniff , radwho und smbencrypt . Mit dem Befehl

```
sudo apt-get install freeradius
```

werden der Freeradius-Server und die Utilities installiert. Das Installationsskript legt den Benutzer *freerad* an und fügt diesen den Gruppen *shadow* und *ssl-cert* hinzu. Anschließend werden die SSL-Zertifikatseinstellungen aktualisiert und ein SSL-Schlüssel erzeugt. Mit dem Hinweis

```
* Starting FreeRADIUS daemon freeradius [ OK ]
```

schließt das Installationsskript nach erfolgreichem Start des Servers ab.

Um zu prüfen, ob der RADIUS-Server korrekt läuft, starten Sie den Server mit dem Parameter -C:

```
sudo freeradius -C
```

```
 Module: Checking post-auth {...} for more modules to load
 } # modules
} # server
radiusd: #### Skipping IP addresses and Ports ####
listen {
        type = "auth"
        ipaddr = *
        port = 0
}
listen {
        type = "acct"
        ipaddr = *
        port = 0
}
listen {
        type = "auth"
        ipaddr = 127.0.0.1
        port = 18120
}
Configuration appears to be OK.
thomas@hogwarts:~$
```

Check: Die Ausgabe des Befehls „freeradius -XC“, welche Module geprüft und welche nicht geprüft werden. Die letzte Zeile deutet in dem Fall darauf hin, dass die Konfiguration korrekt sein könnte.

Mit dem Kommando überprüfen Sie die Konfiguration. Wird der Befehl ohne weitere Ausgaben und Meldungen beendet, deutet das darauf hin, dass die Konfiguration vermutlich korrekt ist – sie muss es allerdings nicht sein, da nicht alle Eventualitäten geprüft werden. Wenn Sie wissen wollen, welche Module auf korrekte Konfiguration überprüft werden, benutzen Sie stattdessen die Parameter *-XC*. Der Parameter *-X* schaltet in den Debug-Modus. Im Zusammenspiel mit *-C* erfahren Sie so auch, welche Module nicht überprüft werden.

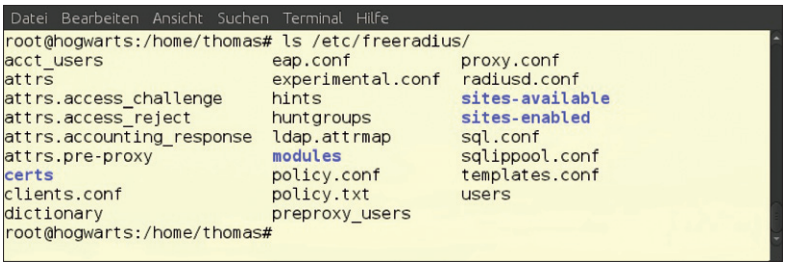
3.3.3 Freeradius konfigurieren

Die Konfigurationsdaten des Freeradius-Servers stehen üblicherweise unter */etc/raddb*. In Ubuntu und Debian finden Sie diese Dateien im Verzeichnis */etc/freeradius*. Beachten Sie, dass Sie die Inhalte des Verzeichnisses nur als *root* sehen können; auf einer Konsole in Ubuntu wechseln Sie zur root-Identität mit dem Befehl *sudo su* und Ihrem Passwort. Im Konfigurationsverzeichnis sucht der Server nach Dateien wie dem Wörterbuch und den Benutzerdaten. Auch die 800 Zeilen lange und gut dokumentierte Hauptkonfigurationsdatei *radiusd.conf* ist dort zu finden.

```
thomas@hogwarts:~$ less /etc/services | grep radius
datametrics     1645/tcp        old-radius
datametrics     1645/udp        old-radius
radius          1812/tcp
radius          1812/udp
radius-acct     1813/tcp        radacct         # Radius Accounting
radius-acct     1813/udp        radacct
thomas@hogwarts:~$
```

Lauschprotokoll: Auf welchen Ports Freeradius horcht, steht in der Datei /etc/services. Mit dem Befehl „less /etc/services | grep radius“ erhalten Sie sofort die gewünschten Informationen.

Auf welchen Ports Freeradius horcht, steht in der Datei */etc/services*. Wie oben erwähnt, sind das standardmäßig die Ports 1812 und 1813; auch der Freeradius-Server macht hier keine Ausnahme. Der Port 1813 dient dabei für die Accounting-/Konto-Informationen. Dass der Server die Information über die Ports aus der Datei */etc/service*s bezieht, liegt an der Einstellung der Direktive in der Datei */etc/freeradius/radiusd.conf*: Da steht *port = 0*, und das bedeutet, dass die Einstellungen aus der */etc/services* geholt werden sollen.



Geordnet: Unter Debian und Ubuntu stehen die Konfigurationsdateien von Freeradius im Verzeichnis /etc/freeradius.

Den Port können Sie auch manuell mit dem Parameter *-p PORT* festlegen. In dem Fall wird die Direktive in der Konfigurationsdatei */etc/raddb/radiusd.conf* ignoriert. Wenn Sie allerdings den Port manuell festlegen, müssen Sie noch mit *-i IP-ADRESSE* die IP-Adresse angeben, die der Server nutzt, also etwa:

```
freeradius -p 1645 -i 192.168.3.4
```

3.3.4 Freeradius mit virtuellen Servern

Freeradius kann auch mit virtuellen Servern umgehen. Das hat den Vorteil, dass RADIUS-Anfragen nur an den betroffenen Server geleitet werden. Wollen Sie virtuelle Server neu definieren, dann legen Sie pro virtuellen Server eine Datei im Verzeichnis */etc/freeradius/sites-enabled/* an.

Die sieht ähnlich aus wie das folgende Beispiel:

```
server foo {
listen {
ipaddr = 127.0.0.1
port = 2000
type = auth
}

authorize {
update control {
```

```
Cleartext-Password := "bob"
}
pap
}

authenticate {
pap
}
}
```

Wenn Sie danach in einen Terminal den Befehl

```
$ radtest bob bob localhost:2000 0 testing123
```

eingeben, sollte Ihnen der Server den Zugang gewähren. Ein Tipp zum Schluss: Sehen Sie sich alle Dateien im Verzeichnis /etc/freeradius und darunter genau an. Sie enthalten wertvolle Informationen zum Einrichten des RADIUS-Servers. Ziehen Sie außerdem das Howto (http://wiki.freeradius.org/create/Basic+configuration+HOWTO), die Dokumentation (http://freeradius.org/doc/) und die FAQ (http://wiki.freeradius.org/index.php/FAQ) auf der Freeradius-Homepage zurate.

Thomas Hümmler

Thomas Hümmler ist freiberuflicher Journalist und beschäftige sich mit Betriebssystemen, Office-Anwendungen, freier Software, dem Internet und anderen IT- und Technik-Themen.

TecChannel-Links zum Thema	Webcode	Compact
Workshop – Freeradius für Linux einrichten	2036067	S.115
Praxis: Netzwerkzugriffsschutz (NAP) in Windows-Umgebungen	2035833	S.94
Tipps und Tricks – WLANs sicher konfigurieren	2035470	S.105

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

4 WLAN

Der zunehmende Einsatz von Smartphones und Tablet-PCs in Firmen wird weltweit für ein starkes Wachsen von drahtlosen Netzen sorgen. Laut aktuellen Studien bauen Unternehmen neue drahtlose Netze auf und erweitern bestehende Infrastrukturen. Das stellt eine Herausforderung für IT-Abteilungen dar.

4.1 iPad und iPhone zwingen zu WLAN-Ausbau

Der zunehmende Einsatz von Smartphones und Tablet-PCs in Firmen wird weltweit für ein starkes Wachsen von drahtlosen Netzen sorgen. Laut aktuellen Studien bauen Unternehmen neue drahtlose Netze auf und erweitern bestehende Infrastrukturen. Eine Herausforderung für IT-Abteilungen.

Beim Ingolstädter Automobilkonzern Audi arbeitet man bereits seit einem halben Jahr daran, für den Einsatz von iPad und iPhone in der Fahrzeugfertigung die drahtlosen Netze zu erweitern. „Durch das iPad werden sich Änderungen in der gesamten Netzwerkarchitektur ergeben, weil wir zunehmend über WLAN und UMTS auf unsere Daten zugreifen“, meinte dazu schon im Oktober Jürgen Holderried. Dafür, so der Leiter der IT-Services bei der Audi AG, sei es erforderlich, die Sicherheitszonen umzubauen, „um so eine geeignete, sichere und stabile Umgebung für den Betrieb gewährleisten zu können – egal, ob der Anwender sich im Firmennetz aufhält oder unterwegs ist“. So wie Audi geht es derzeit wahrscheinlich vielen Unternehmen weltweit, die an Projekten arbeiten, iPad und iPhone im Unternehmen produktiv einzusetzen. Davon sind – auch das zeigt das Beispiel Audi – längst nicht nur drahtlose Netze außerhalb der Firmen betroffen, sondern zunehmend auch die innerhalb der IT-Infrastruktur.

Der Boom, haben aktuelle Studien ergeben, sorgt auch bei den Produzenten von WLAN-Ausrüstung für Hochzeiten. So haben die Marktforscher von Infonetics Research herausgefunden, dass der weltweite Umsatz mit Drahtloszubehör allein im vierten Quartal 2010 um 28 Prozent im Vergleich zum Vorjahresquartal auf 769 Millionen US-Dollar (rund 558 Millionen Euro) gestiegen ist.

4.1.1 Cisco, Aruba und HP liegen vorne

Ein Report von Marktforscher Dell’Oro bestätigt diesen Wachstumstrend: Für das komplette Jahr 2010 seien die Umsätze mit WLAN-Accessoires um 25 Prozent auf einen Gesamtwert von mehr als fünf Milliarden US-Dollar – das entspricht rund 3,6 Milliarden Euro – gestiegen. Dabei würden die firmeninternen Netze den Löwenanteil ausmachen.

Allerdings rangiert der weltweite Umsatz in Höhe von 18,8 Milliarden US-Dollar (rund 13,6 Milliarden Euro) mit Netzwerktechnologien noch immer deutlich vor dem der WLANs. Bei den Wachstumsraten dagegen liegen die Drahtlostechnologien mit zehn Prozent deutlich vorne (Netzwerktechnologien: plus ein Prozent).

Die wachsende Zahl mobiler Endgeräte habe bei den Firmen Aktivitäten für den Aufbau neuer und den Ausbau bestehender Drahtlosnetzwerke ausgelöst, so das Ergebnis beider Studien. Die Netzwerke müssten in der Lage sein, immer mehr Smartphones und Tablet-PCs mit dem Internet und den firmeneigenen Netzwerken zu verbinden. Wo das nicht gehe, müsse man die bestehenden Kapazitäten eben erweitern. Beim Umsatz vorne liegen drahtlose Systeme von Cisco, gefolgt von Aruba Networks, Hewlett-Packard und Motorola, hat Infonetics in seiner Studie herausgefunden.

Allein in den vergangenen sechs Monaten habe sich der Markt stärker verändert als in den sechs Jahren davor, stellt Roger Hockaday, Marketingdirektor des Anbieters Aruba in Europa, fest. Der größte Teil dieses Wachstums gehe auf das Konto von Apples iPad. Vor der Auslieferung des Tablet-PCs seien drahtlose Netze in Unternehmen eher ein Luxusgut gewesen, beispielsweise, um Besuchern Internetempfang zu ermöglichen.

4.1.2 Netzwerkarchitekturen müssen auf den Prüfstand

Heutzutage sei daraus aber schon eine Notwendigkeit geworden, weil die Mitarbeiter eher auf drahtlose Verbindungen Wert legten als auf drahtgebundene. So könnten sie Geräte wie das iPad nicht nur in ihrem Büro oder in Konferenzräumen, sondern überall im Unternehmen einsetzen.

Die IT-Abteilungen in den Unternehmen müssten daher ihre Netzwerkarchitekturen auf den Prüfstand stellen, fordert Hockaday. Es seien mit Drahtlosnetzen größere Gebiete abzudecken als zuvor.

Durch neue Geräte mit wachsenden Fähigkeiten – so verfügt zum Beispiel das Apple iPad 2 über zwei integrierte Kameras und FaceTime-Technologie für einfache Videokonferenzen – entsteht in exponentieller Größenordnung zusätzlicher Bedarf an Bandbreite.

Thomas Pelkmann

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation CIO.

TecChannel-Links zum Thema	Webcode	Compact
iPad und iPhone zwingen zuWLAN-Ausbau	2034964	S.120
Test: WLAN-Management aus der Cloud	2035994	S.122
Virtual Wi-Fi – Windows 7 als WLAN-Access-Point einsetzen	2035894	S.128

4.2 Test: WLAN-Management aus der Cloud

In vielen Bereichen sind Cloud-Services längt etabliert, denkt man etwa an Storage aus der Cloud oder an Mail-Systeme in der Cloud. Ein WLAN aus der Cloud klingt hingegen zunächst befremdlich. Dabei hat der Gedanke bei näherer Betrachtung durchaus etwas für sich: Warum soll sich ein Unternehmen einen teuren WLAN-Controller oder -Switch kaufen? Oder warum sich mit explodierenden Kosten herumärgern, wenn im Enterprise mehrere Controller für verschiedene Standorte erforderlich sind? Und was passiert, wenn der Controller mit dem Wachstum des WLAN-Netzes nicht Schritt hält?

Mit der Meraki-Lösung könne man flexibel auf sich ändernde Anforderungen reagieren, ohne in zentrales Administrations-Equipment investieren zu müssen. Grund genug, die Lösung einem Praxistest zu unterziehen.

Über den deutschen Distributor Sysob wurden uns zwei Meraki-Access-Points vom Typ „MR16“ sowie eine Lizenz für den „Enterprise Cloud Controller“ zu Verfügung gestellt. Ein Access Point steht dabei mit 649 Euro in der Preisliste, und für die Jahreslizenz des Cloud Controllers sind 150 Euro (jeweils zuzüglich Mehrwertsteuer) zu veranschlagen. Beim MR16 handelt es sich um einen 802.11n-Access-Point mit zwei Funkteilen, sodass die 2,4- und 5-GHz-Frequenzbänder gleichzeitig genutzt werden können. Für das Gerät, das auch die älteren 802.11-Standards a, b und g unterstützt, gibt Meraki einen Datendurchsatz von bis zu 600 Mbit/s an.

4.2.1 Testaufbau und Inbetriebnahme

Als Testszenario wählten wir eine Multihousing-Umgebung, in dem an zwei Standorten identische WLANs abgebildet werden sollten. Die physikalische Installation der Accees Points unterscheidet sich nicht von der anderer. Per Ethernet wird die Verbindung zum LAN hergestellt. Die Stromversorgung kann wahlweise über ein Netzteil oder Power over Ethernet erfolgen. Aufgrund seiner Leistungsfähigkeit sollte der MR16 an einen Gigabit-Ethernet-Switch angeschlossen werden.

Access Point: Der MR16 arbeitet mit zwei Funkteilen und unterstützt 802.11a/b/g/n.

Nach der Verkabelung steht einer Inbetriebnahme nichts mehr im Weg, wenn der Anwender folgenden Punkt beachtet: Der Access Point benötigt ausgehende Verbindungen auf den UDP-Ports 7351 und 9350 sowie den TCP-Anschlüssen 80, 443 7734 und 7752, um später mit dem Cloud Controller kommunizieren zu können.

Bei der ersten Inbetriebnahme sollte man sich nicht von den blinkenden LEDs des Access Point verunsichern lassen. Er nimmt Verbindung zu den Meraki-Servern auf und lädt, falls erforderlich, gleich ein Firmware-Update herunter – ein Umstand, den man Mitarbeitern mitteilen sollte, falls die Access Points nicht von IT-Fachpersonal installiert werden.

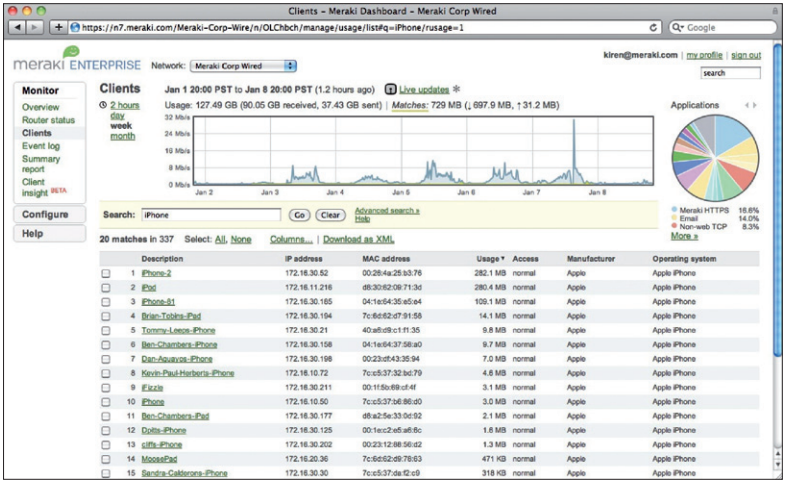
WLAN Access Point MR 16 Access Point	
Hersteller	Meraki (http://meraki.com)
Distributor	Sysob (www.sysob.com)
WLAN-Standards	802.11 a/b/g/n
Funkteil	je ein Sender für 2,4 und 5 GHz, gleichzeitiger Betrieb möglich
Performance	bis zu 600 Mbit/s
Sicherheit	WEP, WPA, WPA2
Stromversorgung	Power over Ethernet oder optionales Netzteil
Preis	649 Euro zzgl. MwSt.

4.2.2 Konfiguration per Browser

Die eigentliche Konfiguration erfolgt dann über den Cloud Controller, auf den via Browser per HTTPS zugegriffen wird – vom Hersteller als Meraki Dashboard bezeichnet. Beim ersten Aufruf ist ein Admin-Account einzurichten. Um die Access Points zu verwalten, müssen diese anhand ihrer Seriennummer beim Controller angemeldet werden. Sollen gleich mehrere Access Points hinzugefügt werden, empfiehlt sich eine andere Vorgehensweise: Wer eine Meraki-Ordernumber hat, erspart sich mit dieser die Eingabe einzelner Seriennummern und kann die Access Points en bloc aktivieren.

Beim Erstkontakt mit dem Dashboard überraschte die Administrationsoberfläche trotz der Funktionsvielfalt durch ihre Übersichtlichkeit. Über die vier Reiter *Monitor*, *Configure*, *Organization* sowie *Help* wird auf die Unterpunkte zugegriffen.

Unter dem Stichwort *Organization* erfolgen die grundlegenden Konfigurationsschritte, wie Eingabe der Lizenzinformationen, Vergabe des Netznamens oder Anlegen der Admin-Accounts. In die Tiefe des Controllers führt dann die Option *Configure*. Aufgrund der Vielzahl an Einstellmöglichkeiten sind hier nur die aus unserer Sicht interessantesten Funktionen dargestellt.



Admin-Oberfläche: Die Konfiguration erfolgt per Dashboard.

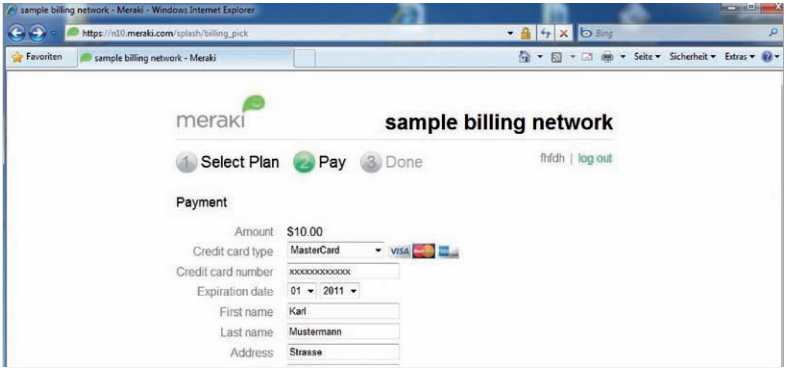
4.2.3 Arbeiten mit dem Dashboard

Allgemein sollte der Admin bei der Arbeit mit dem Dashboard auf einen Punkt achten: Ist er auf Netzwerkebene zugange, dann gelten alle Änderungen für alle Access Points an allen Standorten sowie alle WLANs. Die nächste Stufe ist die Konfiguration auf WLAN-Ebene – hier werden bis zu 15 SSIDs unterstützt -, wobei sich diese Einstellungen wiederum auf alle dazugehörigen Standorte und Access Points auswirken.

Darüber hinaus ist noch der Zugriff auf einzelne Access Points und Standorte möglich. Wer auf diese Unterscheidung achtet, wird mit der Admin-Oberfläche keine Problem haben.

Wie beim Surfen im Netz führen eine Art „Hyperlinks“ in weitere Untermenüs. Dabei ist das Gros der einzelnen Menüpunkte meist direkt mit einem Hilfe-Link versehen, sodass kaum auf das PDF-Handbuch zurückgegriffen wurde.

Positiv fiel uns die Zahl von bis zu 16 unterstützten SSIDs auf, die ein weites Feld an Einsatzmöglichkeiten eröffnen, etwa ein Kern-WLAN für eigene Mitarbeiter, ein zweites für freiberufliche Mitarbeiter und ein drittes für Partner. Ein viertes könnte dann für zahlende Gäste sein, um nur ein Beispielsszenario zu entwerfen. Für jedes WLAN können dabei beispielsweise eigene Filterregeln oder Bandbreitenbeschränkungen eingerichtet werden. Hier gefiel uns sehr gut, dass der Controller direkt die Möglichkeit offeriert, eigene Webvorschaltseiten zu entwickeln, die beim ersten Zugriff auf das WLAN angezeigt werden.



Simpel: Selbst kostenpflichtige Gäste-WLANs lassen sich mit wenigen Mausklicks einrichten.

Selbst ein einfacher Billing-Plan für zahlende WLAN-Benutzer lässt sich mithilfe des Controllers schon von Haus aus realisieren. So sind entsprechende Module zur Bezahlung via Kreditkarte bereits vorkonfiguriert. Die erzielten Einnahmen rechnet Meraki via Paypal dann mit dem Anwender ab.

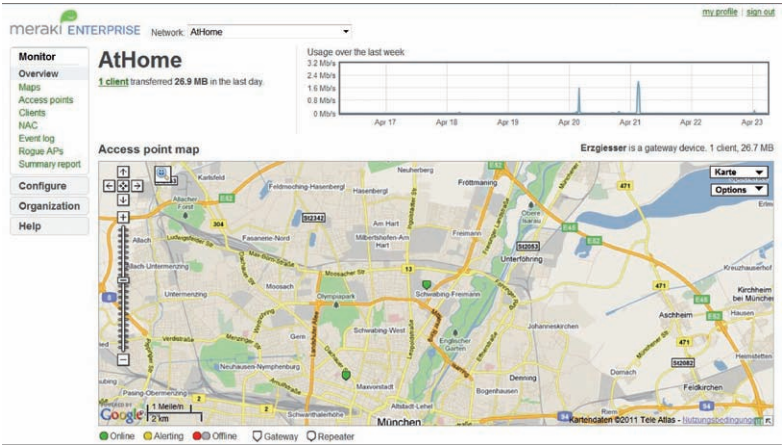
Eine andere clevere Option ist, dass der Controller prüfen kann, ob auf einem Client ein aktueller Virenscanner installiert ist, bevor er den Zugriff auf das WLAN ermöglicht. Weitere Features wie die automatische oder zeitgesteuerte Suche nach Rogue APs oder das Scannen nach Interferenzen, um einen störungsfreien Kanal zu finden, zeigen deutlich, dass der Hersteller Meraki mit seinen Access Points die Business-Klientel adressiert.

4.2.4 Intelligentes Monitoring

Die Konfiguration ist aber nur ein Teil des IT-Business; genauso wichtig ist es, den reibungslosen Betrieb der WLANs im Alltag überwachen zu können. Die entsprechenden Optionen hierzu findet der Administrator unter dem Punkt *Monitor*.

Beim Aufruf der Seite informiert eine Google-Maps-Karte über die Positionen der Access Points sowie ihren Betriebszustand. Alternativ zur Google-Karte können auch Gebäudepläne verwendet werden. Ein grünes Icon zeigt funktionierende Geräte, Rot steht für ausgefallene beziehungsweise nicht erreichbare Access Points, und ein gelbes Icon signalisiert, dass eine Fehlermeldung vorliegt.

Ein anderes Feature des Cloud Controllers sehen wir vor dem Hintergrund der deutschen Gesetzeslage (Datenschutz etc.) mit gemischten Gefühlen: Der Controller protokolliert WLAN-Zugriffe genau mit MAC-Adresse, Geräteart, Uhrzeit, Ort und Datenvolumen. Darüber hinaus analysiert er die übertragenen Daten und lässt so Rückschlüsse darauf zu, wozu der Anwender das WLAN genutzt hat (etwa Mailen oder Surfen).



Alles im Blick: Auf einer Google-Karte zeigt Meraki die Position und den Funktionsstatus der Access Points an. Eigene Gebäudepläne lassen sich integrieren.

Lässt man die rechtlichen Implikationen beiseite, sind das Funktionen, die aus Sicht des Netzwerkers nur zu begrüßen sind. Mit ihrer Hilfe ist eine proaktive Kapazitätsplanung möglich, oder der Administrator kann direkt reagieren, wenn unerwünschte Anwendungen wie P2P oder Streaming etwa die WLANs verstopfen.

WLAN Controller	
Hersteller	Meraki (http://meraki.com)
Distributor	Sysob (www.sysob.com)
Produkt	Enterprise Cloud Controller
Typ	WLAN-Management aus der Cloud
Performance	Administration von bis zu 1000 WLANs mit jeweils bis zu 10.000 Access Points
Plattform	bis zu 16 virtuelle APs (SSID), bis zu 16 VLANs (802.1q), Bridge Mode, NAT Mode, dynamische Kanaloptimierung, dynamische Frequenzwahl
Sicherheit	WEP, WPA, WPA2, 802.1x EAP, TKIP und AES, Rogue AP Entdeckung, NAC, Radius-Support, MAC-Listen, Walled Garden, Content-Filter
Weitere Features	Traffic Shaping, Vorschaltseiten, Billing-System, Monitoring, Traffic-Analyse, E-Mail-Alarm
Preis	Jahreslizenz 150 Euro, 3 Jahre 300 Euro, 5 Jahre 450 Euro, jeweils zzgl MwSt.

Über Störungen informiert das System zudem per E-Mail, wobei der Administrator selbst definieren kann, über welche Vorfälle er unterrichtet wird: etwa ob ein Access Point ausgefallen, ob Rogue APs entdeckt wurden oder ob ein Co-Administrator Veränderungen vorgenommen hat.

4.2.5 Fazit

Insgesamt überzeugt uns das Cloud-Konzept von Meraki: Zum einen muss der Anwender keine hohen Summen investieren, um eine gemanagte, kontrollierte WLAN-Umgebung aufzubauen. Zum anderen offeriert der Cloud-Controller eine Vielzahl an Administrations- und Konfigurationsoptionen, die bei anderen Lösungen oft in Form von Add-ons oder Zusatzmodulen zu erwerben sind.

Gerade die Vielfalt ist ein Pluspunkt: Egal, ob WLANs für mehrere Firmenstandorte, Bezahl-Hotspot oder getrenntes Gäste-WLAN, die unterschiedlichsten Szenarien lassen sich mit wenigen Mausklicks realisieren. Deshalb gebührt den Meraki-Entwicklern zum Schluss ein Lob für ihre Admin-Oberfläche: Sie haben es geschaff, eine Vielzahl an Features und Einstellmöglichkeiten so zu verpacken, dass das System auch ohne tagelanges Handbuchstudium bedienbar ist.

Vor- und Nachteile

Plus:

- Physikalische Installation durch Nicht-IT-Fachkräfte möglich
- Keine fixen Investitionen für WLAN Controller
- Einfache Bedienung und standortübergreifendes Remote-Management komplexer WLANs
- Vielfältige Einsatzmöglichkeiten (Billing, Vorschaltseiten etc.)
- Monitoring-Funktionen

Minus:

- Sende- und Empfangsleistung könnten besser sein (kann auch an der Bausubstanz liegen)
- Preis für Access Point
- Weder Netzteil noch Power-Injector für PoE gehören zum Lieferumfang

Jürgen Hill

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation Computerwoche.

4.3 Virtual Wi-Fi – Windows 7 als WLAN-Access-Point einsetzen

Per Virtual Wi-Fi können sich Client-Computer mit dem Windows-7-System kurzschließen und so die Internetverbindung des Systems nutzen. Diese virtuelle WLAN-Karte, die auf der eingebauten WiFi-Lösung aufsetzt, bezeichnet Microsoft auch als Wireless Hosted Network. In früheren Windows-Versionen konnte ein WLAN entweder im Ad-hoc-Modus oder im Infrastruktur-Modus betrieben werden. Bei Ersterem kann man Client-Computer anbinden, ohne eine Internetverbindung nutzen zu können. Beim häufigeren Infrastruktur-Modus verbindet sich der Windows-Rechner beispielsweise mit einem Router und nutzt dessen Internetverbindung. Beide Modi parallel zu betreiben ging nicht.

Hier setzt Wireless Hosted Network an. Die Technik dupliziert die echte WLAN-Karte als zweite virtuelle Verbindung. Diese erscheint als ganz normale Netzwerkverbindung und lässt sich auch genauso konfigurieren. Beide Verbindungen, also die physische und die virtuelle, können dazu mit verschiedenen Netzwerken verbunden sein. Das ermöglicht dann die Anbindung an verschiedene WLANs auch mit verschiedenen Verbindungsmodi. Das heißt: Andere Client-Computer verbinden sich ganz normal mit der virtuellen WiFi-Karte, während die physische Netzwerkkarte im Software Access Point mit dem echten WLAN verbunden ist.

4.3.1 Funktion und Voraussetzungen

Die Einrichtung ist sehr einfach durchzuführen, erfolgt aber über die Befehlszeile. Sind Sie mit dem Notebook unterwegs, können Kollegen oder Freunde auf diesem Weg per WLAN eine Verbindung mit dem Notebook aufbauen.

Ist das Notebook oder der Computer über ein Netzwerkkabel oder der WLAN-Karte mit dem Internet verbunden, können andere Clients per WLAN eine Verbindung zum Notebook herstellen und die Internetverbindung des Notebooks nutzen. Das funktioniert natürlich auch, wenn Sie per UMTS-Stick eine Internetverbindung herstellen. Außerdem können Sie mit der Funktion die Reichweite bestehender WLANs verlängern, indem Sie das Notebook als Repeater einsetzen.

Voraussetzung ist, dass die Virtual-Wi-Fi-Technik vom eingesetzten Treiber unterstützt wird, und auch die Netzwerkkarte muss die Funktion unterstützen. Das ist leider nicht immer der Fall. Klappt die Einrichtung bei Ihnen nicht, versuchen Sie, einen neuen Treiber zu installieren. Gelingt die Einrichtung auch mit einem neuen Treiber nicht, ist Ihre WLAN-Karte wahrscheinlich nicht kompatibel zur Virtual-Wi-Fi-Technik – leider unterstützen nicht alle Karten diese Funktion.

Windows 7 verwendet als Verschlüsselungstechnik WPA2, das heißt, die Verbindungen zum virtuellen WLAN sind sehr sicher. Allerdings müssen dazu natürlich der entsprechende Treiber und die Karte auch das WPA2-Protokoll unterstützen.

4.3.2 Flexibel ein- und ausschalten

Die Einrichtung nehmen Sie am schnellsten über die Eingabeaufforderung vor. Im Internet kursieren verschiedene Zusatz-Tools, allerdings müssen Sie diese installieren und belasten damit unnötig das System.

Sie können die Einrichtung in der Befehlszeile mit wenigen Schritten selbst vornehmen und über Verknüpfungen dann die Funktion an- oder ausschalten. Das hat den Vorteil, dass Sie sich selbst eine Batchdatei oder ein Skript schreiben, mit dem Sie den Access Point mit einem Klick einrichten und über Verknüpfungen dann konfigurieren.

Nach der erstmaligen Einrichtung können Sie diese Funktion jederzeit wieder deaktivieren und auch schnell erneut aktivieren. Im ersten Schritt müssen Sie die Funktion generell für Ihren Windows-Computer aktivieren. Anschließend steuern Sie die Anbindung von Computern über die virtuelle Netzwerkkarte. Das heißt, nach der Einrichtung der Lösung sind diese Befehle nicht erneut einzugeben, aber Sie können jederzeit die Anbindung anderer Clients ausschalten.

4.3.3 Schritt-für-Schritt-Einrichtung

1. Öffnen Sie eine Eingabeaufforderung über das Kontextmenü mit Administratorrechten.
2. Geben Sie den folgenden Befehl ein:
   ```
   netsh wlan set hostednetwork mode=allow ssid=<Name des
   Netzwerks> key=<Kennwort für den Verbindungsaufbau mit
   mindestens 8 Zeichen> keyUsage=persistent
   ```
   Den Namen des Netzwerks (SSID) und das Kennwort können Sie also frei wählen. Nach dem Befehl ist die Funktion aktiviert. Sie müssen den Befehl nicht erneut ausführen.
3. Anschließend erhalten Sie die Meldung der erfolgreichen Einrichtung; diese sind im Detail:
   • *Der Modus für das gehostete Netzwerk ist so festgelegt, dass das gehostete Netzwerk zugelassen wird.*
   • *Die SSID des gehosteten Netzwerks wurde erfolgreich geändert.*
   • *Die Benutzerschlüsselpassphrase des gehosteten Netzwerks wurde erfolgreich geändert.*
4. Starten Sie anschließend den Gerätemanager, zum Beispiel durch Eingabe von *devmgmt.msc* im Suchfeld des Startmenüs.
5. Überprüfen Sie, ob im Bereich Netzwerkadapter die neue Netzwerkkarte angezeigt wird. Diese listet Windows als Microsoft Adapter für Miniports virtueller Wi-Fis auf. Nur wenn keine Fehler erscheinen und der neue Adapter erscheint, unterstützen Ihre WLAN-Karte und der Treiber die Funktion. Erhalten Sie eine Fehlermeldung, hilft oft ein anderer Treiber.

6. Rufen Sie über *ncpa.cpl* die Netzwerkverbindungen auf. Auch hier muss eine neue Verbindung erscheinen. Diese baut auf die erstellte Virtual-Wi-Fi-Karte auf. Die neue Netzwerkverbindung kann eine Verbindung mit anderen WLANs aufbauen als die echte WLAN-Karte im System. Sie verwenden die virtuelle Karte zur Anbindung anderer Computer.
7. Der nächste Schritt besteht darin, dass Sie das Netzwerk aktivieren. Nach der Erstellung ist es zwar in Windows 7 schon integriert, aber noch nicht verfügbar. Dazu geben Sie den Befehl
   `netsh wlan start hostednetwork`
   in einer Eingabeaufforderung ein, die Sie mit Administratorrechten gestartet haben. Sie können diesen Befehl natürlich auch als Verknüpfung auf dem Desktop hinterlegen. Auf diesem Weg aktivieren Sie schnell und einfach das Netzwerk, wenn Sie es deaktiviert haben. Sie müssen die Meldung erhalten, dass Windows das Netzwerk erfolgreich gestartet hat. Suchen Sie auf anderen Computern oder auch mobilen Geräten wie iPhones oder anderen Smartphones nach neuen WLANs, erscheint das Netzwerk und ist bereit für den Verbindungsaufbau.

4.3.4 Virtual Wi-Fi konfigurieren und anhalten

Wollen Sie sich den Status des Netzwerks anzeigen lassen, öffnen Sie ebenfalls wieder eine Eingabeaufforderung mit Administratorrechten und geben den Befehl:

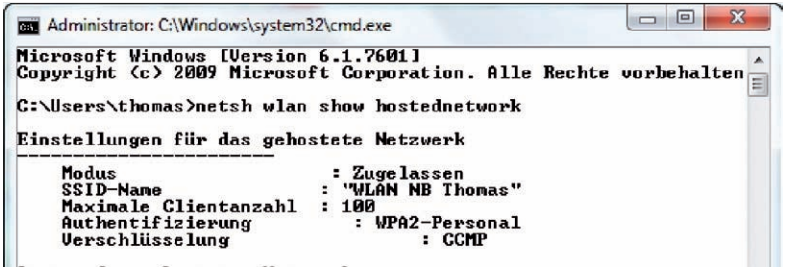
```
netsh wlan show hostednetwork
```

ein. Den Sicherheitsschlüssel zeigen Sie mit

```
netsh wlan show hostednetwork security
```

an. Wollen Sie den Schlüssel ändern, verwenden Sie den Befehl

```
netsh wlan set hostednetwork key=<Neues Kennwort>
```



Abfrage: Per Befehl können Sie sich den Status des virtuellen Netzwerks anzeigen lassen.

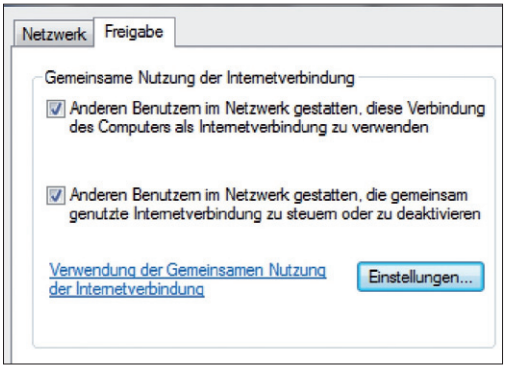
Der Befehl

```
netsh wlan show settings
```

zeigt die globalen Einstellungen für WLANs in Windows 7 an.

Damit die angebundenen Clients die Internetverbindung des Notebooks nutzen können, müssen Sie in den Eigenschaften der Netzwerkverbindung, die mit dem Internet verbunden ist – also der WLAN-Karte, dem UMTS-Stick oder der Kabelnetzwerkverbindung auf der Registerkarte *Freigabe* –, den Zugriff zulassen.

Gemeinsame Sache: Über die Freigabe konfigurieren Sie die gemeinsame Internetnutzung.



Durch die Freigabe der Internetverbindung erstellt Windows 7 auch einen kleinen DHCP-Server. Das heißt, die Clients, die sich an das virtuelle WLAN anbinden, müssen für DHCP konfiguriert sein.

Wollen Sie verhindern, dass sich Clients mit dem virtuellen Netzwerk verbinden, können Sie es mit dem Befehl

```
netsh wlan stop hostednetwork
```

anhalten. Verbindungen verweigern Sie mit dem Befehl

```
netsh wlan set hostednetwork mode=disallowed
```

Alle diese Befehle lassen sich problemlos auch als Verknüpfung erstellen. Auf diese Weise können Sie mit wenigen Klicks das Hosted Network starten oder anhalten.

Thomas Joos

4.4 Clevere WLAN-Tipps für Windows

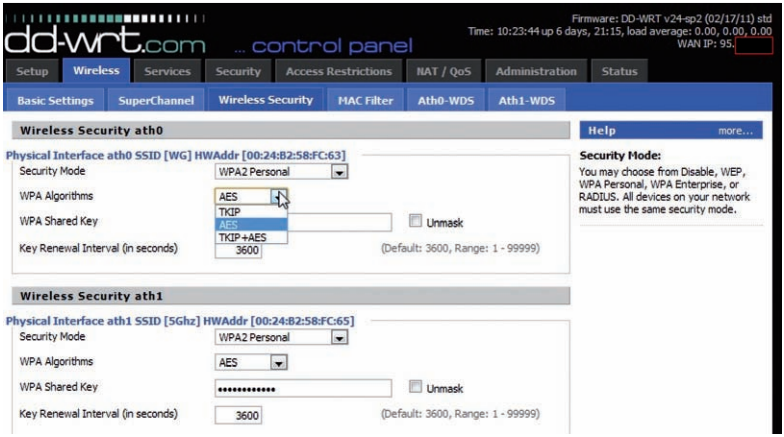
Die Kombination aus Windows-eigenen WLAN-Einstellmöglichkeiten und Softwarefunktionen der Hersteller von WLAN-Adaptern ist manchmal allein schon problematisch genug. Ein Funknetz wird zudem oft von Computern mit unterschiedlichen Betriebsystemversionen genutzt. Dazu kommt WLAN-Hardware, die jeweils unterschiedlich schnelle 802.11-Standards unterstützt. In der Regel gewinnt dann der langsamste gemeinsame Nenner, auch wenn es andere Möglichkeiten gibt. Selbst Windows 7 als moderne Ausgabe des Microsoft-Betriebssystems kriegt das nicht immer perfekt hin.

Wir haben die besten Tipps zur Optimierung und zum stressfreien WLAN-Zugang mit Windows-Computern zusammengestellt. Den Anfang macht natürlich die Performance-Optimierung:

4.4.1 Geschwindigkeitsbremse TKIP lösen

Sie haben Ihre komplette WLAN-Infrastruktur auf 802.11n-Geräte umgestellt, aber irgendwie fehlt es an der Geschwindigkeit?

Sind 802.11n-WLANs zu langsam, liegt dies möglicherweise an der Unterstützung für TKIP als Verschlüsselungsprotokoll. Der Grund dafür ist, dass der Standard für 802.11n den maximalen Durchsatz nicht erlaubt, wenn TKIP zum Einsatz kommt. Stattdessen wird die Leistung auf 54 MBit/s und damit das Niveau von 802.11g gedrosselt. Alle aktuellen WLAN-Geräte sollten WPA2-AES als Verschlüsselungsmodus unterstützen. Es schadet daher nicht, TKIP unter den Tisch fallen zu lassen, wenn alle Geräte den neueren Standard beherrschen.



Bremse lösen: Wird das WLAN per TKIP gesichert, drosselt 802.11n automatisch die Geschwindigkeit.

Sollten noch einige ältere Geräte im Netzwerk vorhanden sein, die nur TKIP unterstützen, ist es oft sinnvoller, ein zweites WLAN ausschließlich für diese Geräte aufzusetzen. Dazu ist teilweise nicht einmal neue Hardware notwendig, viele aktuelle Router können zusätzliche virtuelle WLAN-Zugangspunkte erstellen.

4.4.2 Mehr Geschwindigkeit ohne Netzwerkkompression

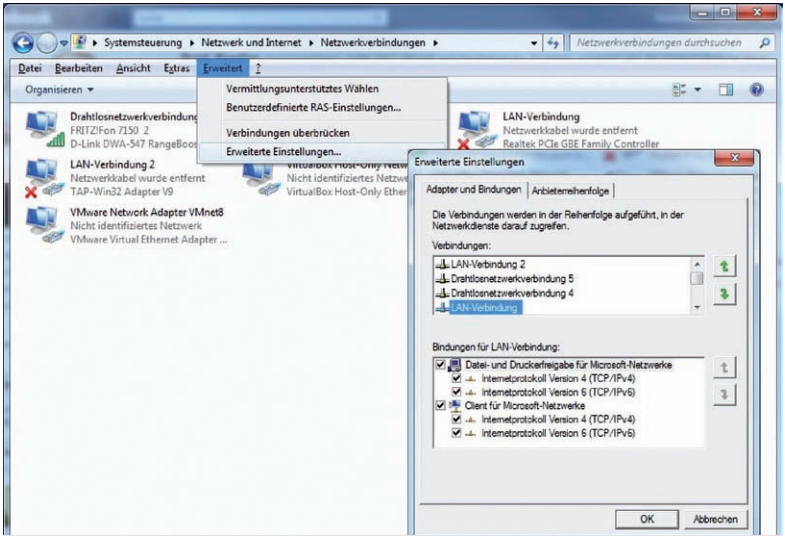
Mit Windows Vista hat Microsoft die Netzwerkkompressionstechnik Remote Differential Compression, kurz RDC, eingeführt. In gemischten Netzwerken kann diese jedoch die Leistung ausbremsen. RDC lässt sich zwar deaktivieren, allerdings ist die Funktion ein wenig versteckt. Unter Windows 7 und Vista muss man in den Menüpunkt *Programm deinstallieren oder ändern* wechseln. Hier findet sich die Option, mit der sich Microsoft-Dienste entfernen lassen, unter Windows 7 heißt sie *Windows-Funktionen aktivieren oder deaktivieren*, der Menüpunkt benötigt administrative Rechte, um gestartet zu werden.

Remote Differential Compression: In Netzwerken mit Windows XP ist RDC eher eine Bremse.

In einem deutschsprachigen Windows nennt sich die Funktion *Remoteunterschiedskomprimierung* und ist standardmäßig aktiviert. Entfernt man den Haken und klickt „OK“, dauert es einige Minuten, bis Windows die Änderungen angewendet hat. Ein Neustart ist nicht notwendig.

4.4.3 (W)LAN-Verbindungen priorisieren

Ist ein PC mit Windows 7 sowohl per WLAN als auch LAN verbunden, kann es sein, dass die in der Regel langsamere WLAN-Verbindung bevorzugt wird. Mit einer Priorisierung lässt sich der bevorzugte Netzwerktyp allerdings einstellen.



Reihenfolge: Über das Menü kann man die Priorität der Netzwerkadapter anpassen.

Dazu öffnen Sie zunächst das *Netzwerk- und Freigabecenter* und wählen dann die Option *Adaptereinstellungen ändern*. Im Folgenden Menü sollte alle installierten Netzwerkadapter samt deren aktuellem Status zu sehen sein.

Ein Druck auf die Alt-Taste erweitert die Ansicht um die Menüleiste. Hier können Sie im Menü *Erweitert* den Punkt *Erweiterte Einstellungen* aufrufen. Im Bereich *Verbindungen* lässt sich nun die Priorität festlegen, in der Windows 7 aktive Netzwerkverbindungen nutzen soll.

4.4.4 Drucker je nach WLAN automatisch wählen

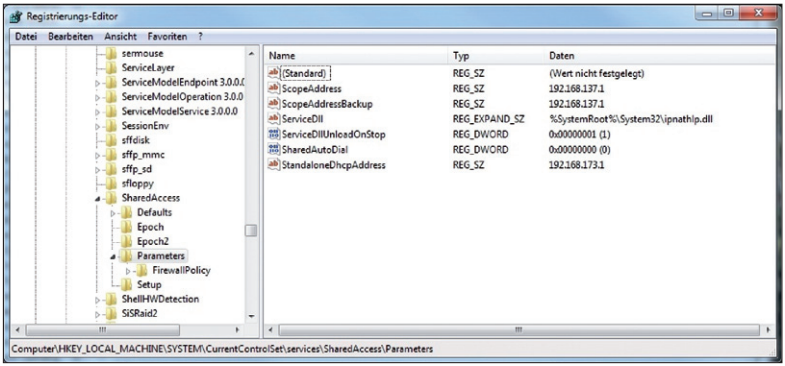
Windows 7 kann den Standarddrucker wechseln, wenn sich der Rechner mit einem anderen Netzwerk verbindet. Das Location Aware Printing Feature soll mobilen Nutzern helfen: Die Funktion kann je nach dem verbundenen Netzwerk einen anderen Drucker automatisch konfigurieren – etwa wenn man vom Arbeitsnetzwerk in das LAN zu Hause wechselt. Diese Lösung funktioniert mit Windows 7, setzt allerdings die Versionen Professional, Enterprise oder Ultimate voraus.

Die Funktion wird in *Geräte und Drucker* konfiguriert. Dort müssen Sie einen der Drucker markieren. In der Menüleiste von *Geräte und Drucker* über den Geräten ist nun die Option *Standarddrucker verwalten* sichtbar. Wählen Sie diese, erscheint ein Dialog, in dem sich das Netzwerk auswählen und ein entsprechender Drucker zuordnen lassen. Sollte der Menüpunkt *Standarddrucker verwalten* nicht erscheinen, hat ihn Ihr Netzwerk-Admin möglicherweise per Richtlinie abgeschaltet.

4.4.5 IP-Adresse des virtuellen Windows-Wi-Fi-Hotspots ändern

Unter Windows 7 und Windows Server 2008 R2 lässt sich das Betriebssystem leicht in einen virtuellen Hotspot verwandeln. Wer allerdings eine andere IP-Adresse nutzen möchte, muss dies über die Registry konfigurieren.

Wenn Sie Windows 7 in einen Wi-Fi-Hotspot verwandelt haben, wird Ihr PC dabei automatisch zu einem DHCP-Server, der IP-Adressen aus dem Bereich 192.168.137.xxx verteilt. Der Rechner selbst erhält die IP 192.168.137.1.



Adresszuordnung: Per Registry lässt sich die vergebene IP des virtuellen Wi-Fi-Hotspots ändern.

Die IP-Range lässt sich in der Registry von Windows ändern. Die passenden Einträge sind „ScopeAdress“, „ScopeAdressBackup“ und „StandaloneDhcpAdress“, der passende Pfad ist

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Shared
Access\Parameters
```

4.4.6 MAC-Adresse von WLAN-Adaptern ändern

Einige Programme oder Netzwerkkonfigurationen setzen eine bestimmte MAC-Adresse im Adapter voraus. Oft kann man die Adresse im BIOS von PC und Notebook ändern, aber das ist umständlich. Unter Windows geht es einfacher und schneller. Wer die MAC-Adresse eines in Windows installierten WLAN-Adapters ändern will, kann dies direkt über die Netzwerkeinstellungen tun – wenn man das passende Menü findet. Ein Rechtsklick auf den jeweiligen Adapter zeigt das Kontextmenü; hier kann man die Eigenschaften auswählen.

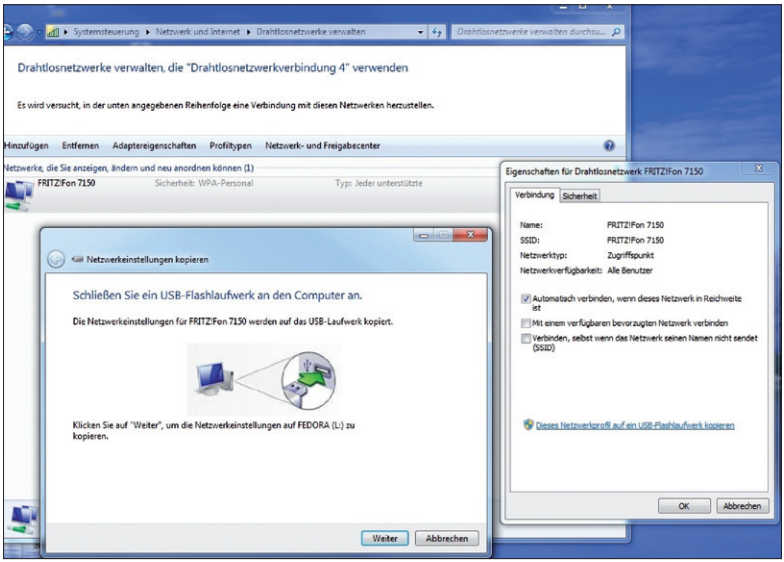
Ein Klick auf *Konfigurieren* zeigt das entsprechende Menü, über den Reiter *Erwei-*

tert gelangt man anschließend in die passende Rubrik. Um die Adresse zu ändern, wird diese als zwölfstellige Zahl unter „MacAddress“ eingetragen. Unter Windows XP heißt der entsprechende Eintrag „NetworkAddress“. Die Adresse setzt sich aus den Nummern 0 bis 9 sowie den Buchstaben A bis F zusammen.

Vor der Änderung sollte man allerdings die eigentliche Adresse des Adapters aufschreiben. Das klappt unter jeder Version am einfachsten, indem man auf der Kommandozeile den Befehl *ipconfig /all* eingibt. Die MAC findet sich als Wert hinter „Physikalische Adresse“.

4.4.7 WLAN-Einstellungen auf USB-Stick kopieren

In Windows 7 lassen sich die WLAN-Konfigurationseinstellungen einfach an andere Systeme weitergeben. Dazu steht ein Assistent zur Verfügung, der die Zugangsdaten samt Einstellung auf ein USB-Medium überträgt.



WLAN: Mithilfe des Assistenten lassen sich auch komplizierte Wi-Fi-Einstellungen übertragen.

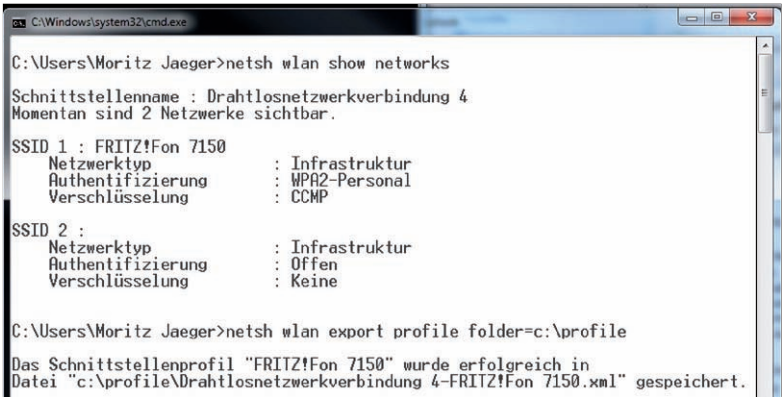
Der Assistent für die Weitergabe der Zugangsdaten findet sich in der Verwaltung der drahtlosen Netzwerke unter *Systemsteuerung\Netzwerk und Internet\Drahtlosnetzwerke verwalten*.

Ein Rechtsklick auf das jeweils gespeicherte WLAN zeigt die Eigenschaften; dort können Nutzer mit administrativen Rechten die Option *Dieses Netzwerkprofil auf ein USB-Flashlaufwerk kopieren*. Ein Klick auf den Link startet den Assistenten.

Natürlich können die Informationen auch auf anderen Systemen wieder eingespielt werden. Der Assistent richtet einen Autostart-Eintrag ein. Sobald ein USB-Stick am System angemeldet wird, zeigt der Autostart einen Drahtlosnetzwerkinstallations-Assistenten an, der die Informationen in das jeweilige System überträgt.

4.4.8 WLAN per Kommandozeile verwalten

In Windows 7 ist eine umfangreiche Kommandozeile integriert. Über diese kann man sich via netsh auch mit einem WLAN verbinden – oder den kompletten Vorgang von einem Script steuern lassen.



Kommandozeile: Per netsh kann man sich auch ohne Assistent mit einem WLAN verbinden.

Zunächst muss man in eine Kommandozeile wechseln; dies ist die Voraussetzung für *netsh*. Das Tool stellt zahlreiche Funktionen rund um Wi-Fi zur Verfügung, die sich so auch in entsprechende Skripte integrieren lassen. Der Befehl *netsh wlan show networks* zeigt beispielsweise alle verfügbaren Netzwerke an, egal ob diese eine SSID übertragen oder nicht.

Um sich nun per Kommandozeile oder Script mit einem Netzwerk zu verbinden, muss ein passendes Profil als XML-Datei angelegt sein. Der Befehl *netsh wlan export profile* erstellt eine passende Vorlagendatei. Dazu sollte man noch den Schalter *folder=Laufwerk\Ordnername* nutzen, um die Information schnell zu finden. Unter Umständen muss der Ordner zunächst angelegt werden.

Diese XML-Datei kann man nun bearbeiten und mit den notwendigen Zugangsinformationen versehen. Wer es sich einfach machen will, exportiert die Datei von einem Rechner, der bereits mit dem WLAN verbunden ist. Auf einem neuen PC kann man die Konfiguration anschließend über den Befehl *netsh wlan add profile filename="Laufwerk\Ordner\Dateiname.xml"* einlesen. Der Befehl *netsh wlan con-*

nect SSID sollte anschließend die Verbindung herstellen. Wie bereits erwähnt, lässt sich dieser Vorgang auch über die Windows-Power-Shell skriptgesteuert durchführen. Weitere Informationen zur Power Shell finden Sie im Artikel „Shell Scripting unter Windows" (**Webcode** 1761680).

4.4.9 DD-WRT – WLAN-Leistung erhöhen

Mit der alternativen Firmware DD-WRT lassen sich selbst günstige Router mit komplexen Netzwerkfunktionen ausstatten. Allerdings kann es zu Problemen kommen, wenn die Geräte einen Atheros-Chipsatz für das WLAN-Modul verwenden, wie etwa den Netgear WNDR3700. Nach dem Upgrade auf DD-WRT kann es sein, dass die Sendeleistung massiv einbricht.

Vorsichtig anpassen: Man kann sich an die erlaubten Grenzwerte herantasten, um eine bessere WLAN-Leistung zu erhalten.

Unter Umständen kann man in den Einstellungen der Firmware korrigieren. Im Menü *WLAN – Basis-Einstellungen* (abhängig von der Firmware-Version) können Sie die Sendeleistung sowie den Gewinn der Antenne (Antenna Gain) anpassen. Allerdings müssen Sie dabei vorsichtig vorgehen: In Deutschland gelten strikte Obergrenzen für die Sendeleistung.

2,4-GHz-WLANs (etwa 802.11b und g) dürfen maximal 100 Milliwatt oder 20 dBm (Dezibel Milliwatt) abstrahlen, bei WLANs auf 5-GHz-Basis (802.11a und n) sind es bis zu 200 Milliwatt – Vorsicht, das entspricht 23 dBm. Der Wikipedia-Eintrag zu *WLAN* gibt mehr Hintergrundinformationen dazu, auch, wie sich die komplette maximale Leistung berechnet.

4.4.10 Thinkpad – Probleme bei Access Connections und WLAN-Dienst

Die Software Access Connections ist fester Bestandteil nahezu jedes Lenovo-Notebooks. Sie verwaltet die Netzwerkverbindungen und stellt automatisch eine Verbindung zu bekannten Netzwerken her. Allerdings macht sie immer wieder Zicken –, bei der Reparatur muss man teilweise zu drastischen Maßnahmen greifen.

Nach Updates kann es beispielsweise vorkommen, dass sich die Thinkpad-Software und der in Windows integrierte Dienst zur Verwaltung von WLAN-Zugängen ins Gehege kommen. Oftmals kann man dann über Access Connections keine neue Verbindungen mehr anlegen oder auf bestehende Informationen zugreifen. Damit lassen sich auch die eigentlichen Stärken der Software – etwa das automatische Ausführen von Programmen, wenn man mit einem bestimmten Hotspot verbunden ist, oder das Aktivieren bestimmter Proxy-Einstellungen –, meist nicht mehr nutzen.

Nützlich, aber problematisch: Access Connections bietet einige Zusatzfunktionen – es kann allerdings auch Probleme bereiten.

Die Probleme sind oftmals nur durch eine Neuinstallation des Programms zu lösen. Die jeweils aktuellste Version von Access Connections bietet Lenovo auf dieser Website an. Allerdings sollten Sie zunächst die gespeicherten Profile exportieren. In Access Connections findet sich die passende Option unter dem Reiter *Standortprofile*. Um auf Nummer sicher zu gehen, sollte man zudem alle gespeicherten WLAN-Profile in Windows löschen. Die Netzwerke sind unter Windows 7 im *Netzwerk und Internet – Drahtlosnetzwerke verwalten* abgelegt. Nach der Deinstallation von Access Connections muss der Rechner neu gestartet werden, anschließend kann die Software wieder eingespielt werden. Sicherheitshalber sollte man danach den Rechner noch einmal neu starten.

Michael Eckert, Moritz Jäger

5 Tools

Mal eben das Netzwerk auf Sicherheit prüfen, einen MySQL-Server remote administrieren oder den laufenden Netzverkehr checken? Mit den richtigen Softwarewerkzeugen können sich Administratoren die Arbeit erleichtern. Die folgenden Beiträge stellt eine Auswahl an hilfreicher Netzwerk-Software detailliert vor.

5.1 Empfehlenswerte Netzwerk-Tools für alle Fälle

Was ist eigentlich ein Netzwerk-Tool? Ein meist nur kleines Stück Software, das einem aber erheblich die Arbeit als Administrator erleichtern kann. Und daraus ergibt sich eine Fülle an Möglichkeiten. Dies verdeutlicht auch die entsprechende Rubrik in unserer Produktdatenbank, in der sich zahlreiche Netzwerk-Tools unterschiedlichster Ausprägung tummeln.

Das Thema Netzwerk umfasst eine Vielzahl von Anwendungsbereichen, ein großer Teil davon entfällt auf den Bereich Sicherheit. Solche Security-Tools erleichtern Administratoren die Arbeit beim Aufspüren eventueller Sicherheitslücken im Firmennetz. Wir haben an dieser Stelle eine Auswahl an Netzwerk-Tools zusammengestellt, die Ihnen bei vielen Herausforderungen die Arbeit erleichtern können. Wer es primär mit Microsoft-Umgebungen zu tun hat, wird natürlich auch in den Systinternals fündig. In dem Beitrag Sysinternals – Gratis-Tools fürs Netzwerk finden Sie eine Reihe der Netzwerk-Tools ausführlich erläutert.

5.1.1 Admins Liebling: PuTTY

Wer mit einem Windows-Rechner Linux- und Unix-Server administrieren muss oder darf, der kann auf PuTTY schlecht verzichten. Bei diesem Tool handelt es sich um einen freien Telnet- und SSH-Client. Telnet dürfte in diesen Tagen weniger als Protokoll eingesetzt werden. Die Wahl der meisten Administratoren heutzutage ist SSH. PuTTY bringt eine xterm-Emulation mit sich, und damit können Sie sich auf die Konsole von Unix- oder Linux-Rechnern verbinden. PuTTY gibt es auch für Linux oder Unix und befindet sich zum Beispiel im Softwarelager von Ubuntu oder Linux Mint.

Unter Windows ist der Nutzen dieser Applikation allerdings größer, da Sie unter Linux in der Regel ohnehin eine Konsole zur Verfügung haben. Allerdings können Sie mit PuTTY häufig verwendete Verbindungen speichern und sparen sich unter Umständen Eingabeorgien. Somit hat das Programm auch unter Linux durchaus seine Existenzberechtigung.

5.1.2 Mac OS X mit MacFUSE erweitern

Wie der Name schon vermuten lässt, ist MacFUSE für Apples Betriebssystem Mac OS X. Die Software erlaubt es, die nativen Dateisystemkapazitäten von Mac OS X zu erweitern. Ist das Grundpaket installiert, lässt sich jedes Dateisystem von Drittanbietern verwenden, das auf MacFUSE aufsetzen kann. Entwickler können dafür MacFUSE SDK benutzen.

Die Dateisysteme können lokal sein oder aus dem Speicher kommen, und auch das Einbinden von Netzwerkdateisystemen ist denkbar. Technischer ausgedrückt bedeutet dies, dass Sie mittels MacFUSE ein voll funktionierendes Dateisystem in den User-Space von Mac OS X einbinden können. Voraussetzung ist Mac OS X 10.4 „Tiger“ oder höher. Die FUSE-API (File-system in USEr space) kommt eigentlich von Linux. Aus diesem Grund gibt es viele existierende FUSE-Dateisysteme, die sich unter Mac OS X einsetzen lassen.

Das Quell-Repository von MacFUSE beinhaltet bereits diversen Quellcode für nützliche Dateisysteme. Dazu gehören sshfs, procfs, AccessibilityFS, GrabFS, LoopbackFS, SpotlightFS und YouTubeFS.

5.1.3 OpenVPN für Macs: Tunnelblick

Für Linux und Windows gibt es doch recht komfortable OpenVPN-Clients. Unter Mac OS X heißt die wohl beste Lösung Tunnelblick – eine grafische Oberfläche für OpenVPN, die das Einwählen in ein Virtual Private Network erleichtert. Die derzeit aktuelle Version 3.1 funktioniert mit Mac OS X 10.4 „Tiger“ oder höher. Wer 10.3 „Panther“ am Laufen hat, kann auf die alte Version Tunnelblick 2.0.1 zurückgreifen. Die Einwahldaten für VPN finden Sie unter ~/Library/Application Support/Tunnelblick/Configurations. Die Software nimmt sowohl conf- als auch ovpn-Dateien. Sollten Sie mehrere Einwahlpunkte konfigurieren wollen, erstellen Sie einfach entsprechende Unterordner.

Sobald die Software installiert ist, finden Sie ein kleines Symbol in der oberen Leiste des Betriebssystems. Sind die Einwahlpunkte hinterlegt, klicken Sie einfach auf das kleine Tunnel-Symbol und aktivieren die VPN-Verbindung.

5.1.4 iStumbler und NetStumbler

iStumbler ist ein Netzwerk-Erkennungs-Tool für Mac OS X. Es unterstützt AirPort-Netzwerke, Bluetooth-Geräte, Bonjour-Dienste und Ortsinformationen. Das Tool unterstützt Apples Betriebssystem von 10.2 „Jagwire“ bis zum aktuellen 10.6 „Snow Leopard“. iStumbler zeigt Ihnen bei WLANs zum Beispiel an, welche Verschlüsselung das Netzwerk verwendet oder welcher 801.11-Modus eingesetzt wird. Zudem kann die Software den Hersteller des Routers oder Access-Points erkennen.

Für Windows gibt es eine ähnliche Software, die sich NetStumbler nennt. Auch damit können Sie WLANs ausfindig machen und viele Informationen über die drahtlosen Netzwerke herauslesen.

5.1.5 Mit Ntop das Netzwerk überwachen

Ntop ist ein Monitoring-Tool für Netzwerkaktivitäten. Die Entwickler selbst vergleichen es ein wenig mit dem bekannten Unix-Befehl top. Die Applikation basiert auf libcap und wurde so entwickelt, dass sie sich auf jeder Unix-ähnlichen Plattform und auch unter Win32 betreiben lässt.

Das Netzwerkwerkzeug kann Netzwerkverkehr anhand vieler Protokolle sortieren. Darüber hinaus ist es in der Lage zu sehen, wer mit wem kommuniziert. Ntop kann unter anderem mit Ethernet-Geräten, Loopback, Token Ring, PPP, PPPoE, Raw IP und FDDI umgehen. An Netzwerkprotokollen unterstützt es mitunter IPv4, IPv6, IPX, DecNet, AppleTalk, Netbios, OSI und DLC.

Richtig eingesetzt kann es Flaschenhälse im Netzwerk aufzeigen oder einfach nur Missbrauch im Firmennetzwerk aufdecken.

5.1.6 Turnschuh-Administration ade: Webmin

Mit Webmin können Sie Ihren kompletten Linux-Server bequem über den Browser administrieren. Das Tool ist ein richtiger Tausendsassa. Es kann mit vielen Serverdiensten, zum Beispiel Apache, DNS, DHCP, Samba, Postfix und MySQL, umgehen. Ebenso können Sie mit Webmin die komplette Benutzer- und Gruppenverwaltung durchführen. Auch Hardwarekonfiguration, Bandbreiten-Monitoring und vieles mehr haben Sie mit diesem Tool im Griff.

Nach der Installation ist das Tool über den Browser standardmäßig unter https://<IP-Adresse oder Name des Servers>:10000 zu erreichen. Webmin ist mit Sicherheit das Schweizer Taschenmesser für die netzwerkbasierte Administration von Linux-Servern.

Allerdings ist es nicht auf Linux beschränkt. Die Software unterstützt unter anderem auch offiziell Mac OS X, P/UX, IBM AIX, DragonFly BSD, FreeBSD, NetBSD, Solaris, SGI Irix und OpenBSD. Ob Ihr System zu den unterstützten Betriebssystemen gehört, erfahren Sie in dieser Liste.

5.1.7 Datenübertragung mit FileZilla

FileZilla dürfte eines der beliebtesten Tools sein, wenn es um das Thema Datentransfer geht. Das Tool unterstützt die Protokolle FTP, FTP via SSL/TLS (FTPS) sowie SSH File Transfer Protocol (SFTP) und kostet nichts. Damit ist der Anwender gut für Datentransfers im Internet gerüstet. Darüber hinaus kann FileZilla mit

IPv6 umgehen und unterstützt HTTP/1.1-, SOCKS5- und FTP-Proxies. Sehr schön ist auch, dass FileZilla in über 40 Sprachen erhältlich ist. Das Programm unterstützt zudem ein Fortsetzen, wenn Dateien größer als 4 GByte transferiert werden. Die Warteschlange können Sie entweder mit Drag & Drop befüllen oder mittels des eingebauten Dateimanagers. Um das Netzwerk nicht komplett zu blockieren, können Sie Geschwindigkeits-Limits setzen. Ebenso haben Sie die Möglichkeit, bei der Remote-Verbindung nach Dateien zu suchen.

Das Programm unterstützt Tabs, wie man es von modernen Internet-Browsern gewohnt ist. Somit können Sie gleichzeitig Verbindungen zu mehreren Servern offen haben. In den Unterpunkten Bookmark und Server lassen sich etliche Verbindungen hinterlegen und Verbindungen schnell mittels weniger Mausklicks öffnen. FileZilla sollte auf keinem Rechner fehlen, auf dem viel mit Datentransfer im Internet gearbeitet wird. Die Software ist für Windows, Mac OS X und Linux gleichermaßen erhältlich.

5.1.8 Netzwerksicherheit-Nonplusultra: BackTrack

BackTrack ist eigentlich kein Netzwerk-Tool an sich, sondern eine Linux-Distribution, die aber wahrscheinlich die kompletteste Netzwerk-Tools-Sammlung an freien Werkzeugen beinhaltet (siehe auch Linux-Distributionen für den Sicherheits-Check). Hier findet der Administrator wirklich fast alles, was er braucht, um die Sicherheit im Firmennetz zu überprüfen.

Die Tools dieser Linux-Distribution sind mit Vorsicht zu genießen, denn schnell könnten Sie mit einem Bein im Gefängnis stehen, wenn Sie die Hacker-Tools falsch einsetzen. Sie finden in BackTrack alle möglichen Exploit-Werkzeuge und auch das bekannte Metasploit-Framework.

Sollten Sie das Firmennetzwerk auf Sicherheit überprüfen wollen, schadet es auf keinen Fall, sich vorher eine Genehmigung vom Chef zu holen. Mit BackTrack lässt sich sehr viel Unsinn anstellen, wenn man nicht vorsichtig damit umgeht.

5.1.9 Die freie Ghost-Konkurrenz: Clonezilla

Eigentlich jedem Systemadministrator dürften die Klon-Software-Pakete Norton Ghost oder Symantec Ghost Corporate Edition bekannt sein. Vorteil von Letzterer ist, dass sie Multicasting beherrscht und somit Masseninstallationen deutlich schneller ablaufen. Die freie Lösung Clonezilla beherrscht sowohl Unicasting als auch Multicasting. Clonezilla basiert auf DRBL, Partclone und udpcast. Somit können Sie komplette Partitionen oder Festplatten sichern und wieder herstellen. Es gibt zwei verschiedene Versionen: Clonezilla Live eignet sich für das Sichern einzelner Maschinen und deren Wiederherstellung. Mit Clonzilla SE (Server Edition) steht eine perfekte Software für Masseninstallationen zur Verfügung. Laut Aussage der Entwickler können Sie mehr als 40 Computer gleichzeitig klonen.

Erkennt Clonezilla das Dateisystem, bearbeitet die Software lediglich die benutzten Blöcke. Das steigert die Effizienz beim Sichern oder Wiederherstellen enorm. In einem Test haben die Entwickler 41 Computer mittels Multicasting mit einem 5,6 GByte großen Systemabbild befeuert – der Vorgang war nach ungefähr zehn Minuten abgeschlossen. Clonezilla unterstützt folgende Dateisysteme: ext2, ext3, ext4, reiserfs, reiser4, xfs, jfs, FAT, NTFS, HFS+, UFS und VMFS. Das zu sichernde Abbild können Sie auf einem lokalen Massenspeicher, SSH-, Samba- oder NFS-Server ablegen. Mit drbl-winroll, das aus der Feder der gleichen Entwickler stammt, können Sie Host-Namen, Gruppe und SID von geklonten Windows-Rechnern automatisch ändern.

5.1.10 GNOMEs Network Tools

Wer einen Linux-Rechner mit GNOME betreibt, hat wahrscheinlich auch die Network Tools installiert. Bei Ubuntu oder Linux Mint sind diese per Standard enthalten. Damit können Sie nicht nur Informationen über die im System befindlichen Netzwerkgeräte erfahren. Die Network Tools stellen auch grafische Oberflächen für Ping, Netstat, Traceroute, Port Scan, Lookup, Finger und Whois bereit. Ebenso lassen sich MTU, Geschwindigkeit und Transfervolumen empfangener und gesendeter Daten auslesen – manchmal möchte man etwa wissen, ob ein bestimmter Rechner noch eine aktive Netzwerkverbindung hat. Statt auf der Konsole mit ping zu hantieren, bereitet die grafische Lösung in den Netzwerk-Tools das Ergebnis schön auf und lässt sich zudem recht komfortabel bedienen.

5.1.11 Ein ganzes Netzwerk mit fping untersuchen

Mit ping kann man nur einen Rechnern anpingen, außer man wendet ein entsprechendes Skript an. Will man in einem Netzwerk herausfinden, welche Rechner am Leben sind, geht das mit fping wesentlich einfacher. Wie ping nutzt es eine ICMP-Anfrage (Internet Control Message Protocol) und wartet auf eine Antwort des befragten Rechners. Darüber hinaus ist fping in Skripts angenehmer zu benutzen, weil die Ausgabe sehr einfach zu parsen ist. Sie können dem Kommandozeilen-Tool einen ganzen Bereich zuweisen, der angepingt werden soll. Ebenso könnten Sie die zu pingenden Rechner in einer Textdatei hinterlegen. Statt die Anfrage an nur einen Rechner zu schicken, schickt fping ein Paket an einen Rechner und hüpft dann sofort zum nächsten. Gibt es eine Antwort, vermerkt die Software dies und nimmt den Computer aus der noch zu pingenden Liste. Sollte ein Host binnen einer bestimmten Zeit nicht antworten, wird dieser als nicht erreichbar vermerkt.

Sie finden weitere Informationen zu fping in der Man-page (man fping). Die Dokumentation ist auch online hinterlegt. Fping ist ursprünglich für UNIX-ähnliche System entwickelt worden, es gibt aber auch eine Portierung für Windows.

Jürgen Donauer

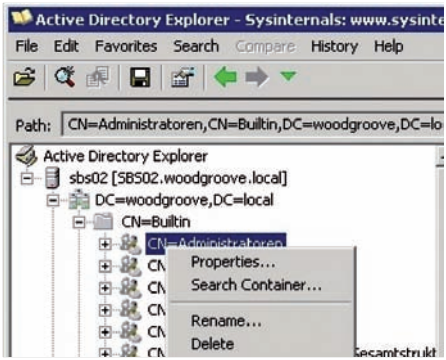
5.2 Sysinternals – Gratis-Tools fürs Netzwerk

Mit den Sysinternals-Tools richtet sich Microsoft vornehmlich an IT-Professionals im Allgemeinen und Administratoren im Besonderen. Die Werkzeuge sollen Admins die Verwaltung, Problembehebung und Diagnose von Windows-Systemen und -Anwendungen erleichtern. Microsoft gliedert die kostenlosen Sysinternals-Dienstprogramme in verschiedene Kategorien. Wir beschäftigen uns mit Tools für die Netzwerkadministratoren, die den Nutzer bei Aufgaben wie der Verbindungs- und Freigabeüberwachung unterstützen können.

5.2.1 AdExplorer (Active Directory-Explorer) – im Active Directory navigieren

Der Active Directory-Explorer bietet eine Verwaltungsoberfläche für die Active-Directory-Datenbank, ähnlich zu ADSI-Edit. Beim Verbindungsaufbau legen Sie den Domänencontroller fest sowie die Benutzer, mit denen Sie sich verbinden wollen. Sie können die Daten auch speichern, sodass Sie nicht jedes Mal eine Authentifizierung durchführen müssen, um sich mit dem AD zu verbinden.

Das Tool hat eine Explorer-ähnliche Oberfläche und erlaubt die Navigation im Active Directory. Sie können zur Analyse auch Schnappschüsse des produktiven AD erstellen. Die Schnappschüsse lassen sich nachträglich bearbeiten. Über das Menü *File/Create* Snapshot erstellen Sie einen solchen Schnappschuss. Im Fenster können Sie einstellen, bis zu welcher CPU-Last der Schnappschuss den Server belasten soll. Haben Sie einen Schnappschuss erstellt, können Sie diesen parallel zur Verbindung mit dem aktuellen Active Directory oder einem anderen Schnappschuss über das Menü *File* laden. Anschließend steht der Menüpunkt *Compare* zur Verfügung, mit dem Sie einen Vergleich zwischen den Schnappschüssen oder dem produktiven AD durchführen können.



Sysinternals ADExplorer: Bearbeiten von Active Directory im AD-Explorer.

Zwar kann Windows Server 2008 R2 solche Snapshots auch über das Befehlszeilen-Tool *ntdsutil.exe* erstellen, aber nicht so einfach und leicht bedienbar wie AD-Explorer. Sie können das Tool auf jedem Computer starten, der Mitglied einer Domäne ist, und müssen nicht den Domänencontroller verwenden. Sie haben die Möglichkeit, mehrere Schnappschüsse zu unterschiedlichen Zeitpunkten erstellen. Diese können Sie nachträglich vergleichen, um so Änderungen nachzuverfolgen. Der Active-Directory-Explorer erlaubt das Anpassen von Einstellungen im Active Directory, direkt auf Ebene der Datenbank. Sie können Attribute ändern, Einstellungen anpassen und Objekte löschen oder erstellen.

Die Navigation erfolgt ähnlich wie beim Windows Explorer. Sie haben über den Menüpunkt *Favorites* auch die Möglichkeit, verschiedene Bereiche im AD direkt wieder anwählen zu können, wenn Sie diese häufiger benötigen, zum Beispiel bestimmte Organisationseinheiten. Über *Search* können Sie sehr detaillierte Suchabfragen im Active Directory durchzuführen. Komplexe Suchabfragen lassen sich im Suchfenster abspeichern und auf diesem Weg jederzeit wieder aufrufen. Im Suchfenster können Sie nach Attributen und nach Kombinationen von Attributen suchen. Zusätzlich lassen sich die Sicherheitseinstellungen und Berechtigungen anpassen, dies geschicht über *Properties* im Kontextmenü von Objekten.

Die Bedienung des Tools ist auch für ungeübte Administratoren intuitiv möglich. Sie müssen das Tool nicht installieren, sondern können die *.exe-Datei direkt starten und auf diesem Weg das Werkzeug via USB-Stick verwenden.

5.2.2 AdInsight (Insight for Active Directory) – Verbindungsanalyse

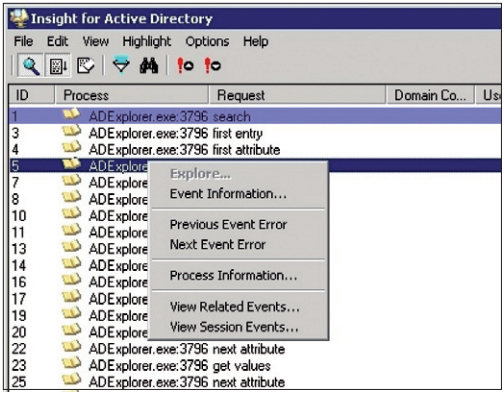
Mit AdInsight analysieren Sie die LDAP-Verbindungen eines Servers in Echtzeit. Das Tool verwendet dazu die Datei *wldap32.dll*, die den Zugriff auf das Active Directory steuert. Es zeigt, ähnlich dem Netzwerkmonitor für den Netzwerkverkehr, alle Anfragen von Clients an den Domänencontroller an, auch Daten, die der Domänencontroller blockiert. AdInsight hilft also, Authentifizierungsprobleme von Anwendungen und Computern zum Active Directory zu finden und zu beheben.

Sie können die Daten, die das Tool ausliest, auch als Textdatei speichern und so nachträglich analysieren. Wenn Sie mit der rechten Maustaste auf einen Eintrag klicken, erhalten Sie weitere Informationen über die einzelnen Einträge. AdExplorer zeigt Verbindungsdaten an, sobald ein Programm oder ein Server Daten aus dem Active Directory abrufen will. Nach dem Start sehen Sie daher nicht gleich einen Eintrag, sondern erst wenn ein Programm über das Netzwerk auf das Active Directory über die Datei *wldap32.dll* zugreifen will.

Über den Menüpunkt *File* können Sie den aktuellen Scanvorgang abspeichern und nachträglich über AdInsight öffnen. Über *File\Export to Text File* exportieren Sie die Ausgabe als Textdatei. Da sich beim Verbindungsaufbau mit dem AD viele Daten ansammeln, haben Sie die Möglichkeit, über *Edit\Find* die Anzeige zu filtern.

Weitere Filteroptionen stehen über den Menüpunkt *View* zur Verfügung. Die verschiedenen Anzeigen lassen sich farblich hervorheben, um einen besseren Überblick zu erhalten. Diese Informationen finden Sie über den Menüpunkt *Highlight*. In den verschiedenen Spalten zeigt ADInsight genauere Daten an. Die Spalte User enthält, falls verfügbar, den Benutzernamen, mit dem die Anwendung versucht, auf das AD zuzugreifen. Sie müssen für die Messung das Tool nicht installieren, aber direkt auf dem Server starten. Das Tool ist vor allem sehr hilfreich, wenn ein AD-abhängiger Dienst wie Exchange nicht funktioniert. Durch die umfangreichen Filtermöglichkeiten erkennen Sie schnell, worin der Fehler besteht.

Übersicht: Sie können sich die aktuellen Verbindungen zum Active Directory anzeigen lassen.

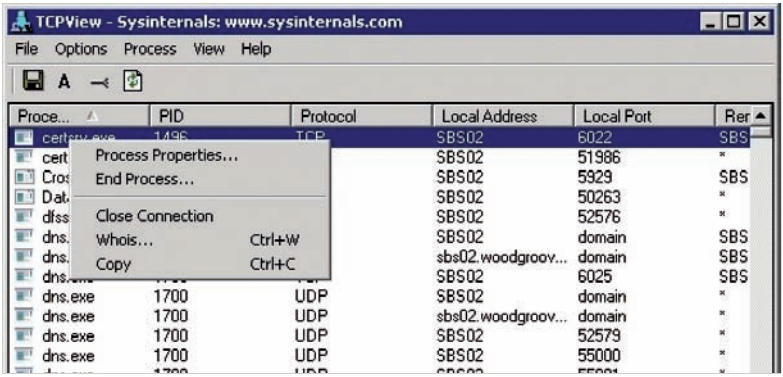


5.2.3 Geöffnete Ports überwachen mit TCPView

Zur Analyse der Netzwerkverbindungen auf einem Server ist es unerlässlich, sich die geöffneten Ports anzuzeigen. Mit TCPView können Sie sich in einer grafischen Oberfläche alle TCP- und UDP-Endpunkte eines Computers anzeigen lassen. Zusätzlich sehen Sie, welche Prozesse auf die Endpunkte und Ports zugreifen.

Sie sehen also nicht nur geöffnete Ports wie bei anderen Programmen, sondern detaillierte Informationen über den Prozess, dessen ID, das Protokoll, die Remote-Adresse und den Port. Das Tool enthält noch das Programm *tcpvcon.exe*, das die gleichen Informationen wie TCPView in der Befehlszeile anzeigt, etwa zur Verwendung in Skripts. Lässt sich der Name des zugreifenden Computers aufrufen, zeigt TCPView auch diesen an. Neben der reinen Anzeige können Sie im Tool auch direkt Verbindungen trennen. Klicken Sie diese dazu mit der rechten Maustaste an.

Weitere Möglichkeiten des Kontextmenüs sind ausführlichere Informationen sowie das Beenden des Prozesses, der die Verbindung aufbaut. Sie können Informationen in die Zwischenablage kopieren und Spezialisten zusenden, welche die Verbindung analysieren können. Das Tool baut auf Daten auf, die das Windows-Tool Netstat liefert, bietet aber mehr Angaben und ist leichter zu bedienen.



TCPView: Das Tool zeigt die geöffneten Ports sowie die beteiligten Computer und Prozesse.

TCPView aktualisiert die Verbindungen jede Sekunde; Sie können über *Options\ Refresh Rate* die Abtastrate ändern. Verbindungen, die den Status innerhalb der Abtastrate ändern, sind gelb markiert. Gelöschte Endpunkte zeigt das Tool rot an, neue Endpunkte in Grün. Den aktuellen Verbindungsstatus können Sie über das Menü abspeichern. Wollen Sie die Ausgabe über ein Skript steuern, verwenden Sie am besten das Befehlszeilen-Tool *tcpvcon.exe*. Die Ausgabe ähnelt netstat, enthält aber mehr Informationen. Die Syntax des Tools lautet:

```
tcpvcon [-a] [-c] [-n] [Prozessname oder PID]
```

- -a – Zeigt die Endpunkte an
- -c – Ausgabe als CSV
- -n – Keine Namensauflösung

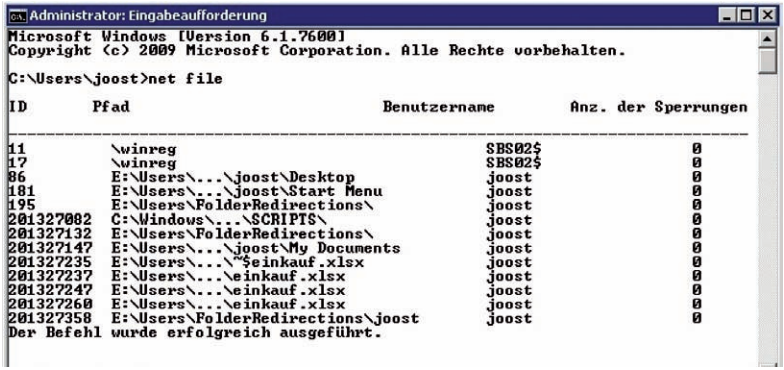
5.2.4 PSFile – über das Netzwerk geöffnete Dateien anzeigen

Öffnen Anwender eine Datei auf einem Computer über das Netzwerk, lässt sich das ebenfalls anzeigen. Dazu verwenden Sie das Tool psfile.exe.

Sie können zwar ebenso mit dem Befehl *net file* eine Liste der über das Netzwerk geöffneten Dateien anzeigen. Allerdings schneidet dieser Befehl lange Pfadnamen ab. Außerdem kann *net file* keine Daten auf Remote-Computern abfragen, sondern nur für das lokale System.

Geben Sie nur psfile an, zeigt das Tool geöffnete Dateien an, inklusive des genauen Dateipfads. Wollen Sie die geöffneten Dateien auf einem Computer im Netzwerk abfragen, können Sie dazu ebenfalls psfile verwenden. Die Syntax dazu ist:

```
psfile [\\<Computer> [-u <Benutzername> [-p <Kennwort>]]]
[[Id | <Pfad>] [-c]]
```



Einfach: net file zeigt die geöffneten Dateien im Netzwerk.

- -u – Mit dieser Option können Sie den Benutzernamen zum Anmelden am Remote-Computer angeben.
- -p – Mit dieser Option geben Sie das Kennwort für den Benutzernamen an. Wenn Sie kein Kennwort angeben, müssen Sie dieses bei der Ausführung des Befehls angeben.
- -Id – Hier können Sie die ID der Datei angeben, von der Sie ausführlichere Informationen anzeigen lassen wollen oder die geschlossen werden soll.
- Pfad – Pfad der Dateien, die angezeigt werden sollen.
- -c – Schließt die Dateien, deren ID Sie angegeben haben.

5.2.5 Über das Netzwerk mit Shutdown.exe und PsShutdown.exe herunterfahren

Sie haben die Möglichkeit, über die Befehlszeile den Computer herunterfahren oder neu zu starten. Sie benötigen dazu nur genügend Rechte. Dazu können Sie das Befehlszeilen-Tool *shutdown.exe* von Windows benutzen. Dies zählt natürlich nicht zu den Windows-Sysinternals, sei aber aufgrund der Funktion und des Bezugs zum darauffolgenden Tool an dieser Stelle angeführt.

Verwenden Sie den Befehl *shutdown /r /f /t 0*, fährt der Computer sofort herunter (*/t 0*), startet neu (*/r*) und schließt alle geöffneten Programme vorher (*/f*). Die Option /f zwingt den Computer zum Beenden der laufenden Anwendungen, auch wenn nicht gespeichert wurde. Der Befehl shutdown /s /f fährt den Computer herunter und startet ihn nicht neu. Mit dem Befehl shutdown /a brechen Sie den aktuellen Vorgang ab. Die wichtigsten Optionen des Shutdown-Befehls sind:

- /g – Startet den Computer neu und fährt registrierte Anwendungen automatisch nach dem Neustart hoch.

- /i – Zeigt die grafische Benutzeroberfläche an. Dies muss die erste Option sein.
- /l – Meldet den aktuellen Benutzer ab. Diese Option kann nicht zusammen mit den Optionen /m oder /d verwendet werden.
- /s – Fährt den Computer herunter.
- /r – Fährt den Computer herunter und startet ihn neu.
- /a – Bricht das Herunterfahren des Systems ab.
- /p – Schaltet den lokalen Computer ohne Zeitlimitwarnung aus. Kann mit den Option /d und /f verwendet werden.
- /h – Versetzt den lokalen Computer in den Ruhezustand.
- /m \\<Computer> – Legt den Zielcomputer fest.
- /t xxx – Stellt die Zeit vor dem Herunterfahren auf xxx Sekunden ein. Der gültige Bereich reicht von 0 bis 600, der Standardwert ist 30. Die Verwendung von /t setzt voraus, dass die Option /f verwendet wird.
- /c „Kommentar“ – Kommentar zum Neustart bzw. Herunterfahren. Es sind maximal 512 Zeichen zulässig.
- /f – Erzwingt das Schließen ausgeführter Anwendungen ohne Vorwarnung der Benutzer. /f wird automatisch angegeben, wenn die Option /t verwendet wird.
- /d [p|u:]xx:yy – Gibt die Ursache für den Neustart oder das Herunterfahren an. p zeigt, dass der Neustart oder das Herunterfahren geplant ist, u sagt, dass die Ursache vom Benutzer definiert ist. Wenn weder p noch u angegeben ist, ist das Neustarten oder Herunterfahren nicht geplant.

5.2.6 PsShutdown.exe mit mehr Optionen

Wem die Optionen von *shutdown.exe* nicht ausreichen, die Windows standardmäßig bietet, der verwendet das Sysinternal-Tool *PsShutdown*. Die Optionen des Tools sind ähnlich. Mit der Option -t können Sie einen Sekundenwert angeben oder den Zeitpunkt festzulegen, zu dem ein Shutdown ausgeführt werden soll. Den Zeitpunkt legen Sie durch die Verwendung der 24-St"unden-Schreibweise fest:

```
psshutdown -m "Dieses System wird aus Wartungsgründen neu
gestartet" -t 23:00 -r
```

Mit -c geben Sie dem Anwender auf dem Computer die Möglichkeit, den Vorgang abzubrechen. Sie können auch gleichzeitig mehrere Systeme neu starten:

```
psshutdown -r \computer1,computer2,computer3
```

Alternativ können Sie die Rechnernamen in eine Textdatei schreiben und diese verwenden:

```
psshutdown -r @rechnerliste.txt
```

In dieser Datei darf in jeder Zeile nur ein Computername aufgelistet sein. Sie müssen bei der Verwendung im Netzwerk das Tool nicht auf jedem Rechner installieren, vielmehr genügt der Start von einem einzelnen Computer aus. Im Vergleich zu shutdown.exe bietet das Tool zusätzliche Optionen, beispielsweise auch die Möglichkeit das System zu sperren.. Das Tool hat folgende Optionen:

```
psshutdown [[\\computer[,computer[...] | @file [-u user [-p
psswd]]] -s|-r|-h|-d|-k|-a|-l|-o [-f] [-c] [-t nn|h:m] [-n s]
[-v nn] [-e [u|p]:xx:yy] [-m "Nachricht"]
```

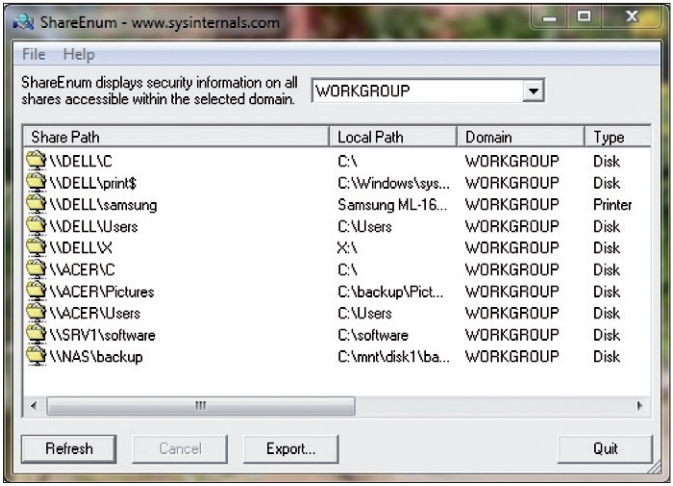
- computer – Gibt an, welchen Computer Sie herunterfahren wollen. Mit der Option * fahren Sie alle Computer der Domäne herunter.
- @file – Verwendet die Datei als Rechnerliste der Computer, die Sie herunterfahren wollen.
- -u – Benutzername, mit dem Sie das Herunterfahren durchführen wollen.
- -p – Kennwort für das Benutzerkonto.
- -a – Bricht einen Vorgang ab.
- -c – Angemeldeter Benutzer kann den Vorgang abbrechen.
- -d – Verordnet dem Computer eine Pause (Suspend).
- -e – Grund für das Herunterfahren (u für Benutzer, p für geplant).
- -f – Geöffnete Anwendungen werden beendet, auch ohne Speichern.
- -h – Ruhezustand aktivieren.
- -k – Computer ausschalten.
- -l – Computer sperren.
- -m – Nachricht zum Herunterfahren.
- -o – Abmelden des Benutzers Logoff the console user.
- -r – Neustart.
- -s – Shutdown ohne ausschalten.
- -t – Shutdown.

5.2.7 ShareEnum – Freigaben im Netzwerk anzeigen

Mit ShareEnum lassen Sie sich alle Freigaben in einem IP-Bereich oder einer Domäne anzeigen. Verfügen Sie über genügend Rechte, können Sie die gefundenen Freigaben per Doppelklick öffnen. Das Tool kann entweder einen IP-Bereich oder alle PCs und Server einer Domäne (oder aller Domänen) auf Freigaben scannen.

ShareEnum zeigt nicht nur die Freigaben an, sondern auch den lokalen Pfad der Freigabe auf dem Server. Über die Schaltfläche *Refresh* starten Sie einen neuen

Scanvorgang. Wollen Sie nur einen Server scannen, geben Sie als IP-Bereich als Start- und Endadresse die gleiche IP-Adresse an.



Freigiebig: ShareEnum zeigt alle Freigaben im Netzwerk an.

In Domänen funktioniert das Tool nicht auf den Domänencontrollern, sondern nur auf Arbeitsstationen. Sie müssen *ShareEnum* mit Administratorrechten starten. Neben Freigaben sehen Sie auch die freigegebenen Drucker im Netzwerk. Wenn Sie die Eigenschaften aufrufen, sehen Sie auch die Sicherheitseinstellungen der Freigaben im Netzwerk. Das Tool ist nicht vollständig kompatibel zu Windows Server 2003/2008/2008 R2. Ausprobieren lohnt sich aber, da der Umgang einfach ist und Sie umfangreiche Informationen über die Freigaben im Netzwerk erhalten.

5.2.8 WhoIs

Mit WhoIs können Sie Informationen über einzelne Server im Internet abrufen und prüfen, welcher Domäne diese zugeordnet sind. In erster Linie wird dieses Befehlszeilenprogramm eingesetzt, um festzustellen, zu welcher Domäne eine IP-Adresse im Internet gehört. Wenn Sie in der Befehlszeile den Befehl

```
whois <IP-Adresse>
```

eingeben, erhalten Sie als Informationen den Domäneninhaber der IP-Adresse. Die Abfrage ist allerdings nicht immer erfolgreich.

Thomas Joos

5.3 Empfehlenswerte Linux-Distributionen für die Netzwerksicherheit

Linux als Server hat sich schon lange etabliert. Bei einigen erfreut sich das freie Betriebssystem auch auf dem Desktop großer Beliebtheit. Interessierte werden sicher unter unseren zehn empfehlenswerten Linux-Distributionen für Desktops fündig. Auf vielen mobilen Geräten ist es ohnehin anzutreffen, häufig wird es aber als solches nicht wahrgenommen.

Es existieren jedoch auch diverse Linux-Ausführungen, die sich explizit mit der Sicherheit respektive dem Schutz des Netzwerks beschäftigen. Diese sind allerdings häufig auch Hybride oder „All in One Server"-Lösungen. In diesem Artikel stellen wir einige Linux-Distributionen rund um die Sicherheit vor.

5.3.1 Firewall und Router: Endian

Die Endian-Firewall (www.endian.com) gibt es als kostenlose Community-Edition, wird aber auch als kommerzielles Produkt angeboten. Zwischen den beiden Produkten gibt es durchaus gravierende Unterschiede. Für die frei verfügbare Community-Version bekommen Sie zum Beispiel keine kommerzielle Unterstützung von Endian. Ebenso gibt es keine Hardwareausgabe, und die Community-Edition lässt sich nicht als Hotspot einsetzen. Die Firma selbst schlägt die Community-Edition vor, wenn man eine kleine Non-Profit-Organisation hat oder diese im Heimbereich (SoHo) einsetzen möchte.

Endian verträgt sich zudem nicht mit anderen Betriebssystemen auf derselben Hardware. Verständlich, denn eine Firewall als Dual-Boot-System würde auch nicht viel Sinn ergeben. Dennoch sollten Sie wissen, dass eine Installation sämtliche Daten auf dem jeweiligen Rechner löscht.

Firewall und Router: In diesem Dialog von Endian konfigurieren Sie die Netzwerkkarte für das LAN.

Die Installation ist in wenigen Schritten durchgeführt. Sie müssen eigentlich nur bei der Vergabe der IP-Adresse der Schnittstelle GREEN aufpassen. Hierbei handelt es sich um die Netzwerkkarte, die sich im inneren Netzwerk befindet. Mit der

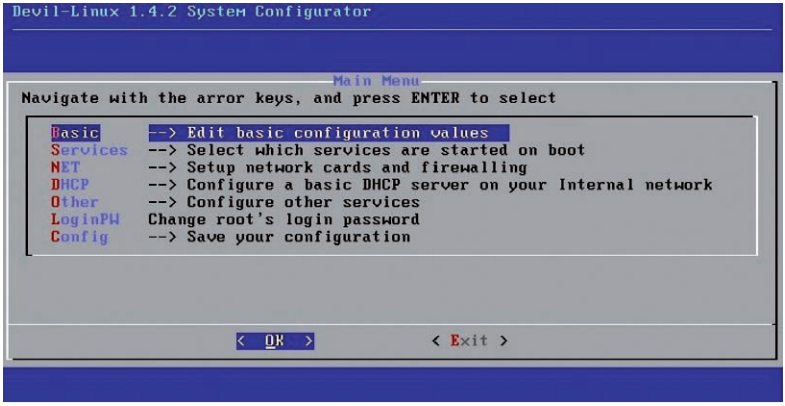
hier vergebenen IP-Adresse erreichen Sie später auch die Administrationsoberfläche via Browser. Ebenfalls wissenswert: Nach einer Installation lautet das root-Passwort endian.

Um die Installation vollständig abzuschließen, rufen Sie im Browser *https://<IP-Adresse GREEN>:10443* auf. Hier können Sie nun beispielsweise Sprache oder Zeitzone vergeben. Ebenso müssen Sie die Lizenzbestimmungen anerkennen. Haben Sie eine Datensicherung, können Sie diese ebenfalls einspielen. Während dieser Phase werden Sie auch aufgefordert, die entsprechenden Passwörter zu ändern. In den weiteren Schritten setzen Sie nun die Netzwerkschnittstellen auf und definieren unter anderem die nach außen gehende Schnittstelle ROT.

Alles in allen greift einem der webbasierte Wizard unter die Arme, und eine Installation ist wirklich in weniger als zehn Minuten durchgeführt. Dies setzt natürlich grundlegende Netzwerkkenntnisse voraus.

5.3.2 Devil Linux: von Admins für Admins

Die Entwickler von Devil Linux (www.devil-linux.org) sagen, dass diese Distribution von IT-Administratoren für IT-Administratoren gemacht wurde. Von daher wisse man, was der Admin so braucht, denn man habe schließlich dieselben Anforderungen. Das Betriebssystem startet in der Regel von einer CD-ROM, die nur lesbar sein sollte. Aus diesem Grund tun sich Angreifer schwer, zum Beispiel rootkits einzuschleusen.



Für Admins: Die Konfiguration von Devil Linux ist nicht hübsch, aber übersichtlich und verständlich.

Neuere Ausgaben lassen sich auch mit einem speziell entwickelten Script auf einen USB-Stick installieren und davon starten. Die Konfiguration kann man auf einer Diskette oder einem USB-Flash-Gerät speichern.

Traditionell ist Devil Linux eine reine Firewall-Distribution. Allerdings wurde das Betriebssystem über die Jahre weiterentwickelt und lässt sich auch zu mehr einsetzen. Mögliche Serverdienste, die Devil Linux zur Verfügung stellt, sind: Proxy, DNS, Mail mit TLS-Unterstützung inklusive Spam- und Virus-Filter, HTTP, FTP, Datei, VPN mit X.509-Unterstützung, DHCP, NTP und IDS Node.

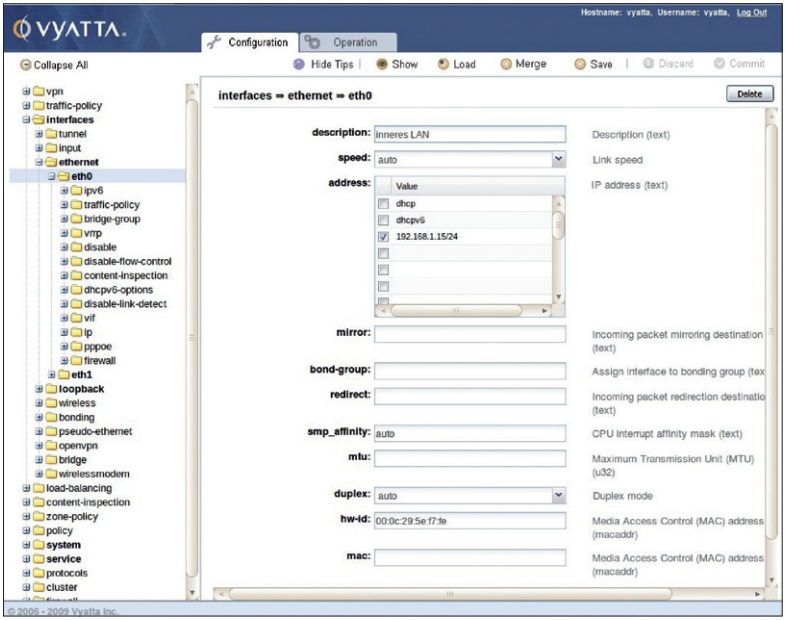
Normalerweise braucht Devil Linux keine Festplatte. Dies ist natürlich anders, wenn Sie die Distribution als Mail- oder Datei-Server verwenden möchten. Deswegen können Sie natürlich Festplattenspeicher optional einbinden. Devil Linux benutzt hierfür den Logical Volume Manager. Somit ist das Anfügen von Plattenplatz oder das Warten der Massenspeicher relativ einfach.

Wenn man Devil Linux startet, dürfte man zunächst etwas verdutzt sein: kein Hinweis auf das Standardpasswort, IP-Adressen oder Installationsanleitungen – doch wenn man es weiß, ist es nicht schwer. Das Standardpasswort für root ist leer. Nach dem Anmelden hilft der Befehl *setup* auf der Kommandozeile. Devil Linux erscheint zunächst sehr rudimentär. Ein Stöbern in der Setup-Routine bringt aber ans Licht, dass es sich hier um eine doch recht mächtige Sicherheitsdistribution handelt. Sogar Webmin ließe sich aktivieren, um einer Turnschuhadministration zu entgehen.

5.3.3 Mit Vyatta Linux das Netzwerk schützen

Eigentlich lässt sich die Firewall- und Router-Distribution Vyatta Linux auch von CD betreiben. Die Entwickler raten davon allerdings ab und empfehlen die Installation auf die Festplatte. Dies sei einfach komfortabler in einer produktiven Umgebung, und man brauche die Konfiguration nicht auf einem externen Datenträger zu speichern. Nach dem Start von der CD benutzen Sie zum Anmelden *vyatta* als Benutzer und *vyatta* als Passwort. Mit dem Befehl *install-system* beginnen Sie den Installationsvorgang. Auch hier will das Betriebssystem die Festplatte für sich haben und weist auf einen möglichen Datenverlust hin. Die Installation geht mehr oder weniger automatisch vor sich. Nach einem Neustart können Sie sich mittels des während der Installation vergebenen Passworts anmelden. Doch nun steht man zunächst etwas allein gelassen da: keine Hinweise, wie es weitergehen soll, keine IP-Adresse, einfach nichts.

Das Eintippen des Befehls *configure* hilft da weiter. Nun ändert sich auch das Zeichen vor dem Eingabemodus von einem „$“ in ein „#“. Somit wissen Sie, wann Sie sich im Konfigurationsmodus befinden. Nun können wir den Rechner zunächst erreichbar machen, indem wir der inneren Netzwerkkarte eine IP-Adresse und eine optionale Beschreibung zuweisen: *set interfaces ethernet eth0 address 192.168.1.15/24* und *set interfaces ethernet eth0 description „inneres LAN“*.

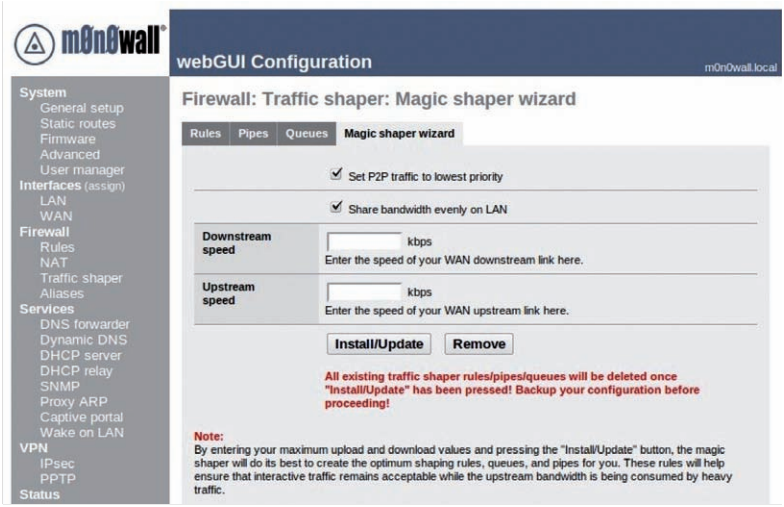


WebGUI: Vyatta lässt sich auch über den Browser administrieren.

Um die Änderungen wirksam zu machen, tippen Sie nun *commit* ein und bestätigen dies mit der Eingabetaste. So können Sie das ganze System administrieren, was zugegebenermaßen ein bisschen umständlich ist. Im Konfigurationsmodus können Sie aber mittels *set service https* und *commit* die Webadministration aktivieren. Nun erreichen Sie den Server unter *https://<IP-Adresse>* und können sich mit *vyatta* und dem vergebenen Passwort anmelden. Selbst mit Weboberfläche eignet sich Vyatta allerdings nur für Netzwerk-, Router- und Firewall-Kenner. Allein mit Ausprobieren kommen Sie bei dieser Distribution nicht weit.

5.3.4 Abbild unter 10 MByte: m0n0wall

Das auf Sicherheit getrimmte Betriebssystem m0n0wall (www.m0n0.ch) fällt ein wenig aus der Reihe, weil es genau genommen auf FreeBSD basiert. Alle Abbilder dieses Systems sind weniger als 10 MByte groß. Schön daran ist, dass es ein VMware-Abbild für Experimentierfreudige gibt. Somit muss man m0n0wall nicht installieren, sondern kann sofort loslegen. Wobei eine Installation auch einfach von der Hand geht: Nach dem ersten Start begrüßt Sie m0n0wall mit einem einfachen Konfigurationsmenü. Dort können Sie eine IP-Adresse für das LAN vergeben, über die Sie später die Webadministrationsoberfläche aufrufen.



Verkehrspolizei: Mit Traffic Shaping lässt sich in m0n0wall der Datenverkehr regulieren.

Per Standard melden Sie sich mit *admin* und *mono* an der Weboberfläche an. Hier sehen Sie nun deutlich, dass es sich bei m0n0wall ein wenig um einen Hybriden handelt. Es ist das klassische Router-/Firewall-Betriebssystem. Schön ist allerdings, dass m0n0wall einen Traffic Shaper eingebaut hat.

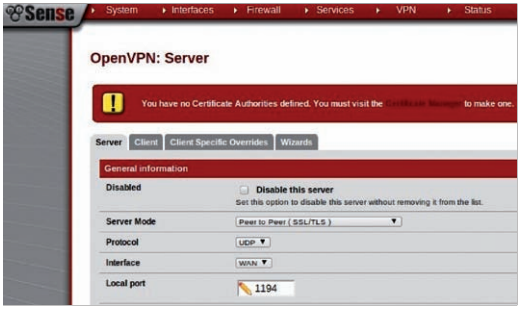
Sieht man sich die Größe der Abbilder an, gibt es wohl kaum mehr Firewall und Router pro MByte. Etwas schade, dass OpenVPN nicht integriert ist. Hierzu gibt es einen Eintrag im Handbuch, dass die Entwickler Probleme mit OPT-Schnittstellen in den Betaversionen von 1.2 hatten, die bis dato nicht gelöst sind. IPSec und PPTP funktionieren aber.

5.3.5 Auf FreeBSD basierend: pfSense

pfSense (www.pfsense.org) basiert ebenfalls auf FreeBSD. Genau gesagt ist es sogar ein Derivat von m0n0wall, das sich im Jahre 2004 davon abspaltete. Man könnte es fast als ein aufgebohrtes m0n0wall bezeichnen, das die Basis erweitert.

Das System ist in drei verschiedenen Geschmacksrichtungen erhältlich: einer Live-CD mit Installer, einer Ausgabe zur Installation auf Festplatten und einer Embedded-Version, die sich speziell für Compact-Flash-Karten eignet. Flash-Speicherkarten vertragen nur eine begrenzte Anzahl an Schreibvorgängen, und somit sind die schreibbaren Dateisysteme in den Arbeitsspeicher ausgelagert. Da sich Version 2.0 bereits im Stadium Release-Kandidat 1 befindet, haben wir diese Ausgabe unter die Lupe genommen.

Sehr angenehm fällt auf, dass pfSense nicht nur mit IPSec und PPTP, sondern auch mit OpenVPN und L2TP umgehen kann. pfSense hat zum Beispiel auch S.M.A.R.T.-Monitoring-Tools an Bord. Das hat zwar nichts mit Firewall oder Router zu tun, dennoch kann es nicht schaden, wenn der Administrator über eventuell kaputtgehende Festplatte informiert ist. Somit kann er einem Ausfall vorbeugen.



VPN-Server: pfSense können Sie als openVPN-Server betreiben.

Ebenso dient das von OpenBSD kommende CARP (Common Address Redundancy Protocol) der Ausfallsicherheit. Hier lassen sich zwei oder mehr Firewalls als Faillover konfigurieren. Mittels pfsync kann die Konfiguration des primären Geräts auf die Failover-Rechner übertragen werden. Sollte also die Haupt-Firewall ausfallen, springt ein Ersatzmann ein.

5.3.6 Die Netzpolizei: IPCop

„Diese bösen Datenpakete stoppen hier", schreiben sich die Entwickler von IPCop (www.ipcop.org) auf die Fahnen. Wie die meisten anderen beansprucht auch IPCop die ganze Festplatte und löscht die bis dato darauf vorhandenen Daten.

Backups blitzschnell: Obwohl recht einfach gehalten, ist das Datensicherungs-System von IPCop wirkungsvoll und in den meisten Fällen völlig ausreichend.

Zum Installieren folgen Sie einfach den Anweisungen des Wizard. IPCop stellt die Netzwerkschnittstellen GREEN, RED, ORANGE und BLUE zur Verfügung. Die meisten Anwender dürften GREEN, die das Verbindungsglied zum schützenden Netzwerk bildet, und RED, die nach außen geht, benutzen. ORANGE wäre für DMZ-Verbindungen und BLUE für zusätzliche Access Points.

Nach der Installation erreichen Sie das Web-Frontend via *http://<IP-Adresse des IPCop-Rechners>:81*. Neben den klassischen Firewall- und Router-Diensten bietet IPCop auch einen Proxy- und DHCP-Server sowie dynamische DNS-Dienste. Ebenso können Sie die Netzlast mittels Traffic Shaping regulieren. Einbrüche lassen sich via Snort erkennen. Schön ist, dass Sie IPCop komplett auf Deutsch umstellen können. Die Entwickler von IPCop arbeiten schon seit längerer Zeit an Version 2.0. Dort werden Sie eine komplett überarbeitete Administrationsoberfläche und viele neue Funktionen finden. Wann die neue Version von IPCop verfügbar sein wird, steht allerdings noch nicht fest.

5.3.7 Übersichtlich: SmoothWall Express

Das SmoothWall-Projekt (www.smoothwall.org) gibt es bereits seit dem Jahr 2000. Das Ziel war damals wie heute, einen Rechner in eine gestählte Firewall zu verwandeln. Seit 2005 basiert das Projekt auf dem Linux-Kernel 2.6. Weiteres Ziel der Entwickler ist, dass SmoothWall auch von Heimanwendern ohne großes Linux-Wissen eingesetzt werden kann. Die Administration erfolgt über einen Webbrowser. Breite Hardwareunterstützung ist ebenfalls im Fokus. Dies gilt natürlich in erster Linie für Netzwerkkarten und Modems.

Wartung mittels WebGUI: Die Browser-Oberfläche der Firewall-Distribution SmoothWall Express.

SmoothWall Express hält, was der Name verspricht: Die Installation ist in weniger als zehn Minuten komplett abgeschlossen. Netterweise bekommt man Hinweise, dass die Webadministrationsoberfläche mittels *http://<IP-Adresse oder Name>:81 oder https://<IP-Adresse oder Name>:441* erreichbar ist.

Mit dem Firewall-System können Sie auch sehr schnell einen Web-Proxy, ein IDS (Intrusion Detection System) und einen pop3-Proxy aufsetzen. Die Administration ist wirklich einfach. Ebenfalls schön ist, dass Anwendern mehrere dynamische IP-Anbieter zur Verfügung stehen. So können Sie Ihre Verbindung mit wenigen Klicks zum Beispiel bei DynDNS.org einrichten.

5.3.8 Fazit

Alle hier genannten Distributionen erfüllen die Arbeit gleichermaßen gut, wenn sie entsprechend konfiguriert sind. Im Prinzip verwenden sie alle dieselben Komponenten. Sicherlich lassen sich einige komfortabler administrieren als andere oder bieten mehr Funktionen an.

Mehr Funktionen bedeuten aber auch mehr Angriffsfläche, was man auf einer Firewall eigentlich gerade vermeiden möchte. Einen klaren Gewinner zu küren ist daher nicht angebracht. Die verschiedenen Distributionen werden mit leicht unterschiedlichen Hintergründen entwickelt, und jede hat ihre Daseinsberechtigung. Vielmehr dürfte es Geschmacksache des Administrators sein, mit welcher er sich am wohlsten fühlt. Ein Firewall- oder Router-System muss schließlich funktionieren und nicht hübsch sein.

Administratoren müssen sich also gut überlegen, welchen Zweck das System erfüllen soll. Ebenso sollten Anwender schon eine Ahnung davon haben, was sie hier tun und wie kritisch das Netzwerk hinter der Brandschutzmauer ist. Hat eine Firma das nötige Know-how in den eigenen Reihen, erfüllen kostenlose Community-Editionen sicher ihren Zweck sehr gut.

Mit „Wird schon passen"-Mentalität und gefährlichem Halbwissen sollte man eine Firewall allerdings nicht administrieren oder aufsetzen. Je kritischer das Netz dahinter ist, desto mehr wäre in solch einem Fall am komplett falschen Ende gespart. Die Entwickler der einen oder anderen hier vorgestellten Sicherheitsdistributionen bieten professionelle Unterstützung an – im Zweifel also lieber die Profis ranlassen.

Jürgen Donauer

Jürgen Donauer war als Systemadministrator zunächst für Informix und später IBM tätig. Dann verschlug es ihn in das Rechenzentrum von Media-Saturn . Dort kümmerte er sich mitunter um die Webserver, Datenbankanbindungen und den Online-Shop. Anschließend war er als Redakteur im Bereich Linux für TecChannel tätig. Derzeit arbeitet Jürgen Donauer als freier Autor für TecChannel sowie als Privatdozent.

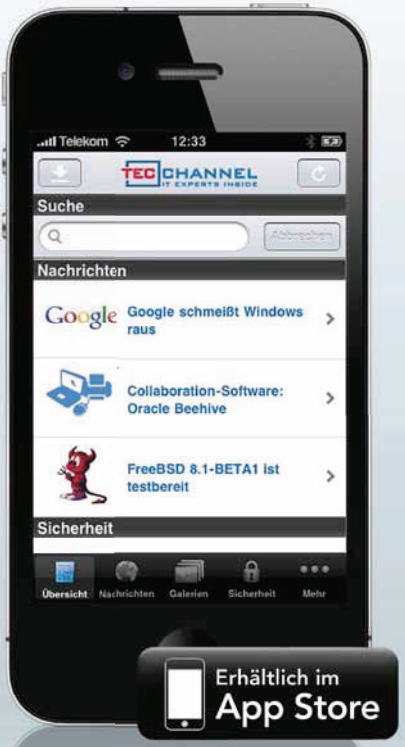
Die neue TecChannel App

Alles drin. Immer dabei. Jetzt fürs iPhone.

News, Infos, Tipps & Tricks für unterwegs!

- topaktuelle News
- Hintergründe
- Analysen
- Tests und Bilderstrecken

» Gratis laden



Vorraussetzungen: Kompatibel mit iPhone, iPod touch und iPad. Erfordert iOS 3.0 oder neuer.

www.tecchannel.de/iphoneapp

Einfach QR-Code mit dem Codereader Ihres iPhones einscannen.Sie werden direkt in den App-Store verlinkt und können die App downloaden. Einen kostenlosen Reader erhalten Sie z.B. unter http://get.beetagg.com/. Es entstehen lediglich Kosten für die Verbindung ins (mobile) Internet.

IDG BUSINESS MEDIA GMBH