Liebe Leserin, lieber Leser,

edel sei der Admin, hilfreich und gut. Das jedenfalls erwarten Chefs, Familie und Freunde, die sich hilfesuchend an Sie wenden. Ob Clients vergeblich den Domänen-Controller suchen, Router ein Eigenleben führen, Server lahmen oder Festplatten schlicht verschleißen und ersetzt werden wollen – an Arbeit mangelt es nie.

Das im Sinn, haben wir diese c't-Sonderausgabe so konzipiert, dass sie Ihnen mit fundierten Praxisbeiträgen den Alltag erleichtert.

Am Anfang stehen wichtige Methoden rund um Windows: Automatisierte Einrichtung, Vernetzung und Wartung halten das Arbeitspferd in Gang. Dazu geben wir Handreichungen für den Umgang mit Heimnetzgruppen und Clients im Firmen-LAN. Wo gehobelt wird, fliegen auch Späne, und auch ein Windows muss mal repariert werden. Wir zeigen, wie das Minibetriebssystem Windows PE dabei hilft.

Server sollen möglichst reibungslos laufen. Dafür geben wir Hilfestellung bei der Fernwartung und Vorsorge gegen Platten- und Stromausfälle. Hat ein Server seine letzte Milch gegeben, unterstützen wir Sie bei der Auswahl von aktuellen Server-Mainboards, Betriebssystemen und kompletten Geräten für kleine Netze.

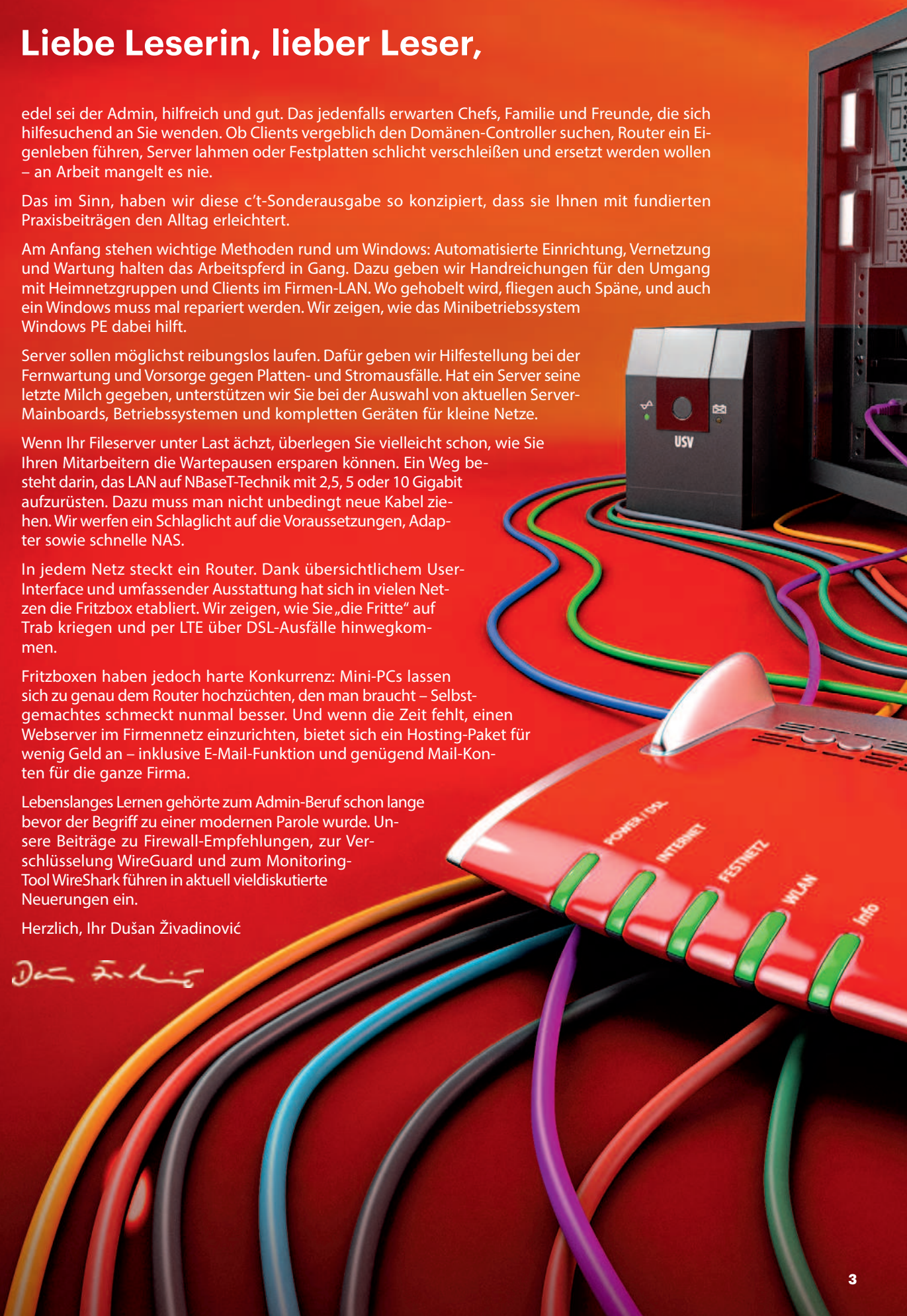
Wenn Ihr Fileserver unter Last ächzt, überlegen Sie vielleicht schon, wie Sie Ihren Mitarbeitern die Wartepausen ersparen können. Ein Weg besteht darin, das LAN auf NBaseT-Technik mit 2,5, 5 oder 10 Gigabit aufzurüsten. Dazu muss man nicht unbedingt neue Kabel ziehen. Wir werfen ein Schlaglicht auf die Voraussetzungen, Adapter sowie schnelle NAS.

In jedem Netz steckt ein Router. Dank übersichtlichem User-Interface und umfassender Ausstattung hat sich in vielen Netzen die Fritzbox etabliert. Wir zeigen, wie Sie „die Fritte" auf Trab kriegen und per LTE über DSL-Ausfälle hinwegkommen.

Fritzboxen haben jedoch harte Konkurrenz: Mini-PCs lassen sich zu genau dem Router hochzüchten, den man braucht – Selbstgemachtes schmeckt nunmal besser. Und wenn die Zeit fehlt, einen Webserver im Firmennetz einzurichten, bietet sich ein Hosting-Paket für wenig Geld an – inklusive E-Mail-Funktion und genügend Mail-Konten für die ganze Firma.

Lebenslanges Lernen gehörte zum Admin-Beruf schon lange bevor der Begriff zu einer modernen Parole wurde. Unsere Beiträge zu Firewall-Empfehlungen, zur Verschlüsselung WireGuard und zum Monitoring-Tool WireShark führen in aktuell vieldiskutierte Neuerungen ein.

Herzlich, Ihr Dušan Živadinović



Inhalt

Windows vernetzen

Server flexibel einsetzen

Fritzbox optimieren

Titelzeilen sind orange hervorgehoben

Intelligentes WLAN

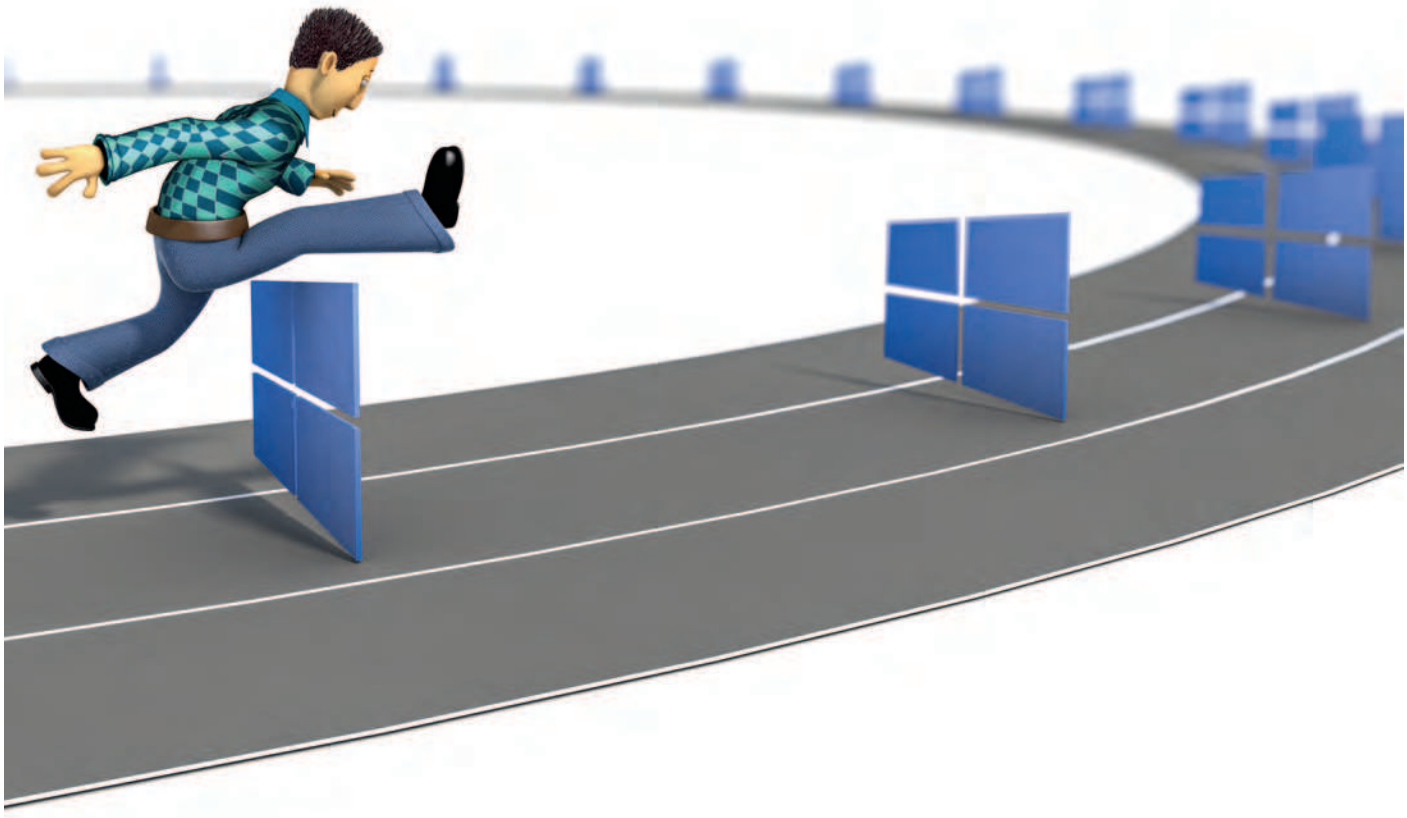
Router & Router-Selbstbau

Hardware für schnelle Netze

Webserver betreiben

Netzwerk absichern

Zum Heft



Hürdenlauf

Windows-10-Clients für das Unternehmensumfeld vorbereiten

Wer Windows 10 im professionellen Umfeld einsetzen will, muss Hand anlegen: Store, Kacheldesign, Cortana und Feature-Updates brauchen einige Gruppenrichtlinien, um im Unternehmen nicht negativ aufzufallen.

Von Jan Mahn

Im Januar 2020 ist Schluss – Microsoft ist fest entschlossen, den Extended Support für Windows 7 wie geplant nach zehn Jahren einzustellen. Bis dahin sollten Administratoren alle Computer mit Online-Anbindung auf Windows 10 umgestellt haben. Doch wer schon einmal ein frisch installiertes Windows 10 Professional gesehen hat, fragt sich spätestens bei den animierten Spiele-Kacheln, ob Microsoft die Zielgruppe der Unternehmenskunden vollkommen vergessen hat. Zum Glück braucht es nur eine großzügige Portion Gruppenrichtlinien, um das Betriebssystem für den professionellen Einsatz bereit zu machen. Voraussetzung sind Kenntnisse im Umgang mit Gruppenrichtlinien und die aktuellen admx-Vorlagen für Windows 10. An einige Bedienelemente werden sich die Anwender aber trotz aller Anstrengungen gewöhnen müssen.

Litfaßsäule abbauen

Die erste, weil offensichtlichste Baustelle ist der Kachel-Bereich des Startmenüs. Was Windows dort anzeigen soll, definieren Sie über eine XML-Datei, die Sie einmalig auf einem Referenzcomputer oder in einer virtuellen Maschine erzeugen müssen. Dieser sollte die gleiche Windows-Version (Professional, Enterprise oder Education) haben wie die Zielcomputer und alle Programme installiert haben, für die Sie Kacheln anzeigen möchten. Melden Sie sich mit einem lokalen Benutzerkonto an und verschieben, entfernen und gruppieren Sie alle Kacheln, bis das Startmenü Ihren Wünschen entspricht. Für den Export öffnen Sie die PowerShell und führen Sie den Befehl `export-startlayout` aus und geben einen Dateinamen mit der Endung xml an:

```
export-startlayout ↵
↳-path C:\users\joe\desktop\start.xml
```

Auf dem Desktop des Benutzers `joe` erscheint eine XML-Datei, die Sie mit einem Texteditor Ihrer Wahl öffnen sollten – denn perfekt ist das Ergebnis noch nicht. Haben Sie herkömmliche Programme (Microsoft nennt sie „Desktop-Apps“) hinzugefügt, tauchen diese in der XML-Datei mit dem Attribut `DesktopApplicationLinkPath` auf, das auf eine Verknüpfung (Lnk-Datei) im Startmenü verweist. Um nicht auf die Existenz dieser Einträge angewiesen zu sein, empfiehlt Microsoft, diesen Pfad durch das Attribut `DesktopApplicationID` zu ersetzen. Eine solche ID bekommt jedes Programm, das sich bei der Installation im klassischen Startmenü eingetragen hat. Um sie herauszufinden, nutzen Sie den PowerShell-Befehl

```
get-startapps | fl
```

Sie erhalten eine Liste aller Programme mit einem Klarnamen und einer ID. Kopieren Sie diese für die Anwendung heraus und

ersetzen Sie damit die Pfadangabe. Eine Kachel für die Remotedesktop-Verbindung ganz oben links sieht dann so aus:

```
<start:DesktopApplicationTile
 DesktopApplicationID=
 "Microsoft.Windows.RemoteDesktop"
 Size="2x2"
 Row="0"
 Column="2"/>
```

Verteilen Sie diese XML-Definition per Gruppenrichtlinie, hat der Benutzer keine Chance mehr, selbst Kacheln zu verändern. Um ihm das zu ermöglichen, ist ein zusätzliches Attribut im XML-Tag `DefaultLayoutOverride` nötig:

```
<DefaultLayoutOverride
LayoutCustomizationRestrictionType=
"OnlySpecifiedGroups">
```

Ist das Startmenü fertig gestaltet, kopieren Sie die XML-Datei auf ein Netzlaufwerk, auf das jeder Computer zugreifen kann. Die zuständige Gruppenrichtlinie „Startlayout“ finden Sie entweder unter „Computerkonfiguration“ oder unter „Benutzerkonfiguration“ im Gruppenrichtlinieneditor unter „Richtlinien/Administrative Vorlagen/Startmenü und Taskleiste“. Aktivieren Sie diese und übergeben Sie einen Netzwerkpfad zur XML-Datei, eingeleitet durch „\\“. Optional könnten Sie die Datei auch vorher auf die Festplatten der Clients kopieren und einen lokalen Pfad angeben.

Schaufenster vernageln

Der Store öffnet das Tor zur weiten Welt: Nutzer können an Softwareverteilung und zentraler Update-Bereitstellung vorbei nach Belieben Filme, Musik, Spiele- und Unterhaltungs-Apps herunterladen. Auf den ersten Blick gibt es dagegen eine einfache Gruppenrichtlinie „Store-Anwendung deaktivieren“ im Ordner „Richtlinien/Administrative Vorlagen/Windows-Komponenten“. In der Beschreibung fehlt jedoch der entscheidende Hinweis, dass diese nur für Windows 10 Enterprise und Education (ausschließlich für Bildungseinrichtungen) wirksam ist. Gleiches gilt für die Richtlinie „Alle Apps aus dem Windows Store deaktivieren“. Unter „Windows-Komponenten/Cloudinhalt“ finden Enterprise-Administratoren die Richtlinie „Microsoft-Anwenderfeatures deaktivieren“, die dafür sorgt, dass dem Benutzer keine Apps mehr vorgeschlagen werden – im gleichen Ordner kann man auch die Windows-Tipps deaktivieren.

Wer Windows 10 Professional gern ohne „Candy Crush Soda Saga“ und ähnliche Apps betreiben möchte, muss etwas mehr Zeit investieren.

Um sich einen Überblick über den App-Bestand auf einem Rechner zu machen, hilft der PowerShell-Befehl `Get-AppxPackage`, beschränkt auf die Rückgabe des internen Paketnamens:

```
Get-AppXPackage | Select-Object ↵
↳-Property Name
```

Einen einzelnen Eintrag wie `Microsoft.WindowsStore` könnten Sie für den gerade angemeldeten Nutzer mit `Remove-AppxPackage` entfernen. Alle Apps verschwinden mit der folgenden Zeile, die Sie zum Beispiel als Start-Skript verteilen können:

```
Get-AppxPackage * | Remove-AppxPackage
```

Bevor Sie sich zu diesem drastischen Schritt entscheiden, überprüfen Sie, ob Sie wirklich alle Apps wegwerfen möchten: Taschenrechner, Karten und Wetter werden einige Nutzer vielleicht vermissen. Sollen bestimmte Apps gar nicht erst für jeden Benutzer eingerichtet werden, müssen Sie die „ProvisionedPackages“, eine Liste der Standard-Apps, bearbeiten. Der Befehl `Get-AppXProvisionedPackage -Online` in einer PowerShell mit Administratorrechten verrät Ihnen, welche Apps ein neuer Benutzer bei der Erstanmeldung bekommt. Sehr elegant funktioniert das Löschen von Standard-Apps aus der Liste, wenn man den PowerShell-Befehl `Out-GridView` einspannt. Der folgende Aufruf öffnet eine grafische Oberfläche in einem neuen Fenster:

```
Get-AppxProvisionedPackage -Online |↵
↳ Out-GridView -PassThru | ↵
↳Remove-AppxProvisionedPackage -Online
```

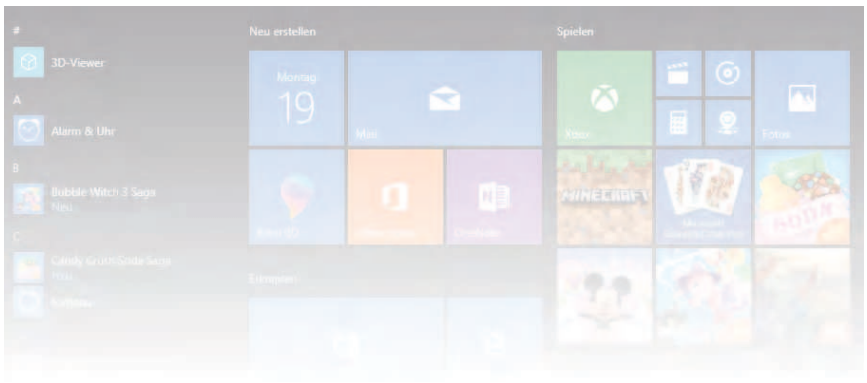
Markieren Sie in der Tabelle eine oder – mit gedrückter Strg-Taste – mehrere Apps und bestätigen Sie mit „OK“. Nach einem neuen Aufruf sind die unliebsamen Pakete verschwunden. Auch den Store selbst (und den Xbox-Store) entfernen Sie auf diese Weise. Um diese Einstellungen zu verteilen, gibt es verschiedene Ansätze, die alle zum Ziel führen: Arbeiten Sie mit Windows-Bereitstellungsdiensten, können Sie ein Aufzeichnungsabbild starten, die oben beschriebenen Schritte ausführen und das Image einpacken lassen. Ein anderer Weg zu einem Image führt über `dism`. Mounten Sie ein Windows-Image über den Befehl

```
Dism /Mount-Image /ImageFile:<pfad>\↵
↳install.wim /index:1 /MountDir:<ziel>
```

Entfernen Sie jetzt eine App über

```
Dism /Image:<pfad> ↵
↳/Remove-ProvisionedAppxPackage ↵
↳ PackageName <name des App-Pakets>
```

Setzen Sie als Namen des Pakets den vollständigen Paketnamen (nicht den Anzeigenamen) ein. Anschließend unmounten Sie das Image wieder, bevor Sie es zur Installation verteilen:



Mit und ohne Bastelei

Hilfe für die Server-Betriebssystemauswahl

Wenn ein einfaches NAS den Ansprüchen nicht mehr genügt und Clouddienste nicht infrage kommen, hilft ein eigener Server. Welches Betriebssystem darauf das richtige ist, hängt sowohl von den Anforderungen als auch vom eigenen Background ab.

Von Peter Siering

Ein eigener Server, der üblicherweise durchgehend läuft, kann allerhand nützliche Dinge erledigen: Dateien bereitstellen, Drucker verwalten, E-Mails empfangen, senden und aufbewahren, gemeinsame Kalender parat halten, die Musik- und Filmsammlung organisieren und an Abspielgeräte liefern, als Ziel für Backups dienen, die Update-Verteilung dosieren, seinen Nutzern weitere Kommunikationsmöglichkeiten eröffnen, das smarte Heim auf Trab halten und mehr.

Bei der Auswahl eines Betriebssystems für Ihren Server sollten Sie sich nicht allein von den Features leiten lassen: Es ist nicht alles sinnvoll, was möglich ist. Die tollsten Funktionen nützen nichts, wenn Sie sie nicht gezähmt bekommen. Die gängigen generischen Linux-Server-Distributionen wie CentOS, Ubuntu-Server oder Debian sind für Experten gemacht, die kein Problem damit haben, Konfigurationsdateien zu bearbeiten und sich Informationen im Netz zusammensuchen.

Linux-Distributionen für Server gibt es aber durchaus in einer Form, die für Laien oder Einsteiger geeignet sind: Sie bringen grafische Bedienoberflächen mit, die sich per Webbrowser erreichen lassen. Die decken alle wesentlichen Aufgaben von der Erstkonfiguration bis hin zu täglichen Aufgaben ab. Die Hersteller leben meist vom Verkauf von Supportabonnements und erlauben vielfach die unentgeltliche Nutzung etwa in Privathaushalten. Community-Foren liefern in Grenzen kostenlosen Support. Das Folgende stellt einige vor. Die Tabelle auf Seite 111 fasst die in dieser Oberfläche erreichbare Grundausstattung zusammen.

Betriebssystem²

Vor der Inbetriebnahme eines Servers sollte man sich überlegen, ob er nicht vielleicht besser in einer virtuellen Maschine (VM) laufen soll. Heutige Hardware ist so leistungsfähig, dass die kleine Mehrbelastung nur bei leistungshungriger Software auffällt.

Virtualisierung schafft zwar eine weitere Komplexitätsebene – schließlich will auch die verwaltet werden – aber bringt auch viele Vorteile mit sich: Eine Server-VM kann man kopieren, sodass man komplexe Änderungen an einer Kopie des Produktivsystems durchspielen kann. Eine VM lässt sich bequemer sichern, bei manchen Produkten sogar regelmäßig auf einen zweiten Server an einem anderen Standort. Hardware-Havarien verlieren so ihren Schrecken.

Ein weiterer Vorteil der Virtualisierung besteht darin, dass man parallel zum Linux-Server auch einen Windows-Server laufen lassen kann, wenn man den partout für eine Software braucht – das gilt natürlich auch umgekehrt. Mit mehreren VMs auf einem Server lastet man aktuelle Hardware womöglich auch erst aus. Statt mehrerer Systeme stellt man ein dickes hin – oder teilt die VMs der Redundanz zuliebe gleich auf zwei Server an verschiedenen Standorten auf.

Welche Software man dafür hernimmt, bleibt eine Geschmackssache. Mit Proxmox gibt es eine hübsche Lösung, die auf Basis von Debian mit ZFS als Dateisystem die automatische Synchronisation von VMs über mehrere Server hinweg erlaubt. Ohne Supportanspruch kann man Proxmox kostenlos nutzen. Microsoft verschenkt seine Virtualisierung mit dem Hyper-V-Server, allerdings ohne GUI (das muss man dann auf einem Client ausführen). Auch VMware hat mit dem ESXi-Server ein kostenlos nutzbares Programm im Portfolio; Funktionen zum automatisierten Kopieren von VMs gibt es bei VMware nur gegen Geld.

Windows für Server

Software für Server stellt auch Microsoft her. Traditionell bringen diese Infrastrukturdienste mit: Der Verzeichnisdienst, das Active Directory, stellt eine zentrale Benutzerdatenbank bereit. Andere Systeme im Netz vertrauen ihr, sodass man sich an alle Netzwerkressourcen mit einem Namen und Passwort anmelden kann. Ergänzt wird das mit Netzwerkdiensten, etwa zur Namensauflösung (DNS) sowie für Adressvergabe (DHCP) und -Management (IPAM).

Über Gruppenrichtlinien können Administratoren Konfigurationsvorgaben allen Nutzern oder Systemen im Netz verordnen. Datei- und Druckfreigaben gehören ebenfalls zum normalen Leistungsumfang. Die regulären Server können darüber hinaus virtuelle Maschinen ausführen (Hyper-V), Updates dosieren (WSUS), Webseiten ausliefern (IIS), VPN-Dienste anbieten und vieles mehr.

Die korrekte Lizenzierung der Microsoft Server-Software ist eine Wissenschaft für sich: Für jeden Client, der sich an authentifizierte Dienste anmeldet, braucht man eine sogenannte Clientzugriffslizenz (CAL). Die ist separat zu bezahlen. Ausgewählte Zusätze, etwa der Mailserver Exchange oder die Terminal-Dienste, die das interaktive Ausführen von Anwendungen wie Office auf dem Server über eine Remote-Sitzung erlauben, erfordern darüber hinaus noch spezielle CALs.

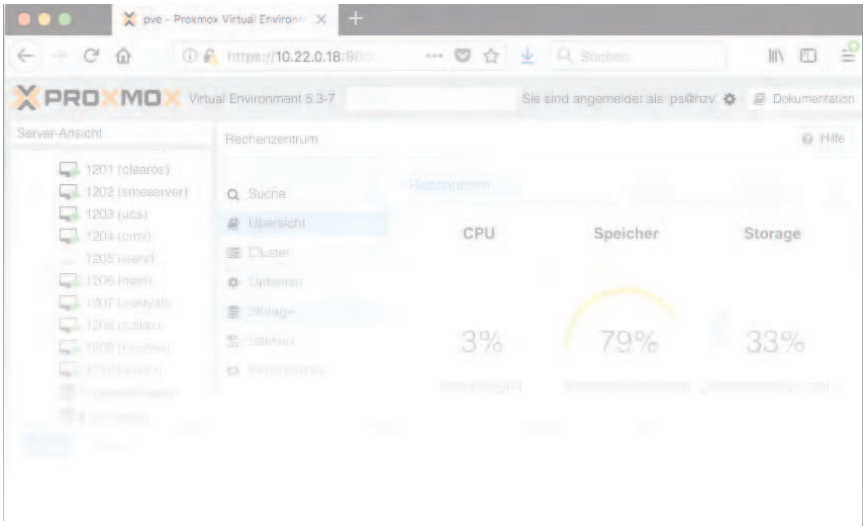
Noch kniffliger wird es bei der Virtualisierung: Serverlizenzen sind bei Microsoft an die Hardware gebunden. Das heißt, wer Software von anderen Anbietern einsetzt, um Windows-Server zu virtualisieren, braucht nicht pro VM eine Lizenz, sondern pro Server, auf der diese VMs laufen könnte. Die Standard-Ausgabe erlaubt immerhin zwei VMs, die Datencenter-Version beschränkt die Zahl der VMs nicht – wohlgemerkt auf einem Server.

Spezielle Versionen von Windows Server, die keine CALs erforderten oder ein vereinfachtes Modell erlaubten, hat Microsoft weitgehend eingestellt: Small Business, Storage, Home und Foundation Server gibt es nicht mehr. Einzig die Essentials-Ausgabe ist noch im Angebot – sie bedient ohne CALs maximal 25 Benutzer. Allerdings hat Microsoft in der 2019er-Ausgabe den letzten interessanten Extra-Dienst, das integrierte Client-Backup, entfernt.

Windows-Server haben technisch einiges zu bieten, etwa mit Hyper-V Replica die Möglichkeit, virtuelle Maschinen regelmäßig auf einen zweiten Server zu kopieren, und Optionen, um die gespeicherten Daten zu deduplizieren. Das Active Directory als zentrale Benutzerdatenbank ist in vielen Netzen unverzichtbar. Doch für kleinere Installationen, die durchaus davon profitieren würden, liegen die Lizenzeinstiegshürden sehr hoch und die Gesamtausstattung lässt zu wünschen übrig.

Was eigentlich bei allen anderen Serverbetriebssystemen selbstverständlich ist, nämlich die Verwaltung aus dem Webbrowser heraus, hält bei Microsoft erst langsam Einzug. Das Windows Admin Center (unter dem Codenamen Honolulu entwickelt) deckt längst nicht alle wichtigen Optionen ab. Viele Details einer Windows-Server-Konfiguration lassen sich nur mit spezialisierten Management-Konsolen erreichen, etwa die Gruppenrichtlinien.

NAS auf Steroiden



Drahtlose Zweigstelle

Fritzbox: Internet-Ausfälle mit Mobilfunk überbrücken

Fritzboxen können bei einem DSL-Ausfall stationäre LTE-Router, Smartphones oder LTE-Sticks als Ersatzweg zum Internet nutzen. Allerdings steht der Router selten dort, wo der Empfang gut ist. Wir haben einige Methoden ausprobiert, um das Funkzubehör mit Verlängerungen an den optimalen Standort zu bringen.

Von Dušan Živadinović

Wer eine Fritzbox braucht, die sich per LTE oder UMTS ins Internet einbucht, wenn der Bagger das Kabel getrennt hat, kann sich natürlich gleich mit dem Modell 6890 LTE wappnen: Diese Box bringt ein Mobilfunkmodem mit und lenkt den Verkehr automatisch darauf um, wenn die Hauptleitung ausfällt (Fallback). Das und die Loadbalancing-Funktion, mit der sie DSL und LTE gleichzeitig nutzt, macht sie für kleine Unternehmen attraktiv.

Im Fallback-Modus lassen sich mit den von Mobilfunkern normalerweise zugeteilten IP-Adressen Server-Dienste nicht nutzen, aber immerhin kann man darüber sämtliche ausgehenden Internet-Anwendungen verwenden (Surfen, Chatten, Streamen, Mailen etc.). Auch alle übrigen an der Fritzbox angeschlossenen Geräte haben dann Zugang zum Internet per Mobilfunk. Dafür genügt eine billige Prepaid-SIM-Karte, zum Beispiel in Kombination mit einem Tagestarif, wie ihn diverse Provider für unter fünf Euro anbieten (z. B. Telekom Data Start M für 2,95 Euro pro Tag oder AldiTalk S für 1,99 pro Tag). Festnetzrufnummern von Netzbetreibern wie der Telekom lassen sich jedoch nicht hilfsweise über Mobilfunk nutzen; die Festnetzanbieter haben das nicht vorgesehen.

Kehrt die DSL-Verbindung zurück, schaltet die 6890 LTE automatisch darauf um (Fallforward). Sehr nützlich ist der Monitor-Modus der Box. Damit hilft sie, den optimalen Standort und die beste Ausrichtung zur Basisstation zu finden. Dabei kommen ihr auch die zwei externen Mobilfunkantennen zugute.

Kein anderes Fritzbox-Modell erreicht ihre Funktionalität, aber man kann andere Modelle immerhin mit externen Mobilfunkmodems nachrüsten. Dafür kommen die Modems von stationären Mobilfunkroutern, Mobilfunksticks oder Android-Smartphones infrage. Stationäre LTE-Router koppelt man per Ethernet an die Fritzbox, Sticks und Android-Smartphones über USB. Prinzipiell eignen sich auch iOS-Geräte, aber Fritzboxen können

sie bisher nicht über USB steuern. Mit FritzOS 7.10 docken sie immerhin per WLAN an deren „Persönlichen Hotspot“ an. Dafür muss die Fritzbox ihren WLAN-Gastzugang abschalten.

Internet-Umleitung per Zweit-Router

Ein Ethernet-Segment darf für Gigabit-Ethernet je nach Konfektionierung bis 100 Meter lang sein. So lässt sich eine Fritzbox im Keller leicht mit einem LTE-Router unterm Dach verbinden. Zur Überbrückung von kurzzeitigen DSL-Ausfällen genügt schon ein älterer Mobilfunkrouter. Zum Beispiel bekommt man den Huawei B390s-2 alias Telekom Speedport LTE800 gebraucht schon ab rund 20 Euro. Wunderdinge sollte man freilich nicht erwarten – das LTE-Modem liefert maximal 50 MBit/s, die LAN-Ports maximal 100 MBit/s (Fast-Ethernet).

Neue Einstiegsmodelle gibt es für unter 100 Euro. Beispielsweise bietet der Mobilfunkprovider Ortel den von Wistron gefertigten WLD71-T1 für 70 Euro (siehe Seite 97). Dessen LTE-Modem könnte zwar bis zu 150 MBit/s liefern, aber sein Switch deckelt die Datenrate auf Fast-Ethernet. Immerhin bekommt man für 30 Euro Guthaben aktuell 60 GByte Übertragungsvolumen mit einer Laufzeit von 28 Tagen – ohne Mindestlaufzeit und Kündigungsfrist. Ähnliche Angebote haben auch die Telekom, O2 Telefónica und Vodafone in petto. Eine Fritzbox 6820, die ausschließlich ein Mobilfunkmodem an Bord hat, bekommt man ab rund 120 Euro.

Der stationäre LTE-Router Netgear LB1111 lässt sich auch über Ethernet mit Strom versorgen (PoE), sodass man am Standort nicht unbedingt eine Steckdose braucht.

Manche LTE-Router lassen sich per Power over Ethernet (PoE) mit Strom versorgen, sodass sie am Aufstellungsort ohne Stromsteckdose auskommen. Das trifft zum Beispiel auf den Netgear LB1111 zu. Er ist für PoE gemäß IEEE 802.3af ausgelegt (max. 13 W). Aber Achtung: Das Modell LB1121 bringt zwar auch PoE mit, doch sein LTE-Modem funkt nur auf LTE-Bändern in den USA. Zwar hat AVM bisher keine Fritzbox für PoE ausgelegt, aber einen LB1111 kann man mit einem PoE-Injektor wie dem TP-Link TL-POE150S oder dem Digitus DN-95102-1 speisen (gibts in der Elektronik-Grabbelkiste ab rund 16 Euro).

Für die Kopplung steckt man ein Ethernetkabel in den LAN-Port eines LTE-Routers. Das andere Kabelende führt man dem WAN-Port der Fritzbox zu. Manchen Modellen hat AVM einen festen WAN-Port spendiert, etwa den Modellen 7580 und 7590. Man schaltet ihn im Menü „Internet/Zugangsdaten/vorhandener Zugang über WAN“ ein. Bei anderen Fritzboxen muss man per Hand zwischen DSL und LAN1 umschalten.

Sind Box und Router verbunden und eingeschaltet, weist der LTE-Router der Box per DHCP eine private IP-Adresse aus seinem Subnetz zu (z. B. 192.168.5.x beim Netgear LB1111). Welche das ist, zeigt die Fritzbox auf der Startseite ihrer Weboberfläche an. Öffnen Sie dann im Browser das Webinterface des LTE-Routers (z. B. 192.168.5.1) und konfigurieren Sie ihn. Tragen Sie also, falls erforderlich, die PIN der SIM-Karte ein und bauen Sie die Mobilfunkverbindung zum Internet auf – damit ist die Internet-Umleitung per Mobilfunkrouter fertig.

Sticks and Stones

Falls es ein Mobilfunkstick sein soll: Die weitaus meisten Modelle sind nur mit dem älteren USB 2.0 bestückt, das nicht mehr als 480 MBit/s befördert. Doch auch damit haben Sie für den Mobilfunkzugang zum Internet genügend Reserven, weil deren Modems nicht über 150 MBit/s hinauskommen (LTE-Kategorie 4). Selbst die schnelleren liefern allenfalls 300 MBit/s (Kategorie 6). Ähnliches gilt für Android-Smartphones.

Mit passiven USB-2.0-Verlängerungen kommt man nur einige Meter weit. Das kann genügen, um einen Stick außer-

Stellwerk-Rohbau

Router-Betriebssysteme auf x86-Mini-PCs installieren

Für manche Vernetzer sind Fertigrouter wie die beliebten Fritzboxen ein zu enges Korsett, das sie gern gegen eine Maßanfertigung eintauschen würden. Wir zeigen, wie Sie die Router-Betriebssysteme pfSense und OpenWrt auf erschwingliche x86-Barebones bekommen.

Von Ernst Ahlers

Sie hätten gern VLANs für mehrere logische Netze, um Smart-Home- und IoT-Gadgets aus dem internen (W)LAN herauszuhalten [1]? Oder soll es ein OpenVPN statt des bei Fritzboxen integrierten IPsec-VPN sein? Dann können Ihnen Alternativen wie pfSense oder OpenWrt weiterhelfen, die Sie auf eigene Hardware pflanzen.

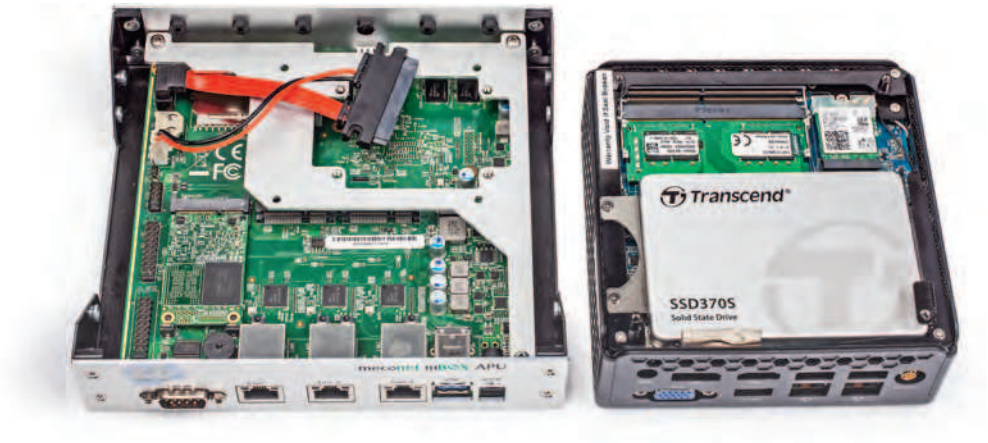
Dieser Beitrag schildert detailliert, wie man diese beiden Router-Betriebssysteme auf zwei Systemen installiert, dem für Router-Betrieb ausgelegten Mainboard APU2D4 von PC Engines – im Folgenden kurz APU – und Zotacs Zbox CI329 Nano (Zbox). Wer andere Hardware als Miniserver oder Router einsetzen will, findet ab Seite 84 Hinweise zur Auswahl.

Das APU-Board ist auf Appliance- beziehungsweise Embedded-Betrieb ausgelegt: Es hat anders als Mini-PCs keinen Bildschirmanschluss, aber als Ersatz dafür eine serielle Schnittstelle (RS-232) und gleich drei Gigabit-Ethernet-Ports. Dazu kommen zwei PCIe-MiniCard-Slots für Erweiterungen (etwa WLAN-Karten), eine mSATA-Fassung sowie Pfostenleisten für Hardware-Erweiterungen (zweite serielle Schnittstelle, GPIO, LPC). Es taugt gut für Embedded-Anwendungen, wo die Performance der im Sommer 2014 erschienenen AMD-CPU GX-412TC (1 GHz, 4 Jaguar-Kerne) ausreicht.

Falls Sie das APU2D4 als montiertes Barebone angeboten finden, spendieren Sie den Aufpreis: Er erspart Ihnen den fehlerträchtigen Gehäuseeinbau, bei dem es auf die wärmeschlüssige Positionierung des CPU-Kühlpads ankommt. Wir probierten die Installationen auf einem APU2C4-System aus. Seit Herbst 2016 bündelt es bei uns als Load Balancer mit pfSense drei Internetanschlüsse [2], stellt fast 500 MBit/s im Downstream bereit und ist bisher sehr stabil durchgelaufen. Laut dem Hersteller PC Engines entspricht das APU2C4 bis auf eine in Details verbesserte Platine dem aktuell angebotenen Modell APU2D4.

Die Zbox ist ein PC-Barebone [3]. Sie kostet zwar rund 50 Euro mehr als ein aus den Komponenten selbst zusammengesetztes APU2D4-System und hat Schnittstellen, die Router nicht brauchen, taugt so aber auch als universeller Miniserver. Der Quad-Core-Prozessor Celeron N4100 in der Zbox ist deutlich moderner als der des APU2D4. Das zeigt sich durch mehr Integer-Performance (PPPoE-NAT-Durchsatz, S. 91) und Krypto-Leistung (AES-Chiffre), was der N4100 seinem hohen Burst-Takt von 2,4 GHz verdankt.

Außerdem zog die Zbox in unseren Versuchen je nach Betriebssystem und Konfiguration etwas bis deutlich weniger stromkostentreibende Idle-Leistung. Man muss auf den dritten Ethernet-Port verzichten, kann dafür aber beliebige Betriebssysteme bequem per vorübergehend angeschlossener Peripherie (USB-Tastatur, -Maus, HDMI-Bildschirm) installieren.



x86-Grundlagen für Router: Das Embedded-System APU2D4 (links) verzichtet auf Bildschirm und Tastatur, bringt dafür aber einen dritten Ethernet-Port und Anschlüsse für weitere Peripherie mit. Die Zbox CI329 Nano ist dagegen ein vollwertiger Mini-PC, der bei Bedarf mit viel RAM auch als Virtualisierungshost dienen kann.

Für die Installation nötige Tools sowie Links zu Hinweisen für beide Router-Betriebssysteme haben wir unter ct.de/wp33 zusammengestellt. Zum Entpacken der Archive unter Windows nahmen wir 7-Zip, Images schrieben wir mit dem Win32 Disk Imager auf die Zielmedien.

Hardwarebestückung

Anders als beim APU2D4 muss man bei der Zbox noch RAM einsetzen. 4 GByte DDR4-SO-DIMM genügen für einen Router vollauf. Die Zbox verkraftet aber bis zu 16 GByte, falls Sie sie als Virtualisierungshost nutzen wollen. So ließe sich beispielsweise mit dem Debian-Linux-basierten Proxmox [4] auch pfSense als virtuelle Maschine betreiben (Link zur Anleitung unter ct.de/wp33).

Zwar kann man pfSense und OpenWrt prinzipiell auch auf ein SD-Kärtchen installieren, das Sie beim APU direkt in die Fassung auf der Platine stecken. Solche Karten vertragen aber typischerweise viel weniger Schreibvorgänge als SSDs. Wenn Sie Logging-Funktionen der Router-Betriebssysteme nutzen wollen, nehmen Sie als Betriebssystemspeicher eine SSD. Bei der Zbox ist das ohnehin die bessere Wahl, weil das Speicherkärtchen beim außen liegenden SD-Card-Slot leicht verloren gehen könnte.

Für die Routerboxen genügt notfalls eine gebrauchte SSD. Auf die Performance kommt es hier ebenso wenig an wie auf die Kapazität. 16 GByte sind für pfSense und OpenWrt weit mehr als nötig.

Bei einer SSD als Betriebssystemspeicher ist wichtig, ein Modell zu erwischen, das die Stromspartechnik SATA Link Power Management unterstützt. Moderne SSD können das in der Regel, aber es gibt Ausnahmen: Mit der mit 19 Euro superbilligen Teamgroup L7 Evo 60 GB zog die Zbox 3,7 Watt (Xubuntu 18.04.1 LTS, ohne USB-Peripherie und Bildschirm bei einem aktiven Ethernet-Port).

Die gerade mal 3 Euro teurere Transcend SSD370S 32GB senkte die Idle-Leistung der Zbox um ein Viertel auf 2,8 Watt. Bei 30 Cent/kWh Stromkosten und Dauerbetrieb hat man den kleinen Aufpreis binnen 1¼ Jahren eingespielt. Zwar ist die SSD370S mit 217 MByte/s Lese- und 42 MByte/s Schreibleistung nach heutigen Maßstäben krötenlahm. Als Speicher für Betriebssystem und Logging-Daten genügt das aber allemal, ebenso wie die 362/37 MByte/s der L7 Evo.

Massenspeicherfeinheiten

pfSense lässt sich auf beiden Systemen vom USB-Stick installieren. Als Ziel ist beim APU2D4 eine mSATA-SSD die geschicktere Wahl, weil sie sich ohne Adapter-Käbelchen und mechanische Montage einfach in die mSATA-Fassung des Boards einsetzen lässt. Mit dem von uns gewählten Transcend-Modell MSA370 klappte die Installation problemlos. Bei 2,5-Zoll-SSDs am SATA-Port zeigte sich das APU hingegen wählerisch: Die Transcend SSD370S erkannte es zwar, aber bei der Installation von pfsense hagelte es dann AHCI/CAM-Fehler. Das blieb bei der Teamgroup L7 Evo aus.

OpenWrt für x86-Rechner muss man direkt auf das Zielmedium schreiben, Details dazu folgen weiter unten. Dafür ist bei SATA-SSDs ein preiswerter USB-zu-SATA-Adapter nötig, den viele PC-Schrauber schon in der Schublade haben dürften. Für mSATA-SSDs wird ein zusätzlicher mSATA-zu-SATA-Adapter fällig. Falls Sie den – oder ein ungenutztes USB-Gehäuse für mSATA-SSDs – nicht zur Hand haben, greifen Sie einfacherweise zu einer SATA-SSD. Indes mochte auch OpenWrt mit der SSD370S im APU2D4 nicht laufen: Der Bootloader Grub beschwerte sich beim Start des Systems über Lesefehler.

Tuninggrenzen

Welche zusätzliche Energieersparnis das Entfernen des WLAN-Moduls aus der Zbox bringt, war nicht messbar: War das WLAN unkonfiguriert, lief also weder als Client noch als Access Point, dann zog der Mini-PC laut unserem Präzisionsleistungsmessgerät LMG95 mit dem mitgelieferten Netzteil genauso viel Leistung, wie wenn das Modul ausgebaut war.

Falls es überhaupt eine Einsparung gab, dann lag sie innerhalb der Fehlergrenze des Messgeräts: Es zeigt zwar weit mehr Stellen an, kann aber ohne zusätzliche Hilfsmittel (externer Shunt) bei diesem Leistungsniveau (2,8 Watt) am Stromnetz „nur“ auf rund 0,04 Watt genau messen. Damit liegt die mögliche Einsparung in der gleichen Größenordnung. Für die paar Milliwatt müssen Sie den Schraubendreher definitiv nicht bemühen.

BIOS-Schrauben

Im APU2D4 steckt Coreboot als BIOS. Es ist ab Werk so eingestellt, dass das System von allen möglichen Massenspeichern startet. Weitere relevante Einstellungen gibt es nicht, Sie können es auf den Vor-

Marke Eigenbau

Acht Webhosting-Pakete für dynamische Inhalte im Test

Nie war es so leicht und preisgünstig wie heute, eine eigene Website aufzusetzen. Rundum-sorglos-Pakete der Webhoster nehmen mit Fertig-Installationen die meiste Arbeit ab – inklusive eigener Domain. Unser Test vergleicht acht Angebote für unter 100 Euro pro Jahr.

Von Holger Bleich

Viele Privatpersonen, Vereinsvorsitzende oder Firmenbosse verlernen, wie wertvoll eine eigene Website sein kann – leider. Ist der Auftritt nämlich gut gemacht, dient er nicht nur der Selbstdarstellung, sondern auch als direkter Draht zu Freunden, Mitgliedern oder Kunden. Wer einmal in einem gut moderierten Webforum diskutiert hat, dem macht Getrolle auf Facebook noch viel weniger Spaß. Zudem ist es unnötig, sich einer proprietären Plattform auszuliefern und freiwillig deren Design-Korsett zu nutzen. Facebook kann Seiten auf der Plattform einfach den Boden unter den Füßen wegziehen – seien Sie lieber Herr im eigenen Haus.

Nach Umfragen des statistischen Bundesamts halten rund 30 Prozent von deutschen Kleinunternehmen dennoch die eigene Website für zu teuer oder zu aufwendig. Sie sollten sich die Rundum-sorglos-Pakete der deutschen Webhoster anschauen. Wer nicht selbst basteln will, findet hier Design-Baukästen und Ein-Klick-Installationen populärer Software wie Wordpress oder Typo3 vor.

Die Preise für Hosting-Pakete mit E-Mail und modernen Webanwendungen purzelten in jüngerer Zeit wieder. Für diesen Test haben wir uns angesehen, was Sie erwartet, wenn Sie weniger als 100 Euro pro Jahr in den Webauftritt stecken wollen. Bei der Sondierung des Marktes orientierten wir uns an unseren vergangenen Tests [1], um eine gewisse Vergleichbarkeit herzustellen.

Kandidatenkür

Maximal 8 Euro monatlich durfte ein Gesamtpaket kosten, plus einmalige Bereitstellungskosten, die manche Hoster gerade bei Verträgen mit geringer Laufzeit erheben. Dennoch sollte das Paket mindestens 50 GByte Webspace, PHP-Ausführung und Datenbanken bieten. Diese Kombination benötigen fast alle Anwendungen, die dynamisch Seiten zusammenbauen.

Wichtig war uns außerdem, dass im Paket die Möglichkeit besteht, Webseiten ohne Aufpreis SSL-verschlüsselt (HTTPS) zu den Browsern zu bringen. Alles andere ist nicht mehr zeitgemäß, zumal aktuelle Browser dazu übergehen, unverschlüsselte Übertragungen prominent als unsicher und damit schlecht zu markieren. Ein SSL-Zertifikat und dessen Bindung an die Domain war für unseren Test also Pflicht.

Bei Strato und 1&1 – inzwischen „1&1 Ionos“ – wurden wir gerade eben noch fündig: Beide Hoster, die Schwesterfirmen unter dem Konzerndach United Internet sind, verlangen für in Frage kommende Pakete just genau 8 Euro monatlich. Knapp darunter liegt All-Inkl. Goneo und Host Europe kamen immerhin schon unter 7 Euro. Ein Neuling im Test ist der französische Cloud-Konzern OVH, der hierzulande massiv die Werbetrommel für seine deutsche Niederlassung rührt. 1blu und Hetzner sind die Billigheimer im Test: Ihre Pakete kosten sogar weniger als 5 Euro pro Monat. Es sei vorweggenommen: Eine Korrelation zwischen den Preisen und der gebotenen Leistung konnten wir nicht feststellen.

Grundfunktionen und sonstige Leistungsmerkmale haben wir für Sie in der Tabelle ab Seite 110 zusammengefasst. Gerade an der Grundausstattung zeigt sich, ob die Hoster auf der Höhe der Zeit agieren. Wir halten es für wichtig, dass die Webserver – in aller Regel Apache-Versionen unter Linux – moderne Übertragungsarten unterstützen. Also sollte nicht nur HTTP 1.1 möglich sein, sondern auch das neuere, effizientere HTTP/2. Außerdem ist es sinnvoll, wenn der Webserver vor der Übertragung Daten (insbesondere Texte, Skripte etc.) komprimiert, um Leitungskapazität und Zeit zu sparen.

HTTP/2 und gzip sorgen dafür, dass Inhalte rascher zum Nutzer kommen, sich Seiten schneller aufbauen. Anders gesagt: Sie sorgen für zufriedenere Besucher; und übrigens auch für ein zufriedeneres Google. Ein erfolgreiches Ranking in der Suchmaschine hängt wesentlich davon ab, wie schnell die Website ausgeliefert wird. Google gibt sogar selbst wertvolle Einblicke. Unter developers.google.com/speed/pagespeed/insights/ kann man jede beliebige URL checken lassen. Da moniert Google dann etwa, wenn die Serverkomprimierung abgeschaltet ist.

E-Mail und Grundschutz

Ein wichtiger Bestandteil der Rundum-sorglos-Pakete ist der E-Mail-Service: Die Webhoster binden die Adressen und Postfächer an die mit dem Paket registrierten Domains, sodass man als Privatperson oder Firma unter dieser Domain erreichbar ist. Mindestens 100 Mail-Adressen lassen sich bei den Testkandidaten vom Admin verwalten, das reicht schon für alle Mitarbeiter kleinerer Unternehmen.

Allerdings sind diese Services verschieden ausgestaltet. Das beginnt bei der Postfachgröße, geht über Sicherheitsmerkmale und endet noch lange nicht bei der Qualität von eingesetzten Webmailern. Ab Seite 112 haben wir diesem Thema deshalb einen eigenen Artikel gewidmet und klären darin, wie praktikabel die E-Mail-Funktionen der getesteten

Tupfer und Skalpell

Was Wireshark 3 ausmacht, warum man es haben will

Das wohl am meisten verwendete Netzwerkanalyse-Tool überhaupt ist Wireshark. Inzwischen ist die quelloffene Software in Version 3.0.2 erhältlich. Wir erklären die wichtigsten Neuerungen, die der Umstieg auf Npcap bringt und anderes mehr.

Jasper Bongertz

Die Software-Suite Wireshark, die Gerald Combs bereits 1998 zunächst unter dem Namen Ethereal aus der Taufe hob, eröffnet Einblicke in die Netzwerkkommunikation zahlreicher Protokolle „auf der mikroskopischen Ebene“. Zwar gibt es ähnlich leistungsfähige Produkte, etwa den Message Analyzer von Microsoft, aber Wireshark ist quelloffen und nicht nur für Windows, sondern auch für Linux und macOS erhältlich.

Das gelingt unter anderem deshalb, weil die Entwickler die grafische Benutzeroberfläche mittels plattformübergreifender Toolkits weitgehend gemäß den Styleguides der jeweiligen Zielplattform implementieren – anfangs haben sie dafür GTK verwendet, seit Version 2 aber Qt. Der Wechsel brachte einen moderneren Look. Auch erwies sich die Qt-Community als agiler, sodass GUI-Probleme schneller gelöst wurden.

Jedoch ist der Umstieg noch nicht abgeschlossen; einige Funktionen sind bisher nur in GTK implementiert. Deshalb installierten manche User beide, das GTK-basierte „Wireshark Legacy“ und die Qt-Version parallel. Seit der Version 3.0 ist aber nur noch die Qt-Variante zu haben. Die Entwickler wollen die Lücken bald schließen. Zum Beispiel gibt es die Wireless-Toolbar für die Kanalauswahl noch nicht in der Qt-Version.

Unter der Haube haben sich viele Änderungen ergeben, die Teil der stetigen Modernisierung sind. Am wichtigsten ist wohl der Wechsel von WinPCAP zu Npcap, dem wohl auch der Inkrement der Hauptversionsnummer geschuldet ist: WinPCAP ist eine Library, die Wireshark unter Windows zum Aufzeichnen des Netzwerkverkehrs benötigte – das Linux-Gegenstück dazu heißt libpcap.

Von WinPCAP zu Npcap

Allerdings haben sich die Entwickler vor Jahren anderen Projekten zugewendet, sodass WinPCAP nicht mehr alle Anforderungen erfüllt. Zum Beispiel ändert Microsoft die Interfaces der Windows-Netzwerktreiber laufend (Network Driver Interfaces Specifications, NDIS), sodass WinPCAP schon auf den ersten Windows-10-Versionen Schwierigkeiten bereitete. Außerdem lässt sich mit WinPCAP weder der WLAN- noch der Loopback-Verkehr aufzeichnen. Eine Zeit lang konnte man für WLAN-Aufzeichnungen auf AirPCAP-Adapter ausweichen, aber inzwischen hat der Hersteller den Vertrieb eingestellt.

Um solche Probleme zu beseitigen, haben Teilnehmer des Nmap-Projekts von Gordon Lyon, besser bekannt als Fyodor, eine neue Bibliothek entwickelt: Npcap für Windows. Denn WinPCAP verwendeten neben Wireshark auch viele andere Projekte – und eben auch Nmap – um mit der Netzwerkkarte zu kommunizieren. Npcap liegt seit April 2018 als Kernelmodul vor. Nach einer Erprobungsphase setzt Wireshark nun standardmäßig darauf.

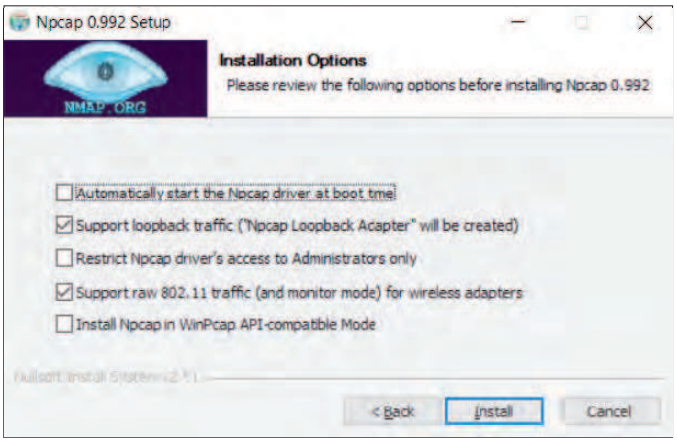
Einige Problemchen, die auf Npcap zurückgehen, sind noch übrig. Wenn der Npcap-Dienst läuft, sieht der Windows-eigene WLAN-Lister manchmal einige WLANs nicht. Stoppt man Npcap, tauchen diese wieder auf (z. B. in der Windows-Taskleiste). Ob das auch auf Ihrem PC der Fall ist, können Sie in einer privilegierten Kommandozeile mit den Befehlen `sc stop npcap` und `sc start npcap` prüfen.

Abgesehen davon lohnt sich Npcap aber. Damit sind endlich Captures der Loopback-Interfaces möglich und man kann die WLAN-Funkschicht (Media Access Control) ohne Spezial-Hardware aufzeichnen (Monitor Modus). Eine Liste geeigneter Adapter finden Sie über ct.de/w7vx.

Um den Monitor-Modus auf Windows nutzen zu können, müsste man Wireshark eigentlich mit administrativen Rechten starten. Aus Sicherheitsgründen ist das aber keine gute Idee. Abhilfe schafft das Kommandozeilen-Tool `WlanHelper.exe`, das im Verzeichnis `C:\Windows\System32\npcap`

liegt. Damit lässt sich der Monitor-Modus der WLAN-Karten per Hand aktivieren, sodass sie Radioschicht-Informationen liefert und selbst nicht mehr aktiv am WLAN teilnimmt (Receive-Only).

Den Funkkanal kann man in Wireshark mangels entsprechender Toolbar ebenfalls noch nicht einstellen. Auch dafür braucht man den WlanHelper. Wie man ein WLAN-Capture mit Npcap erzeugt, beschreibt der Autor dieses Beitrags ausführlich in einem englischsprachigen Blog-Eintrag (siehe ct.de/w7vx).



Mit der neuen Bibliothek Npcap kann Wireshark endlich den Verkehr von Loopback-Interfaces und WLAN-Adaptern mitschneiden.

Politur und Umbau

Daneben haben die Entwickler die Struktur und Terminologie von Wireshark in einigen Details aktualisiert. Beispielsweise haben viele Anwender das Fehlen eines DHCP-Display-Filters kritisiert. Stattdessen musste man die Funktion unter dem Stichwort „bootp“ suchen, obwohl DHCP das Bootstrap Protocol längst abgelöst hat. Wireshark 3 trägt dem nun endlich Rechnung und bringt den Filter „dhcp“ mit.

Gleiches gilt für „ssl“, das durch „tls“ ersetzt ist. Beide alten Filter – sowohl bootp als auch ssl – kann man aber noch verwenden; die Filtereingabezeile färbt sich dann zur Warnung gelb, weil beide in einer künftigen Version verschwinden werden.

Traditionell verändern sich mit jeder Wireshark-Version auch viele der Protokoll-Dissectoren, die unter Anderem die Bits und Bytes der Pakete in lesbare Information verwandeln. Zum Beispiel lässt sich jetzt das moderne VPN-Protokoll WireGuard entschlüsseln, wenn man Wireshark die passenden Schlüssel gibt. Dazu muss man die Einstellungen öffnen und im Bereich Protokolle/Wireguard die Keys eintragen.

Und wer Wireshark nur gelegentlich nutzt, wird schätzen, dass man nun Filter einfach per Drag & Drop erzeugen kann, indem man Elemente aus dem Decode-Bereich auf die Filtereingabezeile zieht – etwa, um schnell und ohne Tippen den Verkehr eines bestimmten TCP-Ports zu filtern.

Ein weiteres, leider gut verstecktes neues Feature ist die Möglichkeit, die Kryptoschlüssel für TLS-Verbindungen in Pcapng-Dateien zusammen mit den verschlüsselten Paketen zu speichern. Das erleichtert den gemeinsamen Versand etwa zu einem externen Analysedienstleister. Andernfalls müsste man nicht nur die Pcapng-Datei, sondern auch sslkeylog.log verschicken.

Dazu haben die Entwickler das Pcapng-Dateiformat um einen Blocktyp erweitert, in den man die Schlüsselinformationen von Firefox oder Chrome ablegen kann; in beiden Browsern definiert man eine Ausgabedatei über die Umgebungsvariable SSLKEYLOGFILE.

Zum Ablegen nutzt man das mitgelieferte Utility `editcap`. Sinnvollerweise kann man Schlüsseldaten mit editcap auch entfernen. Das Tool ist auch deshalb praktisch, weil es sich skripten lässt. So kann man batchmässig große Mengen von Dateien bearbeiten, während Wireshark immer nur eine Datei offen halten kann. Überhaupt ist editcap das „Schweizer Taschenmesser“ für die Manipulation von Netzwerkpaketdateien. Bei Bedarf kann man damit Pcapng-Dateien sauber auseinanderschneiden oder ungewollte Duplikate entfernen, die durch bestimmte Messtechniken entstehen.

Mal was anderes: ExtCap

Schon seit einer Weile kann Wireshark über optionale ExtCap-Schnittstellen externe Datenquellen für Aufzeichnungen anzapfen.

Zum Beispiel lassen sich damit Dongles von NordicSemi für die Aufzeichnung des Bluetooth-LE-Verkehrs verwenden. Dabei reicht ein Kommandozeilen-Tool Bluetooth-LE-Pakete per Pipe an Wireshark weiter. Aktuell ist die Einrichtung des Pipe-Tools aber noch mit reichlich Fummelei verbunden.

Eigentlich sehr praktisch ist auch die Möglichkeit, per SSHDump einen Mitschnitt auf einem entfernten Rechner zu starten (z. B. mit tcpdump) und die Pakete über SSH in Wireshark einzulesen – ohne selbst die Kommandozeile zu bemühen. Beim ersten Versuch des Autors klappte