IT-ADMINISTRATOR.DE

12/2009

€ 12,60 ISSN 1614-2888

iadministrator

Das Magazin für professionelle System- und Netzwerkadministration

Mobiles Arbeiten, Home Office und Wireless

4 119583 212605 12

Cybercrime

Daniels Netzwerk ist geschützt. Ihres auch?

Wir halten Ihre Systeme am Laufen!

Mit der neuen Management-Konsole können Sie jetzt noch effizienter arbeiten.

Daniel muss sich um vieles kümmern. Er sorgt für die Verfügbarkeit des Systems und ein robustes Netzwerk. Außerdem löst er die technischen Probleme seiner Kollegen.

Wegen Cybercrime macht er sich keine Sorgen. Wie 250 Millionen Menschen weltweit verlässt er sich auf Kaspersky Lab, wenn es um den zuverlässigen Schutz vor Trojanern, Phishing-Mails, Hackerangriffen und Spam geht.

Überprüfen Sie jetzt, ob auch Ihr Unternehmen richtig geschützt ist. Überzeugen Sie sich davon, wie Kaspersky Lab Ihren Berufsalltag mit innovativen Administrationsfunktionen erleichtert. Jetzt auch für Windows 7!

www.stop-cybercrime.de

Certified for Windows Server 2008 · Compatible with Windows 7 · CITRIX ready

KASPERSKY lab

www.kaspersky.de

EDITORIAL

Aufwärts, 2010!

Liebe Leser,

eines war dieses Jahr bestimmt nicht: langweilig. Kaum eine Branche, die nicht in irgendeiner Form von der Krise betroffen war. IT-Investitionen wurden zurückgestellt und die Hersteller litten unter rapide gesunkenen Umsätzen. Für 2010 sehen die Prognosen immerhin etwas freundlicher aus. Da passte denn auch die Meldung des Branchenverbands BITKOM gut ins Bild, der im November noch 20.000 offene IT-Stellen vermeldete. Spezialisten sind nach wie vor gefragt. Eine gute Nachricht.

Ein Lichtblick tat sich auch für Microsoft auf. Das neue und heiß ersehnte Windows 7 wurde dem Softwareriesen förmlich aus den Händen gerissen. Damit schaffte es Microsoft, viele Vista-Verweigerer hinter dem Ofen hervorzulocken und vom schlankeren Nachfolger zu überzeugen. Der spielt besonders mit dem ebenfalls neuen Windows Server 2008 R2 seine Stärken im Netzwerk aus und wirkt insgesamt ausgereifter – nicht zuletzt, da er technisch auf Vista basiert. Welche Neuerungen Windows 7 für Sie und Ihre User mitbringt, erfahren Sie ab Seite 35.

Einen Ansturm ganz anderer Art verzeichnen nach wie vor die Ärzte, Schweinegrippe sei dank. Auch Unternehmen entwickeln eifrig Notfallpläne, um trotz bettlägriger Mitarbeiter weiter zu funktionieren. Ein längst vertrautes Konzept dabei ist das Arbeiten von zu Hause aus – nicht erst seit H1N1. Immer mehr Mitarbeiter sehen sich gar als regelrechte "Road Warrior" und kennen ihre Unternehmenszentrale nur noch vom Hörensagen. Für Sie als Administrator bedeutet das, unzählige mobile Geräte über Netzwerkgrenzen hinweg zu verwalten. Geräte, die in freier Wildbahn ein gefundenes Fressen für Malware und Hacker darstellen. Immerhin können Ihre Remote-Rechner dank freeSSHd kostenfrei sicheren Kontakt zum Unternehmensnetz aufnehmen. Wie, das verraten wir ab Seite 29.

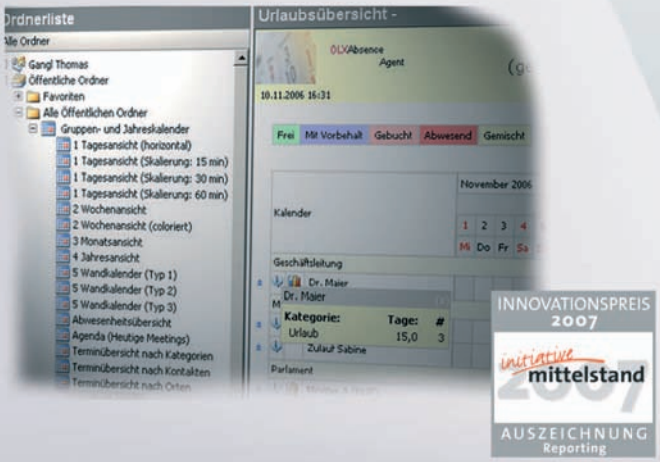
Zu guter Letzt freute sich IT-Administrator im Herbst über sein 5-jähriges Bestehen und zahlreiche treue Leser. Das stete positive Feedback zeigt uns, dass wir auf dem richtigen Weg sind, während kritische Anmerkungen hier und da immer wieder zum Nachdenken anregen. Vielen Dank. Für die kommenden Wochen wünschen wir Ihnen ein frohes Weihnachtsfest und einen guten Start ins neue Jahr. Wir freuen uns auf ein spannendes 2010 mit Ihnen!

Ihr

Daniel Richey
Redakteur IT-Administrator

Wer liefert Ihnen das fehlende Puzzleteil zu Outlook© und Exchange©?

Gruppenkalender
Terminmanagement



INNOVATIONSPREIS 2007
initiative mittelstand
AUSZEICHNUNG
Reporting

Mobiler Zugriff
auch für Öffentliche Ordner

INNOVATIONSPREIS 2007
initiative mittelstand
AUSZEICHNUNG
Mobile Business

Unternehmensweite
Signaturen & Disclaimer

Individualentwicklung
Vertrauen in Erfahrung

www.gangl.de

Ihr Partner für praxisorientierte Outlook© und Exchange© Lösungen!

Ihre Ansprüche sind unser Ansporn!

info@gangl.de ☎+49 7173 9290 53

INHALT

IT-Administrator – Ausgabe Dezember 2009

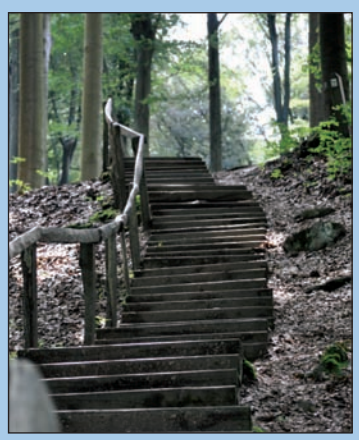
Mobiles Arbeiten, Home Office und Wireless

Im Test: Fujitsu Scaleo Home Server 2205

Mit dem Scaleo Home Server 2205 hat Fujitsu Technology Solutions ein NAS-System mit Windows als Betriebssystem im Angebot. IT-Administrator hat das Gerät im Hinblick auf den Einsatz im Home Office getestet. Dabei konnte der NAS-Speicher seine Vorzüge unter Beweis stellen.

Seite 18

Benutzerverwaltung unter Linux und Windows (2)



Der erste Teil dieser Workshopserie befasste sich damit, Linux-Benutzer mit Hilfe von Winbind an einem zentralen Windows-Domänenkontroller zu authentifizieren. Nun wenden wir uns dem umgekehrten Weg zu, indem wir Windows-Benutzer an einem Linux-Server anmelden und so auf die gewohnte Umgebung zugreifen lassen. Dazu verwenden wir das Samba-Programmpaket und OpenLDAP.

Seite 51

Themenübersicht

- Server- und Systemmanagement
- Clientmanagement
- Storage
- Sicherheit
- Messaging
- Virtualisierung
- Netzwerkmanagement
- Job/Weiterbildung
- Recht

Die Appliance "NA 820" von ICO richtet sich an Sicherheitsanwendungen in Unternehmen

Neues Zuhause für Sicherheitsapplikationen

Mit der **NA 820** bietet **ICO Innovative Computer** kleinen und mittelständischen Unternehmen eine Hardware-Plattform für Anwendungen rund um die Netzwerksicherheit. Die Appliance eignet sich laut Hersteller für den Einsatz als **Firewall**, **VPN-Lösung** oder für andere Sicherheitsapplikationen im Netzwerk. Auch **Unified Thread Management** (UTM)-Applikationen, die verschiedene Sicherheitsapplikationen auf einer Plattform vereinen, sollen für das leistungsstarke System kein Problem darstellen. Ausgestattet ist der 19-Zoll-Server mit einem Intel Core 2 Duo-Prozessor E7500 mit 2,93 GHz und 2 GByte DDR2 Arbeitsspeicher. Für das Betriebssystem (Linux Redhat, FreeBSD) und zum Speichern etwa von Event-Logs steht eine 2,5-Zoll-SATA-Festplatte mit 160 GByte Kapazität zur Verfügung. Zusätzlich ist ein CompactFlash-Slot vorhanden. Auf der Front des Gehäuses mit einer Höheneinheit befinden sich neben einem kleinen Display auch die insgesamt sieben GBit-LAN-Ports sowie zwei USB 2.0-Ports und eine serielle (RS232) Schnittstelle. Um bei System- oder Stromausfällen bestehende LAN-Verbindungen aufrecht zu erhalten, sind vier der sieben LAN-Ports mit Bypass-Funktion ausgestattet. Eine Mini-PCI sowie eine PCI-Schnittstelle runden die Ausstattung des NA 820 ab. Die Network Appliance Plattform NA 820 ist für 649 Euro erhältlich. *(dr)*

ICO: www.ico.de

Schutz mit und ohne Cloud

McAfee erweitert seine **E-Mail-Sicherheitslösung** um einen Online-Service. In Zukunft sollen Kunden wählen können, ob sie eine Hardware-Software-Kombination (Appliance) installieren, die Lösung als Software as a Service (SaaS) beziehen oder eine Mischform aus beidem einsetzen. Nutzer, die das SaaS-Modell wählen, sollen die Möglichkeit erhalten, Filterregeln für eingehende und ausgehende Nachrichten über eine Web-Benutzerschnittstelle zu definieren. **McAfee SaaS Email Protection** schützt dann vor Viren und Würmern, wehrt Spam ab, stellt verdächtige Nachrichten unter Quarantäne und verhindert den Versand von Mails mit vertraulichem Inhalt. Auch das **McAfee Email Gateway** soll die konzernweite Kommunikationsfähigkeit per E-Mail durch Schutzmechanismen aufrechterhalten. Die Appliance weist hierfür schädliche Nachrichten ab und verhindert, dass potenziell vertrauliche Mails nach draußen gelangen. Die zu Redaktionsschluss kurz vor der Veröffentlichung stehende Softwareversion **McAfee Email Gateway 6.7.2** bietet zudem erweiterte Funktionen zur Verschlüsselung im Push- und Pull-Verfahren und ermöglicht ein einheitliches Reporting dank Unterstützung für die Security-Management-Konsole McAfee ePolicy Orchestrator. Die Geräte sind ab sofort verfügbar und kosten ab 1.995 US-Dollar. Version 6.7.2 der Software soll bis Jahresende 2009 veröffentlicht werden und dann ab 21.840 Dollar für 1.000 Benutzer kosten – zuzüglich Gerätekosten. *(dr)*

McAfee: www.mcafee.com

Band-Backup für den Einstiegsbereich

Overland Storage bringt mit der **NEOs-Reihe** automatisierte **Tape Libraries** heraus, die auf die Anforderungen von KMUs und verteilten Umgebungen zugeschnitten sind. Die Einstiegs-Serie umfasst die Modelle NEO 200s und 400s. Die NEO 200s ist ein kompaktes 2U-Modell mit bis zu 38,4 TByte Kapazität. Die NEO 400s mit 4U-Bauhöhe kann schrittweise auf 76,8 TByte erweitert werden. NEOs Libraries nutzen HP LTO3- und LTO4-Bandlaufwerke, die sich laut Hersteller leicht ersetzen lassen und außerdem upgradefähig sind. Herausnehmbare Kassettenmagazine sollen den Datenzugriff beschleunigen und die Kosten der Medienhandhabung senken. Ein integrierter Barcode-Leser dient zur Nachverfolgung von Medien. Ferner verfügen die Geräte über frei konfigurierbare Mail-Slots, um schnell auf einzelne Kassetten zugreifen zu können. Die Backup-Hardware lässt sich über SCSI, Fibre Channel oder SAS anschließen. Darüber hinaus bietet Modell 400s eine redundante Stromversorgung. Im ersten Quartal 2010 will Overland zudem weitere Optionen für Erweiterbarkeit und Verschlüsselung der NEO 400s herausbringen. Die Tape Libraries sind ab sofort zu Preisen ab 2.700 Euro erhältlich. *(ln)*

Overland Storage: www.overlandstorage.com/german/

Mit den Geräten der "NEOs"-Serie bietet Overland Unternehmen aus dem KMU-Bereich bis zu 76 TByte Bandspeicher

Katastrophenschutz

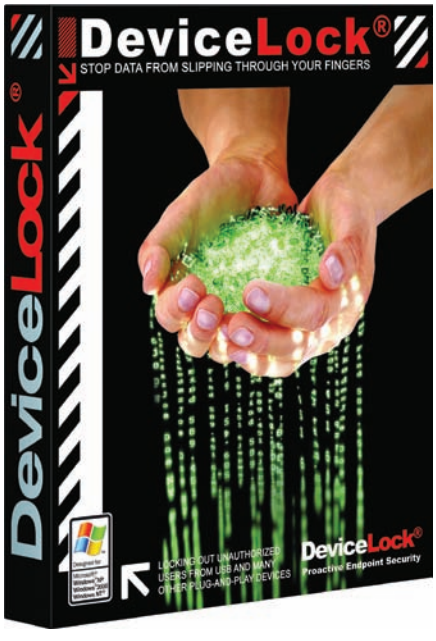
Double-Take ergänzt seine **Workload Optimization Suite** um **Double-Take Backup** und **Double-Take Availability**. Double-Take Availability 5.2 bietet Monitoring-Möglichkeiten auf Anwendungsebene sowie einen verbesserten **Schutz von Microsoft-SQL-Umgebungen**. Daneben kann die Software verfolgen, welche Daten verändert wurden, als die Replikation gestoppt war und die Re-Synchronisierung daher erheblich beschleunigen. An virtuellen Umgebungen unterstützt das Tool dabei VMware ESX v4 und Microsoft Windows Server 2008 mit Hyper-V R2. Die Agenten-Komponente Double-Take Backup 5.2 soll daneben kontinuierlich den gesamten Server (Betriebssystem, Anwendungen und Daten) schützen, Backup-Fenster eliminieren und die gesicherten Daten über WAN-Verbindungen an die Zentrale schicken. Die Lösung kombiniert hierfür Snapshot-Technologien mit CDP-Funktionen (Continuous Data Protection) und ermöglicht so eine Wiederherstellung zu beliebigen Zeitpunkten. So können Administratoren sowohl einzelne E-Mails wie auch ganze Workloads, bestehend aus Betriebssystem, Applikationen und Daten, wiederherstellen. Das Restore kann dabei auf den gleichen Server, neue physische Hardware oder auf eine virtuelle Maschine unter VMware ESX oder Microsoft Hyper-V erfolgen. Ab sofort sind die beiden Tools erhältlich, die Double-Take Availability Standard Edition kostet 3.295 Euro, der Double-Take Backup Agent 995 Euro. *(dr)*

Double-Take: www.doubletake.de

Datenschutz bei Smartphone-Nutzung

DeviceLock erweitert mit **Version 6.4.1** des gleichnamigen Tools den Funktionsumfang der **Data-Leakage-Prevention-Lösung**. Die Software ermöglicht es, den Zugriff auf lokale Ports und tragbare Geräte wie USB, FireWire, LPT, COM, IrDA, DVD/CD-ROM, Bluetooth und Wi-Fi an Firmen-PCs zu kontrollieren sowie bei Bedarf Logs und Schattenkopien der übertragenen Daten anzulegen. Die neue Version unterstützt nun auch Windows 7. Außerdem bietet das Tool Sicherheitsverantwortlichen nun die Möglichkeit zur vollständigen Kontrolle der Synchronisation von iPhone und iPod mit dem PC. Eine Basiskontrolle von BlackBerry-Geräten hat der Hersteller ebenfalls integriert. Diese umfasst die Erkennung der Endgeräte, ein Event-Logging und die Zugriffskontrolle, bei der generell festgelegt werden kann, ob ein Nutzer Daten synchronisieren darf oder nicht. Zum besseren Schutz von Daten auf mobilen Geräten ist DeviceLock zudem mit der Verschlüsselungssoftware DriveCrypt von SecurStar kombinierbar. Damit soll sichergestellt werden, dass auf tragbaren Geräten gespeicherte Unternehmensdaten bei Bedarf verschlüsselt sind. Administratoren haben in Version 6.4.1 außerdem die Möglichkeit, eine Volltextsuche in den Log- und Schattenkopie-Datenbanken von DeviceLock durchzuführen. Ab sofort ist der erweiterte Datenschützer erhältlich. Bei 25-49 Lizenzen kostet die Software 20 Euro pro Rechner. *(dr)*

DeviceLock: www.devicelock.de



DeviceLock 6.4.1 schützt vor Datenverlusten auch durch iPhone und iPod

+++TICKER+++TICKER+++TICKER+++

Fortinet präsentiert die Security-Appliance **FortiGate-1240B.** Das Gerät setzt 40 GBit/s-Firewall- und 16 GBit/s-IPSec-VPN-Traffic durch. Dabei bietet der Hersteller mit FortiOS 4.0 MR1 ein Update seines FortiOS 4.0 Betriebssystems an. Die neue Version verfügt unter anderem über ein zusätzliches Antivirus-Scanning und URL-Filtering für IPv6 Verkehr, Log-Daten-Optimierung und verbesserte Data Loss Prevention (DLP)-Möglichkeiten. Sowohl die Appliance als auch die neue OS-Version sind ab sofort erhältlich. Der Preis für die Appliance beträgt ab 23.500 Euro. *(dr)*

www.fortinet.com/products/fortigate/1240B.html

SMC Networks bietet mit dem **SMC6152PL2 TigerSwitch 10/100** einen Managed Switch mit 48 Power-over-Ethernet-fähigen 10/100-Ports an. Das Modell unterstützt dabei IP-Clustering mit bis zu 32 Switches und verfügt über vier zusätzliche GBit-Ports. Eine Quality of Service-Unterstützung soll zudem für eine zeitgerechte Auslieferung von kritischen Datenpaketen sorgen. Für 1.200 Euro ist der Switch erhältlich. *(dr)*

www.smc.com

IGEL Technology erweitert seine Universal Desktop-Serie mit Microsoft Windows Embedded Standard (WES) um einen Zugriff auf den **Connection Broker** von Leostream. Damit lassen sich virtuelle Windows-Desktops, die im zentralen Datencenter gehostet werden, generieren, verwalten und einem festen User oder Endgerät zuweisen. Bestehende IGEL-Kunden können das Firmware-Update kostenfrei auf der Herstellerseite herunterladen. *(dr)*

www.igel.com

Ab sofort ist die Zwei-Faktor-Authentifizierungslösung **SMS Passcode** in Deutschland verfügbar. Dabei erhalten die Nutzer nach der Anmeldung mit ihrem herkömmlichen Kennwort einen Code auf ihr Mobiltelefon, den sie zusätzlich beim Login verwenden müssen. Die Lösung unterstützt unter anderem Windows Logon und Terminal Services, Citrix Web Interface, Citrix Access Gateway Advanced Edition, RADIUS sowie VPN und SSL-VPN, etwa von Cisco oder Checkpoint. Über Prosoft ist die Lösung mit 50 Lizenzen für 4.250 Euro erhältlich. *(dr)*

www.prosoft.de/produkte/sms-passcode/

CONCEPT International erweitert die Serie der **miniPCs** um das Modell 323. Mit einem Intel Core 2 Duo-Prozessor und dem Grafikchip GM45 soll sich der lüfterlose Rechner etwa für Mess- und Videoanwendungen sowie als Visualisierungs-PC oder wartungsfreier Mini-Server in Industrieumgebungen eignen. Anstatt einer Festplatte verfügt der Windows XP-Rechner in den Maßen 5 x 14 x 16,5 cm dabei über bis zu 16 GByte Flash-Speicher. Für 875 Euro ist der Mini-Rechner zu haben. *(dr)*

www.concept.biz

Mehrstufige Sicherheit für Online-Nutzer

Die Symantec-Tochter **PC Tools** bringt die 2010er-Versionen ihrer Sicherheitssoftware auf den Markt. Die Produkte richten sich an Privatnutzer, aber auch kleinere Netzwerkumgebungen, etwa in SOHOs. Die Tools umfassen **Spyware Doctor mit AntiVirus 2010**, **Spyware Doctor 2010** und **PC Tools Internet Security 2010**. Alle Produkte sind nun Windows 7-kompatibel. Eine Kombination verschiedener Technologien soll zudem einen zuverlässigen mehrstufigen Schutz an jedem möglichen Zugangspunkt bieten und dabei die Art der Computernutzung erkennen. Die verhaltensbasierte Technologie des Behavior Guard (ThreatFire) blockiert dabei laut Hersteller Gefahren schneller als herkömmliche Signaturverfahren. Hierfür analysiert die Komponente das Verhalten von Dateien auf Malware-verdächtige Aktivitäten. Die Module "Site Guard" und "Browser Guard" bieten zudem mehrstufigen Browser-Schutz, der die Analyse dynamischer Inhalte miteinbezieht, um etwa Website-Manipulationen, Roguewareware-Attacken und Drive-by-Downloads zu unterbinden. Dank des "Idle Mode" führt die Software dabei automatisch rechenintensive Aufgaben wie Scans und Updates dann durch, wenn der Computer gerade nicht genutzt wird. Leistungsbeeinträchtigungen sollen sich dadurch auf ein Minimum reduzieren. Spyware Doctor ist für 25 Euro zu haben, Spyware Doctor mit Antivirus kostet rund 34 Euro, während die Komplett-Suite Internet Security mit zusätzlicher Firewall für 42 Euro erhältlich ist. *(dr)*

PC Tools: www.pctools.de

Thin Clients für alle Fälle

Rangee erweitert seine Produktreihe um die drei neuen **Thin Client-Modelle LT120, LT320 und LT520**. Das Einstiegsmodell LT120 bietet mit einer AMD 500MHz CPU laut Anbieter genug Leistung für gängige Terminal Server- und Virtualisierungsanwendungen. Ein Metallgehäuse schützt das Gerät von der Größe eines CD-Laufwerks vor äußeren Einflüssen. Neben vier USB 2.0-Anschlüssen stehen im LT320 zwei PS/2-Anschlüsse für Maus und Tastatur sowie ein paralleler und zwei serielle Anschlüsse zur Verfügung. Ebenso verfügt das Gerät über DVI-D und VGA Grafik-Ausgänge, womit sich zwei Monitore im Dual-Monitor-Betrieb anschließen lassen. Leistungstechnisch ist der Thin Client mit einem VIA 1 GHz-Prozessor und 512 MByte DDR2-RAM ausgestattet. Die größere Variante LT520 bietet einen Intel Atom 1,6 GHz N270-Prozessor, der auch bei größeren Anwendungen genügend Leistung bieten soll. Daneben ist der Rechner mit sieben USB-, einem parallelen und zwei seriellen Anschlüssen ausgestattet. Ein internes DVD-RW Laufwerk und der frontseitig eingebaute Kartenleser für SD- und Micro-SD-Karten erlauben zudem die Nutzung von Speichermedien. Softwareseitig werden alle Thin Clients der neuen Produktlinie mit Rangee Linux für Thin Clients ausgeliefert. Damit unterstützen die Geräte RDP-Remotedesktop, Citrix ICA und XenAPP sowie VMware View. Auch den neuen WLAN-Standard 802.11n verstehen die Geräte bereits. Ab sofort sind die neuen Modelle erhältlich – die Preise liegen je nach Modell und Ausstattung zwischen 194 und 434 Euro. *(dr)*

Rangee bietet die drei neuen Thin Client-Modelle LT120, LT320 und LT520 an

Rangee: www.rangee.com

IT-Administrator und SanDisk verlosen fünf Exemplare des USB-Flash-Laufwerks **SanDisk Ultra Backup** mit einer Speicherkapazität von je 32 GByte im Gesamtwert von 480 Euro. Mit dem **Backup-Stick** lassen sich per Knopfdruck große Mengen an Daten bequem speichern: Ob Bilder, Videos oder große Multimedia-Files – mit einem einzigen Klick ist ohne Kabel oder vorherige Softwareinstallation alles gesichert. Der USB 2.0-Anschluss sorgt dabei für eine schnelle Datenübertragung, für die Sicherheit der Daten ist die 128-Bit AES-Verschlüsselung zuständig. Der Speicherriegel ist in den Größen 8, 16, 32 sowie 64 GByte erhältlich und benötigt einen High-Power USB-Port. Wenn Sie eines der fünf 32 GByte-Exemplare gewinnen möchten, schreiben Sie spätestens bis zum 10. Dezember eine E-Mail an **redaktion@it-administrator.de** mit dem Betreff **SanDisk**. Für die Verlosung wünschen wir Ihnen schon jetzt viel Glück *(ln)*

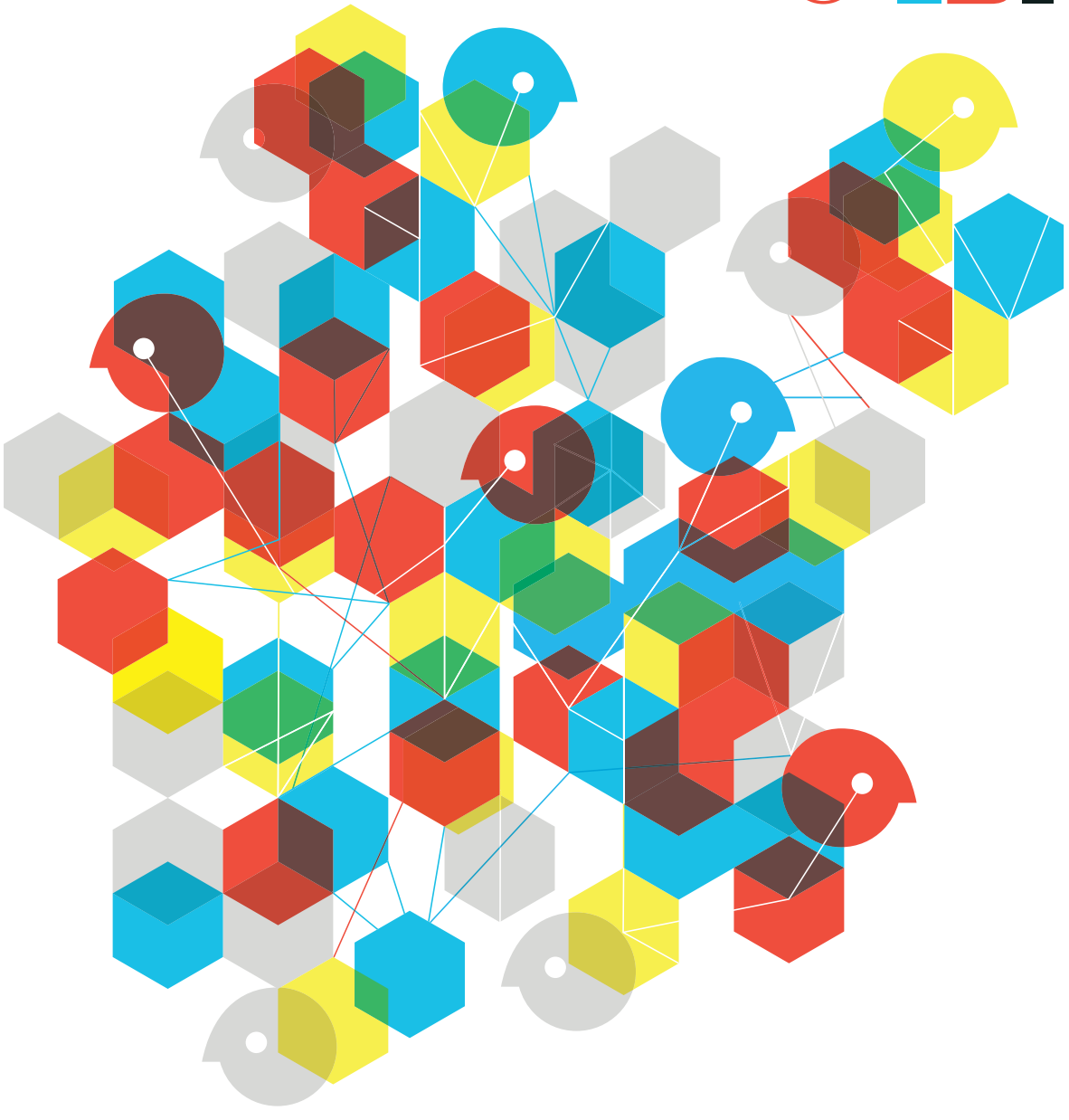
Gewinnen Sie fünf USB-Sticks für einfaches Backup

Intelligente Technologien für einen smarten Planeten

Wer zieht die Grenzen eines Unternehmens – die Mitarbeiter oder die IT?

Immer öfter und immer intensiver arbeiten wir mit Menschen, die sich außerhalb unserer Unternehmensgrenzen aufhalten: mit Partnern, Zulieferern, Kunden und Mitarbeitern im Außendienst oder Home-Office. Genau deshalb erweitert IBM das Collaboration-Portfolio um Tools wie Social Software, Wikis, Instant Messaging – und schafft zugleich neue Formen des Zugriffs, z. B. per Cloud Computing. Mit Cloud-basierten Lösungen wie LotusLive spielt es keine Rolle mehr, auf welcher Seite einer Firewall sich einzelne Mitglieder eines Teams befinden. Alle können ungehindert zusammenarbeiten, und zwar auf dem hohen Sicherheitsstandard, den sie von IBM gewohnt sind. Anders ausgedrückt: Sie können das Teamwork in und um Ihr Unternehmen nahtlos ausbauen, ohne dafür eigens eine kostspielige und komplexe Infrastruktur aufzubauen. Sie müssen Ihre Grenzen nicht einreißen, um über sie hinauszuwachsen.

Smarte Unternehmen brauchen intelligente Software, Systeme und Services.
Also: Machen wir den Planeten ein bisschen smarter. Wie, erfahren Sie unter ibm.com/collaborate/de



O&M IBM IT 26/09

it-sa, 13. bis 15. Oktober, Nürnberg und RSA Conference Europe 2009, 20. bis 22. Oktober, London

Sicher ist sicher

von Daniel Richey

Im Oktober 2008 schloss die Münchner IT-Messe Systems nach 29 Jahren ein letztes Mal ihre Tore. Bekannt war die Messe dabei auch für ihre IT-Security Area – eine dedizierter Bereich nur für IT-Sicherheitsprodukte und -dienstleistungen. Doch sollte das Aus in München nicht gleichzeitig das Ende der erfolgreichen Security-Ausstellung bedeuten. Vielmehr fand die IT-Security Area als "it-sa" in Nürnberg ein neues Zuhause. Veranstaltet vom Secu-Media-Verlag begrüßte die neue Messe vom 13. bis 15. Oktober ihre ersten Besucher.

Bekanntes Konzept: Im blauen und roten Forum erfahren die Besucher der it-sa Neues über IT-Sicherheit

Für Peter Hohl, Geschäftsführer des Secu-Media-Verlags als Veranstalter der it-sa, stand fest, dass die IT-Sicherheitsbranche eine eigene Leitmesse will. Er würdigte die über 250 Aussteller in seiner Eröffnungsrede als Zeichen hierfür und erwartet für die Zukunft sogar fünfstellige Besucherzahlen. Dieses Jahr besuchten immerhin über 6.000 Interessierte die erste it-sa. Besonders wichtig war dem Veranstalter dabei die Tatsache, dass es sich bei der it-sa nicht um eine Regionalmesse handeln soll. So waren etwa Aussteller aus Russland, Malta, Indien oder Italien präsent.

Ein überwiegend positives Bild der it-sa zeichneten auch die Aussteller selbst. Zwar wirkten die Hallen mitunter etwas leer, trotz der über 6.000 Besucher. Doch besonders die Qualität der Kontakte sei hoch gewesen. Wichtige IT-Leiter und Sicherheitsverantwortliche großer und kleinerer Unternehmen hätten sich demnach über die neuesten Produkte und Trends informiert. Überwiegend unbeteiligtes Laufpublikum wie auf anderen Messen war dagegen eher die Ausnahme. Im Gespräch verdeutlichten daher auch einzelne Aussteller, die sich an größeren Ständen eingemietet hatten, im nächsten Jahr mit einem eigenen Stand auf der Messe vertreten sein zu wollen.

RSA Conference Europe 2009

Ebenfalls um Sicherheit drehte sich die zehnte RSA Conference Europe 2009 vom 20. bis 22. Oktober in London. In über 70 Sessions und zehn Tracks konnten sich die Besucher über die neuesten Trends in der IT-Sicherheit informieren. Dazu zählten unter anderem Themen wie die Absicherung virtueller Umgebungen, das Härten von Internetbrowsern oder auch die Sicherheit von Cloud-Computing. Für Art Coviello und Christopher Young, President sowie Senior Vice President von RSA, spielte in ihrer Keynote eine entscheidende Rolle, dass Unternehmen künftig auf ganzheitliche Sicherheitsstrategien setzen. Hierfür sei es wichtig, dass Sicherheit in die IT-Infrastruktur eingebettet sein müsse. Zudem müsse die internationale Zusammenarbeit gestärkt und so ein Ecosystem für IT-Sicherheit geschaffen werden. Dazu zähle etwa, dass sich Banken über laufende Angriffe gegenseitig informieren, um so rechtzeitig Schutzmaßnahmen zu ergreifen.

Computer Associates nutzte das Event daneben, um eine neue Studie zum privilegierten User-Management vorzustellen. Darunter ist die Nutzung von Administrationsaccounts zu verstehen, die Personengruppen und nicht einzelnen Nutzern zugeteilt sind. Daraus ergeben sich Probleme hinsichtlich der Nachvollziehbarkeit von Änderungen und damit der Verantwortlichkeiten. So haben laut der Studie, die Quocirca in 13 europäischen Ländern und Israel durchgeführt hat, denn auch 41 Prozent der befragten Unternehmen solche Accounts eingerichtet. Zwar verfügten immerhin 24 Prozent der Firmen über eine manuelle Kontrolle, um die Aktivitäten zu überwachen. Diese reiche jedoch nicht aus. Vielmehr hätten zahlreiche Sicherheitsvorfälle die Risiken aufgezeigt, die von solchen Superuser-Konten ausgehen. Immerhin plane knapp die Hälfte der Befragten, eine passende Managementlösung künftig zu implementieren. Auch CA stellte mit "Access Control 12.5" eine entsprechende Lösung vor.

IIR-Forum Virtualisierung, 7. und 8. Oktober 2009, Frankfurt/M.

Viele neue Möglichkeiten

von John Pardey

Nachdem Servervirtualisierung nunmehr zu einem Standardwerkzeug des IT-Managements geworden ist, versammelte IIR Technology auf seinem Virtualisierungs-Forum Experten und Praktiker um zukünftige Wege der Virtualisierung zu diskutieren. So standen an den zwei Tagen einerseits Themen wie Desktop- und Storagevirtualisierung, andererseits Fragen nach dem Monitoring und Management auf dem Programm. IT-Administrator war für Sie vor Ort.

Als Keynote-Sprecher präsentierte Prof. Dr. Arnd Bode vom Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften in München keine staubtrockene Kost aus Forschung und Lehre, sondern stellte am Beispiel des eigenen Rechenzentrums den Bedarf und die Notwendigkeit zur Virtualisierung vor. Zwar wird nicht jeder Administrator einen Hochleistungsrechner betreiben, der, wie der von Professor Bode, in den Top 10 der weltweit leistungsfähigsten Supercomputer rangiert, dennoch verdeutlichte der Vortrag erneut die Vorteile, die Konsolidierung durch Virtualisierung bietet. So sparte das Team von Bode durch die Konsolidierung nicht nur Strom und Zeit (durch schnellere Bereitstellung neuer Serverinstanzen), sondern schlicht und ergreifend sehr knapp gewordenen Platz.

Sicherheit fraglich

Im Anschluss ergriff Enno Rey, Berater und Geschäftsführer der ENRW GmbH, das Wort in Sachen Sicherheit der Virtualisierung. Als eine zentrale Aufgabe definierte Rey dabei das Absichern der Virtualisierungsumgebung. Denn die Virtualisierung bringt neue Angriffsszenarien mit sich, die Administratoren kennen und berücksichtigen sollten: denkbar seien Angriffe von Gast zu Gast, von Host zu Gast und vom Gast zum Managementsystem.

Als relevant stuft Rey hier nur die Angriffsmöglichkeit vom Gast zum Host ein, die jedoch bei ESX-Hosts ein ernstzunehmendes Problem darstelle.

Nicht weniger gravierend sind nach Auffassung Reys jedoch organisatorische Mängel im Change- und Configurationsmanagement virtueller Maschinen. Durch unklare Zuständigkeiten und Prozesse entwickeln sich "Rogue VMs" immer mehr zu einem Problem. Eine solche, nicht vertrauenswürdige VM, schaffe Probleme hinsichtlich Data Leakage sowie Virenerkennung und werfe Fragen hinsichtlich der Integrität der VM auf.

Desktopvirtualisierung in der Praxis

In den folgenden beiden Vorträgen stellten Stefan Schmidt, UniCredit, und Florian Loos, Telefónica o2 Germany GmbH, ihre Desktopvirtualisierungsprojekte vor. Während Schmidt den eigenen Einstieg in die Desktopvirtualisierung als Philosophiefrage betrachtete, die im Unternehmen den Terminal Services vorgezogen werde, stellte Loos in seinem Projekt eine Speziallösung für die Softwareentwicklung in Indien vor.

Schmidt machte deutlich, dass sich für sein Unternehmen der Einstieg in diese neue Technologie zwar hinsichtlich des Know-How-Gewinns gelohnt habe, wirklich gerechnet habe sich das Projekt jedoch nicht. Loos hingegen zeigte auf, dass Desktopvirtualisierung als Speziallösung für eine sichere Softwareentwicklung in Indien eine Erfolgsgeschichte sei, die schnell von anderen Abteilungen aus seinem Haus adaptiert wurde.

Archivierung virtuell

Einen interessanten Ansatz für die Langzeitarchivierung stellte im Folgenden Horst Bräuer von der Stadtverwaltung Schwäbisch Hall vor. In städtischen Archiven herrscht die Anforderung, Daten bis zu 100 Jahre aufzubewahren, was insbesondere die Fragestellung nach der zukünftigen Lesbarkeit aktueller Dateiformate aufwirft. Die Stadt Schwäbisch Hall setzt hier auf Open Source-Lösungen, indem die zu archivierenden Daten inklusive des "Reader" (beispielsweise Word oder Excel) und des zugrunde liegenden Betriebssystems mit Virtual Box virtualisiert und anschließend in einem Open Source-Archiv ablegt werden. Durch die offenen Quellen der Virtualisierungs- und Archivlösung wird somit gewährleistet, dass die Daten zukünftig sicher aus dem Archiv rekonstruiert werden können. Ein Vorgang, der aktuell, so Bräuer, bei vielen historischen Dokumenten nicht möglich sei.

Zahlreiche weitere spannende Beiträge rund um Storage- und Servervirtualisierung sowie Lizenzen, Green IT und Cloud Computing rundeten das Forum ab, sodass die Teilnehmer nach zwei Tagen einen Überblick über die Strategien und Techniken jenseits der Server-Virtualisierung im Gepäck hatten.

1. COMIDD Expertengipfel, 8. September 2009, Hanau

Auf Tuchfühlung mit IT-Compliance

von Daniel Richey

Schirmherr Jörg-Menno Harms sieht die Verständnislücke zwischen Politik und IT als Hürde für gute Gesetze

Kaum ein Begriff ist so omnipräsent und gleichzeitig so wenig greifbar wie die Compliance. Laufend finden sich neue Presseberichte zu Regularien wie GdPDU, BDSG, SOX oder Basel II. Die abstrakten Begriffe konkret auf die IT-Landschaft herunterzubrechen, fällt jedoch den meisten Firmen schwer. Die Industrieinitiative COMIDD versucht, den Compliance-Dschungel für Firmen zu lichten. Anfang September fand ihr erster Expertengipfel statt.

Beim Thema Compliance stellen sich Unternehmen meist die Fragen, wo anfangen, was beachten und vor allem – wie mit der bestehenden IT-Umgebung und den verfügbaren Mitteln umsetzen? Besonders kleine und mittelständische Unternehmen stehen vor einem kaum überwindbaren Berg, dessen Gipfel auch noch in Nebel verhüllt ist. Hier möchte die Initiative "IT-Compliance in der Informations- und Datenverarbeitung in Deutschland", kurz COMIDD, Abhilfe schaffen. Im April 2009 von Hewlett-Packard und Optimal Systems gegründet, will sie den Wissensstand zu IT-Compliance erweitern und ein Forum für Soft- und Hardwarehersteller, Dienstleister, Juristen sowie Industrie und Politik bieten.

Anfang September fand der erste "Expertengipfel Compliance" in Hanau statt. Rund 130 Teilnehmer – überwiegend IT-Verantwortliche und Geschäftsleiter – informierten sich in sieben Vorträgen über den Stand der Dinge zur IT-Compliance. Dabei gingen die Referenten durchaus hart mit dem bisherigen Umgang mit dem Thema sowie den gesetzlichen Regelungen ins Gericht, etwa dem überarbeiteten Bundesdatenschutzgesetz (BDSG). Für den Moderator der Veranstaltung, Michael Gießelbach, gab es bereits gefühlte zwei Millionen Compliance-Events und Tonnen an Papier dazu. Alles gesagt sei dennoch nicht, trotz einer gestiegenen Qualität in der Diskussion. Der Director Storage Sales bei Hewlett-Packard sah besonders bei der Frage nach einer rechtskonformen Archivierung noch Klärungsbedarf. So regelten zwar die "Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen" (GDPdU) den Zugriff, nicht jedoch die Form der Archivierung.

Viele Firmen sehen die Compliance-Regeln eher als Strafe denn als Chance, erläuterte daraufhin Professor Dr. Jörg-Menno Harms, der Schirmherr der COMIDD und Aufsichtsratsvorsitzende bei HP. Hier sei besonders der Gesetzgeber gefragt, nicht das Augenmaß zu verlieren und sich auf die Ziele seiner Regelungen zu fokussieren. Die Praktiken für dessen Erreichen sollten hingegen nicht reguliert werden. Überhaupt stimmten die Referenten auf der Veranstaltung im Wesentlichen darin überein, dass die rechtlichen Vorgaben von Nicht-IT-Fachleuten erlassen würden, wohingegen die Umsetzung an IT-Verantwortlichen hängen bliebe, die von den juristischen Feinheiten wiederum keine Ahnung haben. So entstehe denn auch eine gegenseitige Verständnislücke, welche die Umsetzbarkeit behindere.

Ein konkretes Beispiel aus der Praxis stellte Dr. Andreas Rebetzky, CIO bei Bizerba, vor. Der Hersteller von Industriewaagen hat bereits seinen Compliance-Prozess in die Tat umgesetzt. Dabei stand für das Unternehmen besonders im Vordergrund, aus dem Dschungel an Anforderungen die relevanten herauszufiltern und diese als dauerhaften Prozess in die Geschäftsabläufe zu integrieren. So sind nun Teams für die Umsetzung von Regularien verantwortlich, die sich an verständlichen und auf das Unternehmen angepassten Zielen orientieren. Gestaffelt wurde die Umsetzung dabei im Rahmen eines Zielkorridors an der Bedeutung der einzelnen Themenbereiche für Bizerba – bei wichtigen Bereichen wurde auf vollständige Compliance hingearbeitet, während weniger relevante Themen erst einmal grundlegend bearbeitet wurden.

DURCHDACHT BIS INS LETZTE DETAIL.

Leistungsstark.
Intelligent.

DER NEUE PRIMERGY RX200 S5

Verbessern Sie Ihre Energieeffizienz im Rechenzentrum mit dem innovativen PRIMERGY Cool-safe™ Systemdesign der neuen RX200 Rack Server Generation. Erhalten Sie mehr Leistung, verbesserte Erweiterbarkeit und Zuverlässigkeit in Kombination mit einem umfassend verbesserten Verhältnis von Leistung zu Energie – all dies bietet ihnen der neue PRIMERGY RX200 mit Intel® Xeon® Prozessoren in nur einer Rackeinheit.

Fujitsu ist weltweit viertgrößter Anbieter von umfassenden IT-Infrastrukturen. Bei Entwicklung und Produktion setzt Fujitsu international auf „Made in Germany“. So wurde die Verantwortung für strategische Produktbereiche wie x86-basierte Server, Storagesysteme und die Entwicklung innovativer Umwelttechnologien in Deutschland konzentriert. Fujitsu ist ein kundenorientiertes IT-Unternehmen, das flexibel und anpassungsfähig auf alle Anforderungen reagiert. Fujitsu bietet Unternehmen aller Größenklassen qualitativ hochwertige Produkte, Lösungen und Services für die IT-Infrastruktur, die auf weltweit führenden High-Performance-Informationstechnologien basieren.

Mehr Informationen unter http://de.fujitsu.com oder 01805 372 100 (14 ct/Min.)

FUJITSU

Im Test: Tobit David.fx

Das Überall-Büro

von Sandro Lucifora

Mit David.fx liefert die Tobit Software AG seit Mai 2009 eine im Kern runderneuerte Version der deutschen Groupware-Lösung aus. Der Kern der Neuerungen ist die Mobilität und das flexible Arbeiten mit dem System. Ob die vollmundigen Versprechen des Ahauser Unternehmens eingehalten werden, haben wir in einem sechsmonatigen Langzeit-Test für Sie herausgefunden.

Mit dem Slogan "Arbeiten, von wo Sie wollen" startete Tobit Software die Einführung der Groupware David.fx. Wir haben uns einmal genauer angesehen, wie dieses Versprechen umgesetzt wurde und wie sich die neue Mobilität bei David.fx bemerkbar macht. Die Grundstruktur des Systems ist schnell ausgemacht: Der David-Server besteht aus diversen Diensten, deren Basis-Funktionen durch den Service Layer gesteuert werden. Die Mobilität bei David zeigt sich in den neu entwickelten Clients.

Neues Lizenzmodell

Bevor wir uns die technische Umsetzung der Mobilität mit David anschauen, werfen wir ein Blick auf das geänderte Lizenzmodell. Bisher waren in der Basislizenz lediglich die lokalen Zugriffsmöglichkeiten enthalten. Wer über einen der später im Artikel näher beschriebenen Clients auch von extern auf seine Daten zugreifen wollte, musste bisher eine zusätzliche Remote-Lizenz kaufen. Bei David.fx ist diese Funktion jetzt schon in der Basislizenz enthalten.

Der große Vorteil dabei ist, dass nun jeder David-Anwender mal eben von unterwegs oder im Urlaub einen Blick auf seine Nachrichten werfen kann, ohne einen Investitionsantrag für die Zusatzlizenz bei der Geschäftsleitung stellen zu müssen. Zudem ist die neue Version gegenüber dem Vorgänger David.zehn! um einiges preiswerter geworden. Waren für die Fünf-User-Basis-Lizenz inklusive Remote-Clients mindestens 790 Euro zu zahlen, müssen für den gleichen Umfang mit David.fx nur noch 650 Euro überwiesen werden.

Clients in der Übersicht

Neben dem David-Client für Windows, der auch unter Windows 7 arbeitet, gibt es den neuen David-Client iPhone, den bekannten Pocket-Client für Windows Mobile, den David-Client Java und das Webfrontend David-Client Web. Alle Clients, die als Frontends für den David-Server fungieren, erlauben den flexiblen und vollumfänglichen Zugriff auf die eigenen Daten.

Client für Windows jetzt auf IP-Basis

Die größte technische Änderung erfolgte beim David Client für Windows. Hier hat der Hersteller die Kommunikation zwischen dem Client und dem Server auf IP-Basis umgestellt. Bis zu David!zehn lief alles auf Dateiebene und ein Zugriff von außen war nur eingeschränkt möglich oder benötigte den Dateizugriff, zum Beispiel über eine Firewall. Doch das war mehr Schein als Sein, denn der Zugriff war unerträglich langsam.

Für die Installation des David-Clients stehen jetzt zwei Installations-Varianten zur Auswahl: Der normale David-Client und die Ausprägung David-Client Mobile. Der Unterschied ist schnell ausgemacht: Die

Technische Voraussetzungen

Egal, für welchen mobilen David-Client Sie sich entscheiden, es müssen einige technische Voraussetzungen erfüllt sein. Unerlässlich ist die Erreichbarkeit des David-Servers aus dem Internet. Diese erfolgt über die IP-Adresse des Internet-Anschlusses. Die Problematik dabei ist, dass sich gerade beim Einsatz im SOHO-Bereich im Normalfall spätestens alle 24 Stunden die IP ändert. Wenn der Anwender unterwegs ist, muss er entweder die neue IP kennen und im Client manuell ändern oder über einen dynamischen DNS-Eintrag über eine statische Domain verfügen. Ein bekannter Dienst hierfür ist DynDNS. Um DynDNS bei jeder Änderung die neue IP-Adresse mitzuteilen, muss der Router über eine entsprechende Funktion verfügen.

Da dies nicht alle Router können, bietet Tobit Software einen Dienst namens "Server Locater Service" (SLS) an. Dabei steht unter der Domain tobit.net ein persönliches Alias, zum Beispiel it-administrator.tobit.net, zur Verfügung. Diese Domain wird als Server im David-Client eingetragen. Der David-Server prüft nun ständig, ob sich die offizielle IP gegenüber dem DNS-Eintrag geändert hat und veranlasst gegebenenfalls die sofortige Aktualisierung. Für diesen Service berechnet der Anbieter einen Euro pro Monat. Für den Zugriff mit dem Client muss in der Firewall beziehungsweise dem Router Port 80 oder alternativ Port 81 auf den David-Server geroutet sein. Für den Windows-Client bedarf es des Routings von Port 267.

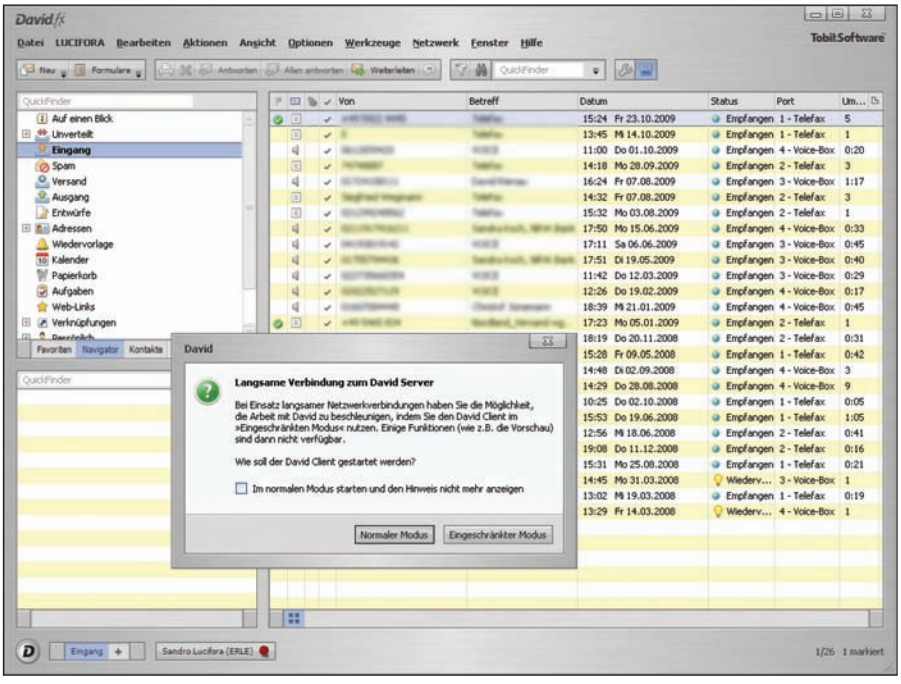


Bild 1: Ist die Verbindung zum David-Server zu langsam, bietet der Client auch einen eingeschränkten Modus an

einfache Installation greift nur über IP auf den David-Server zu und erlaubt die Bearbeitung der Daten auf dem Server. Dabei ist es egal, ob der Zugriff aus dem internen oder dem externen Netzwerk erfolgt. Der Nachteil dabei zeigt sich, wenn der User auch gerne offline mit seinen persönlichen Daten arbeiten möchte, was so nicht geht. Um seine Nachrichten offline zu bearbeiten, wird der David-Client Mobile mit einem minimalen David-Server auf dem Rechner, meist einem Notebook, installiert. Mit dieser Installation werden die persönlichen Daten zusätzlich lokal gespeichert und mit dem David-Server im Unternehmen repliziert.

Die Grundidee dieser Replikation ist hervorragend, doch leider kam im Test die eine oder andere Fehlfunktion zum Vorschein. So verfügt die Groupware auch in der neuen Version noch immer über keine funktionierende Synchronisation von Wiedervorlagen. Das macht sich vor allem dann bemerkbar, wenn der User einmal mehrere Tage sein lokales System nicht mit dem Unternehmens-Server repliziert. Da beide Server in der Zwischenzeit autark arbeiten, erfolgen bei beiden Servern unabhängig die Wiedervorlagen. Der Anwender hat diese Erinnerungen im Offline-Modus auf seinem Notebook bereits bestätigt und ad acta gelegt. Bei einer späteren Replikation werden die auf dem Server in der Firma noch existierenden und nicht bestätigten Wiedervorlagen auf das Notebook kopiert und erneut im David-Client angezeigt – obwohl der Nutzer diese lokal schon längst bestätigt hat. Das passiert, weil David in diesem Fall lediglich mit Kopien der Datenbestände arbeitet und außerdem vorher nicht prüft, ob sich der Status verändert hat. Hier muss Tobit Software noch nacharbeiten.

Beim Einsatz des David-Clients auf IP-Basis zeigt sich das System sehr stabil und benutzerfreundlich. Die Umsetzung ist hier rundum gelungen. Egal, von wo auf der Welt der Zugriff auf die Daten erfolgt, es arbeitet sich so, als säße man im Büro vor Ort. Eine kleine Einschränkung ergibt sich aus der Natur der Sache: Im Gegensatz zum lokalen Netzwerk mit 100 MBit ist die Geschwindigkeit beim Datenaustausch auf die kleinste Geschwindigkeit, bei ADSL-Internetverbindungen auf den so genannten Upstream, begrenzt. Selbst wenn auf beiden Seiten beispielsweise eine 20 MBit-Leitung zur Verfügung steht, beträgt durch den langsameren Upstream der tatsächliche Datendurchsatz in der Verbindung nur 1.024 KBit/s. In der Praxis bedeutet dies, dass mit David.fx rein technisch die Arbeit auch von außerhalb wie vom eigenen Schreibtisch zu erledigen ist, doch für den Zugriff auf die Daten mehr Zeit benötigt wird.

Client für das iPhone mit Mängeln

Wer ein iPhone 3G/3GS sein Eigen nennt, kann ganz entspannt seine persönlichen Nachrichten an diesem Mini-Computer bearbeiten. Ganz neu bietet Tobit dazu den David-Client iPhone über den Appstore zum kostenlosen Download an. Dabei handelt es sich um eine native Applikation. Nach dem Download und der Installation wird schnell deutlich, dass sich der iPhone-Client sauber in die Benutzeroberfläche des Smartphones einreiht, einfach zu bedienen ist und sich der zur Verfügung stehenden Schnittstellen zum Adressbuch und zum Kalender bedient. Mit dem neuen Betriebssystem 3.0

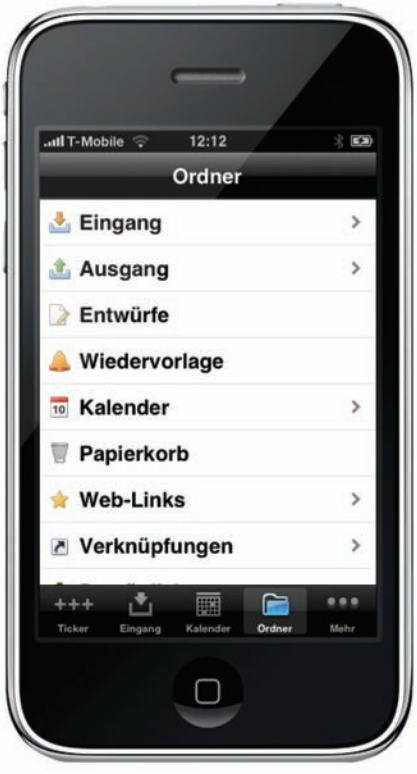


Bild 2: Der David-Client für das Apple-Smartphone hat die iPhone-übliche, übersichtliche Struktur – leider sind nicht alle David-Funktionen verfügbar

Bild 3: Der Ticker informiert auf dem iPhone über alle neuen Nachrichten

funktioniert auch die passive Benachrichtigungsfunktion beim Eintreffen neuer Nachrichten.

Beim zweiten und dritten Blick fällt jedoch auf, dass nicht alle David-Funktionen im iPhone zur Verfügung stehen. In der Ordner-Struktur fehlen die Aufgaben sowie der Zugriff auf die Gruppen-Archive. Schnell zeigt es sich, dass diese Client-Variante auf die persönlichen Nachrichten, den Ticker sowie Adress- und Kalenderdaten reduziert ist.

Als Neuerung lassen sich über das iPhone auch Voice-Mails per E-Mail versenden. Dieser neue Nachrichten-Typ zeichnet eine Sprachnachricht auf und sendet sie als WAV-Datei im Anhang an den E-Mail-Empfänger. Je nachdem, wie groß das Mitteilungsbedürfnis ist, kann das eine echte Alternative zur doch eher mühsamen Texteingabe über die iPhone-Tastatur sein.

Leerzeichen beim Benutzernamen umschreiben

Wenn Ihr Browser beim Aufruf der URL für den David-Client Web oder Java ein Leerzeichen im Benutzername – standardmäßig ist das {Vorname Zuname} – nicht unterstützt, tragen Sie statt des Leerzeichens "%20" ein.

Pocket-Client für Windows Mobile

Schon länger verfügbar und etwas ausgereifter ist die Client-Variante David-Client Pocket. Die für Windows Mobile entwickelte Software wird über ActivSync auf dem PDA installiert und eingerichtet. Anders als der iPhone-Client handelt es sich hierbei nicht um eine in das Betriebssystem eingebettete Lösung. David-Client Pocket läuft im Multitasking-Betrieb auf dem PDA als eigenständige Applikation und ist nicht mit dem eingebetteten Telefonbuch, dem Kalender und der E-Mailfunktion von Windows Mobile verknüpft. Jedoch lassen sich zumindest die David-Kontakte und -Kalendereinträge über ActivSync manuell in das Adressbuch beziehungsweise den Kalender des Telefons transferieren.

Als großen Nachteil empfanden wir, dass die für David geschriebenen DFML-Formulare – wie die mitgelieferte Telefonnotiz als Abwesenheitsbenachrichtigung oder der Urlaubsantrag – auf dem David-Client Pocket nicht als Formular angezeigt werden. Das erschwert die Arbeit; obwohl genau diese Formulare diverse Arbeitsabläufe mit David erleichtern sollen.

Java-Client

Wer weder über ein iPhone noch einen PDA mit Windows-Mobile verfügt, dem bietet sich als Alternative der David-Client Java. Dieser Client ist eine Java-basierte Version für alle Java-fähigen Handys. Auch der Marktführer Nokia unterstützt mit Symbian diese Technologie und ist somit eine willkommene Plattform für den Client. Für diesen Client muss die David WebBox sowie Remote Access für den Benutzer aktiviert sein. Um den David-Client Java zu installieren, haben wir im Handybrowser die URL des David Servers in der Syntax *http://server/username/infocenter/* eingegeben.

Auf richtige Java-Version achten

Für den David-Client Java muss auf dem Mobiltelefon die Java-Version "MIDP 2.0" (Java 2 Microedition) vorhanden sein. Bei Telefonen mit einer älteren Java-Version lässt sich unter Umständen durch ein Update der Telefonsoftware auch die neuere Java-Version zur Verfügung bereitstellen.

Nach der Verbindung und der Eingabe unserer Remote-Zugangsdaten wurde der Java-Client heruntergeladen, die Installation eingeleitet und eine neue Verknüpfung zum Client unter "Programme" angelegt. Den Test haben wir mit verschiedenen Handys durchgeführt, wobei der Download bei dem älteren, aber immer noch im Umlauf befindlichen Modell Nokia 6230i aufgrund der Größe der Datei abgebrochen wurde. In diesem Fall mussten wir die erforderlichen Dateien manuell über die Datenverbindung mit dem PC auf das Handy kopieren und installieren.

Nach dem Start auf dem Mobiltelefon sind sodann alle persönlichen David-Archive und -Daten verfügbar. Neben den Nachrichten erhalten wir auch Zugriff auf die Aufgaben und den Kalender. In der Praxis hat sich herausgestellt, dass der sinnvolle Einsatz der Java-Version stark vom verwendeten Mobiltelefon und vor allem dessen Display und Auflösung abhängig ist. Ein 1,7-Zoll-Handydisplay eignet sich gerade einmal dazu, nur kurz mal eben etwas nachzuschauen oder um einen Termin im Kalender zu prüfen. E-Mails lassen sich gerade noch lesen, schreiben ist nur im Notfall angesagt. Hingegen macht das Arbeiten mit dem Java-Client auf dem Nokia Communicator oder dem Yari von Sony Ericsson wesentlich mehr Spaß.

Web-Client

Der David-Client Web ist die fünfte mobile Client-Lösung. Hierbei handelt es sich analog zu Outlook Web Access um einen David-Client als Webfrontend. Die Seite lässt sich mit jedem gängigen Inter-

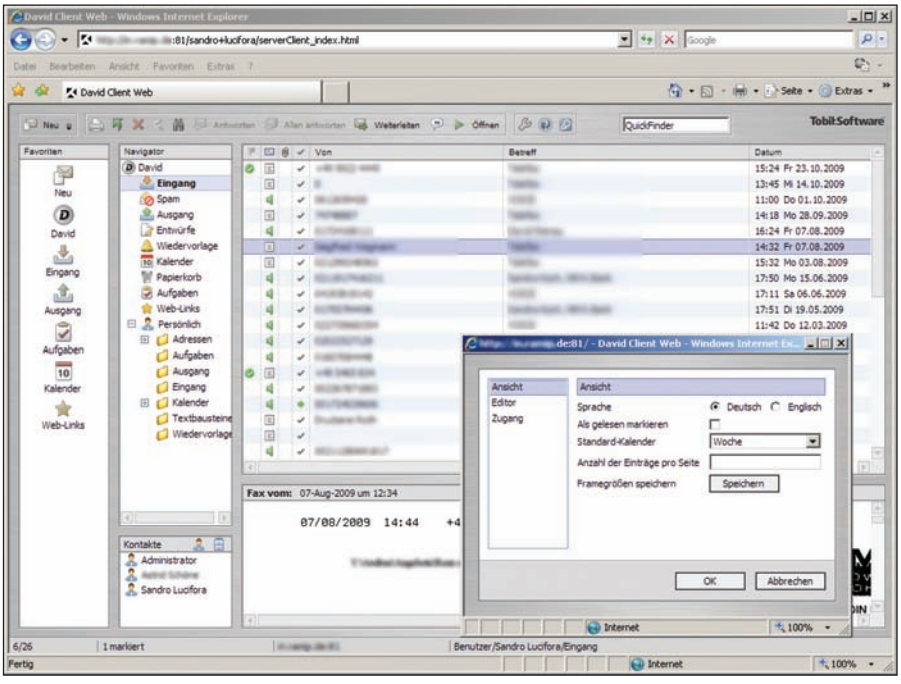


Bild 4: Der Web-Client sieht dem Windows-Client sehr ähnlich und erlaubt auch unterwegs individuelle Einstellungen

netbrowser aufrufen. Im Test haben wir den Client mit dem Internet Explorer 6 bis 8, Firefox 2 und 3 sowie Opera 9 und 10 erfolgreich nutzen können.

Übersichtlich präsentiert sich die Oberfläche: Die Anordnung der Elemente gleicht der in der Windows-Applikation. Im David-Client für Windows haben wir im Benutzerkonto voreingestellt, dass für neue E-Mails und Aufgaben nur Text und nicht HTML verwendet wird. Schrieben wir nun neue E-Mails über den Web-Client, wurden diese trotzdem in HTML geschrieben und versendet. Der Web-Client übernimmt die Nur-Text-Vorgabe also nicht, diese Option lässt sich auch nirgends einstellen. Das stört die sonst in David umgesetzte Corporate Identity empfindlich. Ansonsten gleicht die Arbeit mit der Web-Version nicht zuletzt wegen des nahezu gleichen Look-and-Feels dem Umgang mit dem Windows-Client.

Fazit

Tobit Software hat mit David.fx eine umfangreiche Groupware-Lösung mit überzeugenden Möglichkeiten entwickelt. Die lange Entwicklungszeit des gesamten Produkts ist jedoch nicht nur positiv zu sehen, da der Anbieter im Gesamtpaket immer noch sehr viele technologische Altlasten mitschleppt. Trotzdem ist uns keine andere Groupware bekannt, die einen solch umfangreichen mobilen Zugriff auf die Daten erlaubt. Nur hatten wir leider an manchen Stellen den Eindruck, dass die Umsetzung in der Entwicklung den tollen Ideen und Ansätzen hinterherhinkt. So fanden wir gute und sinnvolle Ansätze bei allen mobilen Clients, doch in der Tiefe betrachtet hat jeder mobile Zugriff seine funktionalen Schwächen. Teilweise fehlen ganze Funktionen, wie beim iPhone die Anzeige der Aufgaben.

Die Umsetzung des David-Clients unter Windows per IP-Verbindung finden wir sehr gut gelöst. Hier ist einziger Wermutstropfen, dass die Offline-Anbindung und die Replikation durch die fehlende durchgängige Synchronisierung aller Daten eher mangelhaft funktioniert.

Insgesamt ist herauszustellen, dass der Hersteller bei den mobilen Clients den Fokus auf die Funktionen für den Nachrichteneingang und -ausgang sowie auf Adressen und Kalender gelegt hat. Wer sich unterwegs auf genau diese Funktionen beschränken kann und will, ist mit jeder der hier genannten mobilen Anbindungen bestens versorgt. Alle anderen Anwender müssen hier und da funktionale Abstriche machen. *(ln)*

Produkt
Für den mobilen Einsatz geeignete Groupware-Lösung.

Hersteller
Tobit
www.tobit.de

Preis
Ein Basispaket für fünf Nutzer ist ab 650 Euro erhältlich.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

***So urteilt IT-Administrator** (max. 10 Punkte)*

Vielfältigkeit an Mobile-Clients	10
Funktionsumfang der Mobiltelefon-Clients	6
Bedienung der Mobiltelefon-Clients	7
Funktionsumfang des Windows Mobile-Clients	9
Bedienung des Windows Mobile-Clients	9
Funktionsumfang des Web-Clients	8
Bedienung des Web-Clients	9

Dieses Produkt eignet sich

optimal für Unternehmen, die ihre Mitarbeiter mit dem David-Client für Windows mit einem vollwertigen Windows-PC extern und nur online arbeiten lassen möchten.

teilweise für Unternehmen, die ihre Mitarbeiter über ein Mobiltelefon vorrangig mit E-Mailnachrichten und Kalendereinträgen versorgen wollen.

nicht für Anwender, die auf einem Mobiltelefon über den vollen Funktionsumfang von David verfügen müssen.

Tobit David.fx
Service Pack 26-10-2009

Im Test: Fujitsu Scaleo Home Server 2205

Zu Hause ist es doch am schönsten

von Christian Knermann

Mit dem Scaleo Home Server 2205 hat Fujitsu Technology Solutions ein NAS-System mit Windows als Betriebssystem im Angebot. IT-Administrator hat das Gerät im Hinblick auf den Einsatz im Home Office getestet. Dabei konnte der NAS-Speicher seine Vorzüge unter Beweis stellen.

Neben den stetig wachsenden Datenmengen ist das zentrale Backup aller Clients ein wichtiges, aber gerne vernachlässigtes Thema. Also muss ein Server her, der allen Clients vom Netbook bis zum Media Center-PC gleichermaßen Speicherplatz zur Verfügung stellt. Neben geringem Platzbedarf und niedrigem Energieverbrauch steht gerade im Home Office-Bereich auch die leichte Bedienbarkeit im Pflichtenheft. Denn wer möchte zu Hause schon als Vollzeitadministrator tätig werden? Als Antwort auf diese Frage empfiehlt Fujitsu den Scaleo Home Server 2205 [1], eine NAS-Box mit Abmessungen von 12 x 41 x 34 cm (H x B x T), die mit ihrem gefälligen Design durchaus im HiFi-Rack im Wohnzimmer ihren Platz findet. Mit den im Lieferumfang enthaltenen Standfüßen kann das Gerät wahlweise waagerecht oder senkrecht aufgestellt werden. An der Front finden sich zwei USB 2.0-Schnittstellen, zwei weitere auf der Rückseite sowie zwei eSATA-Ports. Ans Netz geht der Server über einen GBit-Ethernet-Anschluss. Angenehm fällt auf, dass das System über ein internes Netzteil verfügt, der Kaltgerätestecker wird direkt an der Box angeschlossen und der Kabelsalat hält sich somit in Grenzen.

Innere Werte

Soll das System um weitere Festplatten ergänzt werden, so kann dies ohne Werkzeug erledigt werden. Der Gehäusedeckel ist mit zwei Rändelschrauben fixiert und lässt sich einfach abnehmen. Das solide verarbeitete Gehäuse gibt sich im Inneren aufgeräumt. Von den vier Festplattenrahmen waren in unserem Testsystem zwei bestückt mit Western Digital WD10EACS 1 TByte-Platten aus der Caviar Green-Serie, die mit 5.400 U/min zwar nicht zu den schnellsten ihrer Art gehören, dafür aber einen niedrigen Energieverbrauch und Geräuschpegel versprechen. Letzterem trägt auch die Befestigung der Festplatten Rechnung. Diese werden jeweils mit vier im Lieferumfang enthaltenen Adaptern versehen und in den Rahmen eingehängt. Die Laufwerke sind somit nicht starr mit dem Gehäuse verbunden, wodurch störende

Bild 1: Die Festplatten werden mittels Klapp-Rahmen fixiert, die gelben Adapterstücke wirken schwingungsdämpfend

Intel-Fundament

Die Hardware des Scaleo stammt aus dem Hause Intel und wird dort als Intel SS4200-E angeboten [2]. Basis bildet in diesem Fall das Betriebssystem LifeLine, ein Linux-Derivat des Speicher-Herstellers EMC, das als OEM-Produkt speziell für den Einsatz auf NAS-Systemen vertrieben wird. Passend dazu kümmert sich die Backup-Software EMC Retrospect Express um die Sicherung von Windows, Linux und Mac OS-Clients. Wer sich mit dem Windows Home Server nicht anfreunden mag, findet damit eine Alternative für heterogene Umgebungen.

Schwingungen reduziert werden. Unterhalb der Festplatten befindet sich das Mainboard, das im Scaleo 2205 mit 2 GByte DDR2 RAM und einem x86-Prozessor, dem Intel Celeron 420 mit 1,6 GHz, bestückt ist. Die Kühlung der Komponenten besorgen zwei Lüfter auf der Rückseite des Gehäuses.

Mangels lokaler Schnittstellen für Tastatur und Bildschirm erfolgt die Ersteinrichtung des Servers über das Netzwerk. Dazu nahmen wir den Server in einem exemplarischen Heimnetzwerk mit 6 MBit/s DSL-Anschluss und einem Router vom Typ Fritz!Box 3270 in Betrieb. Von der mitgelieferten CD installierten wir dann die Client-Komponenten auf einem Windows XP-System. Die Setup-Routine richtete die Software "SCALEOwakeup" ein, einen Wake-On-LAN-Client, der sich im Systemtray verankert und auf einfache Weise das Starten des Servers ermöglicht, sofern sich dieser im Ruhezustand befindet. Weiterhin installierten wir den "Windows Home Server-Connector", welcher der Sicherung der Client-Computer dient und, ebenfalls als Tray-Icon, über den Zustand des Servers und der Clients Auskunft gibt. Während des Setups waren lediglich zwei Fragen zu beantworten, nämlich ob Updates der Client-Komponenten automatisch vom Server ausgeliefert werden sollen und ob der Client zu Backup-Zwecken aus dem Ruhezustand geweckt werden soll.

Unser Home Server hatte sich zwischenzeitlich bereits per DHCP mit einer IP-Adresse versorgt und wurde vom Assistenten für die Ersteinrichtung ohne Probleme gefunden. Auch das Setup des Servers war in denkbar wenigen Schritten erledigt. Nach Vergabe von Name und Admin-Passwort waren die automatischen Updates zu konfigurieren. Der Home Server kennt hier zunächst nur zwei Zustände, wahlweise Updates vollautomatisch zu installieren oder komplett zu deaktivieren. Die Zwischenstufen, Updates zur manuellen Installation herunterzuladen oder lediglich zu benachrichtigen, stehen an dieser Stelle nicht zur Wahl. Nach den obligatorischen Fragen zur Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit und zur Übermittlung von Fehlerberichten an Microsoft versorgte sich der Server automatisch mit Windows-Updates und startete anschließend neu.

Administration

Zentrale Anlaufstelle für den Administrator ist anschließend die Windows Home Server-Konsole, zu erreichen über das Tray-Icon des Home Server Connectors oder über den entsprechenden Startmenü-Eintrag. In einer horizontalen Leiste sind die verschiedenen Administrationsbereiche als Icon angeordnet. Über die Schaltfläche "Einstellungen" können Nutzer grundlegende Optionen festlegen. So lässt sich dort beispielsweise das SCALEO Power Management aktivieren. Es handelt sich dabei um ein von Fujitsu vorinstalliertes Add-In, das den Home Server um Energiesparfunktionen erweitert. Ist die Option aktiviert, lassen sich zurück im Hauptfenster über einen an Outlook erinnernden Kalender die Betriebszeiten des Servers festlegen. Dies geschieht über einen Klick in den Kalender und den Menüpunkt "Neue Betriebszeit". Es sind einzelne Termine genauso wie Terminserien möglich. So lässt sich beispielsweise flexibel definieren, dass das System an Werktagen von 8.00 bis 18.00 Uhr aktiv ist, an Wochenenden aber vielleicht nur von 10.00 bis 13.00 Uhr. Außerhalb dieser Zeiten begibt sich das System in den Ruhezustand (Suspend-to-disk), aus dem es manuell über das "SCALEOwakeup" Tool oder zur definierten Zeit automatisch wieder erwacht. Der Stromverbrauch sinkt dadurch signifikant. Wir maßen die Leistungsaufnahme, während drei Clients im Rahmen typischer Bürotätigkeiten Dateien abriefen und auf dem Server speicherten sowie jeweils eine inkrementelle Datensicherung durchführten. Zwar stieg der Leistungsbedarf dabei kurzzeitig auf bis zu 65 Watt, im Verlauf eines Arbeitsta-

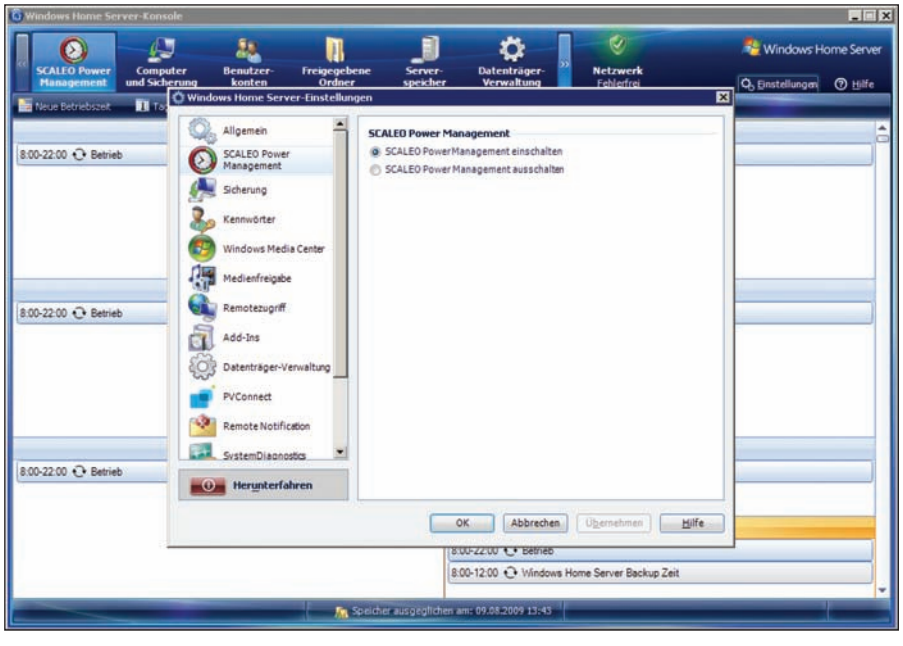


Bild 2: Die Home Server-Konsole erlaubt auf einfache Weise die Administration des Systems

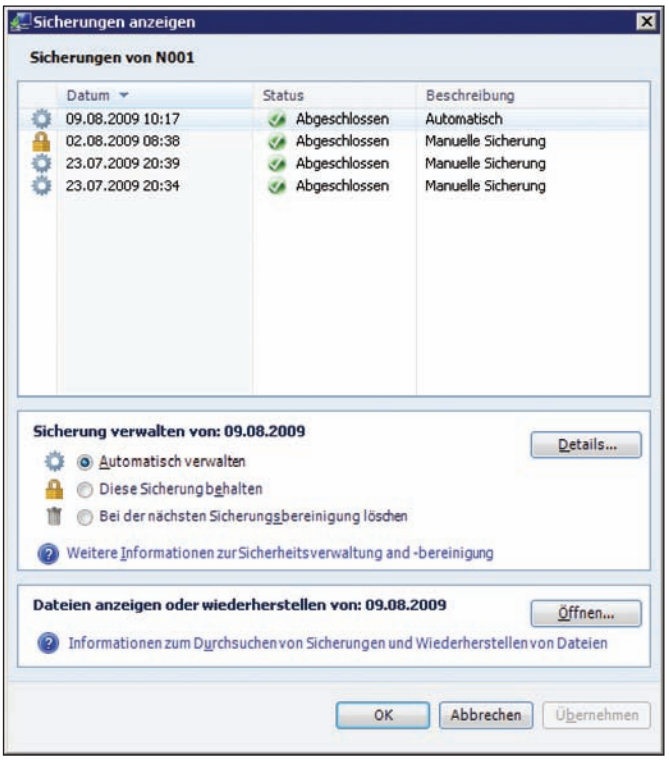


Bild 3: Der Home Server erzeugt automatisch Sicherungen der verbundenen Clients

ges begnügte sich der Server aber mit durchschnittlich 43 Watt. Im Ruhezustand reduzierte sich der Bedarf auf 2 Watt.

Unter "Computer und Sicherung" finden sich die Backups aller Clients, auf denen der Home Server-Connector installiert ist. Die Clients werden automatisch innerhalb eines Zeitfensters gesichert, das unter "Einstellungen" festgelegt wird. Dort definieren Anwender auch, wie viele monatliche, wöchentliche und tägliche Sicherungen der Home Server aufbewahrt. Abweichend von diesem grundlegenden Plan können im Dialog des Hauptfensters einzelne Sicherungen zur Löschung markiert oder aber gesperrt werden, so dass sie der Server dauerhaft aufbewahrt. Über diesen Dialog lassen sich zudem einzelne Elemente aus einer Sicherung wiederherstellen. Der Home Server führt zu Beginn eine Vollsicherung der Clients durch. Anschließend werden platz- und zeitsparend blockbasiert nur die Änderungen seit dem letzten Backup gesichert. Identische Blöcke verschiedener Clients werden ebenso platzsparend nur einmal gespeichert. Sind im Idealfall beispielsweise zehn weitestgehend identische Vista-Clients zu sichern, belegt die Sicherung der Betriebssysteme nur einmalig Platz auf dem Server.

Unter "Benutzerkonten" verwalten Nutzer die Accounts auf dem Gerät. Die nötigen Eingaben für einen neuen Account beschränken sich auf Vor-, Nach- und Anmeldenamen, Kennwort und Zugriffsrechte auf die Freigaben. Weiterhin ist festzulegen, ob dem neuen Account der Remotezugriff gestattet sein soll. Dahinter verbirgt sich der Zugriff über das Webinterface des Home Servers, welches Up- und Downloads von Dateien ermöglicht sowie als RDP-Proxy über den TCP-Port 4125 den Zugriff auf Client-Computer erlaubt. Über die "Einstellungen" muss dazu zunächst der Remotezugriff aktiviert werden. Im entsprechenden Dialog bietet sich – ein Windows Live-Konto vorausgesetzt – auch die Möglichkeit, den Server unter einer Domäne der Form *meinname.homeserver.com* im Web bekannt zu machen. Alternativ böte sich natürlich auch die Möglichkeit, dies über einen DynDNS-fähigen Router zu bewerkstelligen.

Unter "Freigegebene Ordner" finden sich die ab Werk vorhandenen Standard-Freigaben, wie Fotos, Musik oder Öffentlich. Diese vordefinierten Ordner lassen sich weder verstecken noch löschen. Nutzer können jedoch beliebig weitere Freigaben erstellen. Neben dem Namen und einer optionalen Beschreibung stellt sich dabei die Frage, ob die Ordnerduplizierung aktiviert werden soll – dazu später mehr. Im zweiten Dialogschritt werden die Zugriffsrechte für die Benutzer festgelegt. Dabei stehen lediglich drei Stufen zur Verfügung, nämlich "Vollständig", "Lesezugriff" und "Keine". Rechte können ausschließlich pro Benutzer vergeben werden. Gruppen kennt der Home Server nicht, was bei maximal zehn möglichen Accounts aber zu verschmerzen ist. Per Rechtsklick in die Liste der Ordner findet sich über das Kontextmenü die Aktion "Verlauf anzeigen…", die pro Woche, Monat oder Jahr die Entwicklung des belegten Speicherplatzes in einem Diagramm anzeigt. Dabei werden in dieser Grafik nur die bereits vordefinierten Ordner jeweils mit einer eigenen Farbe dargestellt. Alle manuell erzeugten Freigaben erhalten in dem Diagramm den gleichen Grauton, womit die Übersicht nicht mehr zu deuten ist.

Redundante Datenhaltung

Nun zur Ordnerduplizierung, bei der es sich um ein Konzept zur redundanten Datenhaltung handelt, das weder Hardware- noch Software-RAID nutzt. Stattdessen implementiert Microsoft einen Dienst, der Schreibzugriffe auf die Freigaben im Hintergrund auf beide Festplatten repliziert. Der Vorteil gegenüber einem RAID besteht darin, dass nur die Daten doppelt abgelegt werden, für die dies explizit gewünscht ist. So ist die Ordnerduplizierung für die Freigabe "TV-Aufzeichnungen" standardmäßig deaktiviert, da der Ordner seinem Na-

Maximale Anwenderzahl

Zu beachten ist, dass der Home Server nur maximal zehn Benutzerkonten zulässt und keinen Upgradepfad, beispielsweise zum Small Business Server, bietet. Ist bereits abzusehen, dass mehr als zehn Anwender zu versorgen sind, ist entsprechend eines der "großen" Windows Server-Betriebssysteme oder vielleicht ein Linux-Server die bessere Wahl. Weiterhin ist der Home Server auf den Betrieb innerhalb einer Arbeitsgruppe beschränkt und kann nicht zu einem Active Directory Domain-Controller aufgerüstet werden. Dies bedeutet, dass Benutzeraccounts mit identischem Namen und Passwort auf dem Server und den Clients anzulegen sind, um den Anwendern transparenten Zugriff auf die Freigaben des Servers zu ermöglichen.

Der richtige Server.
Zum richtigen Zeitpunkt.

intel Xeon inside
Leistungsstark.
Intelligent.

UMDENKEN BEIM THEMA SKALIERBARKEIT:

HP ProLiant Technologie der nächsten Generation.

Der HP ProLiant ML330 G6 Server.
Dank seines modularen Designs wächst er mit den Business-Anforderungen. Kombinieren Sie den Server mit Windows® Small Business Server 2008 und Sie erhalten eine All-in-One-Lösung, die sich problemlos an steigende Anforderungen anpassen lässt.

Technologien für Ihren Geschäftserfolg

Windows Small Business Server 2008

Standard Edition Deutsch
Bestell-Nr. 504543-041
530,– Euro inkl. MwSt.*

HP ProLiant ML330 G6
- Intel® Xeon® Prozessor E5504 2,00 GHz
- 2 GB Arbeitsspeicher
- HP Smart Array P410/Zero-Speichercontroller (RAID 0/1/1+0)
- ProLiant Onboard Administrator mit Integrated Lights-Out 2
- 2 x 250 GB 3G SATA 7,2K 3,5" MDL Festplattenlaufwerk

Bestell-Nr. 517607-045
1.119,– Euro inkl. MwSt.*

Weitere Informationen finden Sie unter **www.hp.com/de/einstiegserver**
oder Sie rufen uns an unter **01805 – 66 57 75****

* Unverbindliche Preisempfehlung
** 14 Ct. pro Minute aus dem deutschen Festnetz, Mobilfunk abweichend

hp

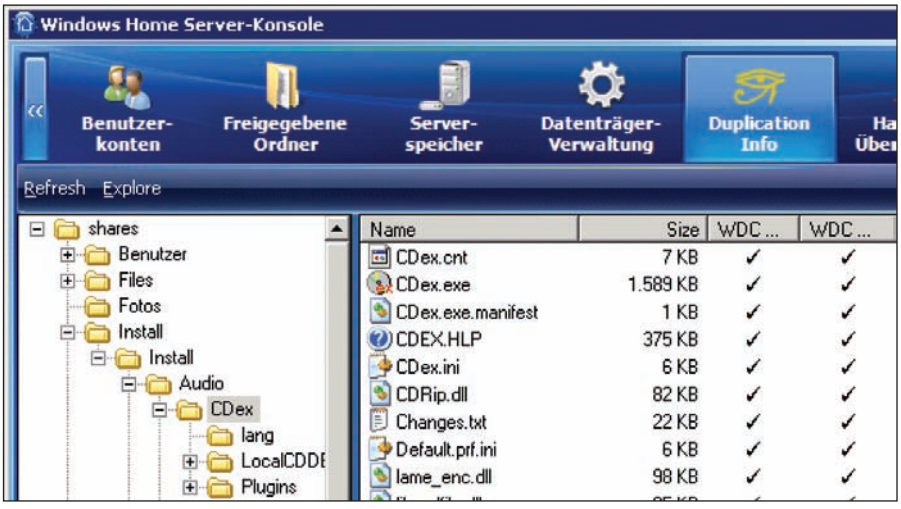


Bild 4: "Duplication Info" zeigt, ob die Ordnerduplizierung funktioniert

men nach in der Regel große Dateien mit geringer Halbwertzeit enthält, die nicht zwingend den doppelten Platz auf dem Server belegen müssen. Ein Nachteil besteht darin, dass das Betriebssystem des Servers selbst nicht von der Duplizierung erfasst wird. Fällt also die Systemplatte aus, ist im Gegensatz zu einem RAID 1 kein nahtloses Weiterarbeiten möglich. Vielmehr muss zunächst das Betriebssystem von der Recovery-CD wiederhergestellt werden, bevor die Daten auf der zweiten Festplatte wieder erreichbar werden. Weiterhin ergibt sich ein Nachteil aus der Tatsache, dass mit Bordmitteln zunächst nicht nachzuvollziehen ist, was die Ordnerduplizierung tut. Im Bereich "Serverspeicher" wird lediglich der globale Status der Festplatten – fehlerfrei oder nicht – angezeigt, der belegte Speicher wird aber nur pauschal und nicht pro Festplatte ausgewiesen. Hier bietet die Erweiterbarkeit des Home Servers Potenzial für Verbesserungen.

Informationen aus erster Hand liefert der Home Server Team-Blog von Microsoft [3], während die deutschsprachigen Home Server-Freunde unter [4] fündig werden. Neben Tipps, Tricks und Leitfäden finden sich im Netz auch zahlreiche, teils kommerzielle, teils frei verfügbare Erweiterungen sowie Add-Ins [5,6]. Für unser Anliegen, mehr über den Zustand der Festplatten und die Ordnerduplizierung zu erfahren, sind die Add-Ins "Windows Home Server Disk Management" sowie "Duplication Info" interessant. Beide können als MSI-Dateien kostenfrei heruntergeladen werden unter [7] und [8]. Werden die Add-Ins in der Standard-Freigabe "\\{home-server}\Software\Add-Ins" abgelegt, so werden sie automatisch in der Home Server Konsole unter "Einstellungen\Add-Ins\Verfügbar" angezeigt und lassen sich mit einem Klick installieren. Anschließend finden sich in der Kopfzeile zwei neue Icons. Unter "Datenträger-Verwaltung" wird nun der Füllgrad der Festplatten einzeln ausgewiesen. Mittels "Duplication Info" können Sie die Verzeichnisstruktur Ihrer Freigaben anzeigen und für die Inhalte einzelner Ordner überprüfen, ob die Datei tatsächlich auf beiden Festplatten vorhanden ist.

Umfangreiche Systemanalyse

Ein weiteres nützliches Tool wird von Fujitsu bereits ab Werk installiert und findet sich im Menü "Einstellungen" der Home Server-Konsole unter "SystemDiagnostics". Wahlweise mittels schnellem oder ausführlichem Test können Nutzer damit die Hardware des Systems auf Herz und Nieren überprüfen. Das Werkzeug lässt sich auch unabhängig von der Home Server-Konsole starten, nämlich über ein Icon auf dem Desktop des Servers. Denn neben der eingeschränkten Sicht der Home Server-Konsole kann sich der Administrator per RDP auch direkt mit dem Desktop des Servers verbinden. Damit besteht die Möglichkeit, über die Funktionalität der Konsole hinauszugehen und beispielsweise über das Software-Applet der Systemsteuerung weitere Windows-Komponenten wie den FTP-Dienst des IIS hinzuzufügen.

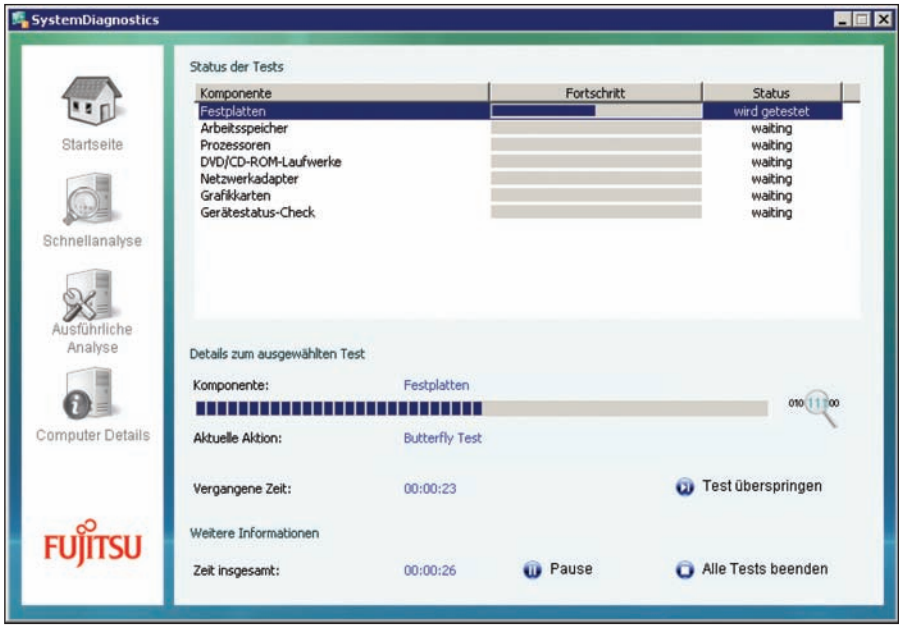


Bild 5: Das Tool "SystemDiagnostics" prüft den Server auf Herz und Nieren

Das komplette Spektrum eines Windows Server 2003 steht damit selbstredend nicht zur Verfügung, denn Komponenten wie Active Directory oder der Terminalserver bleiben außen vor. Der versiertere Administrator erhält aber auf diese Weise zumindest eine ungefilterte Sicht auf das System und kann so bei Bedarf direkt in Ereignisprotokoll oder Systemsteuerung nach dem Rechten sehen. Bei der Frage, was erlaubt ist, helfen in vielen Fällen die Foren weiter. Mindestens zwei Ratschläge sollten Administratoren aber beherzigen: Sie sollten die Benutzeraccounts immer über die Home Server-Konsole verwalten und auf ihre Daten auch lokal auf dem Server immer über die Netzwerkfreigaben zugreifen. Direkte Eingriffe über den Pfad "D:\shares\" könnten die Ordnerduplizierung aus dem Tritt bringen.

Fazit

Entgegen seinem Namen ist der Scaleo Home Server nicht nur für ambitionierte Heimanwender, sondern durchaus auch für kleinere Büros und Unternehmen eine einfach zu bedienende Storage-Lösung, die zudem das Thema Client-Backup gleich mit erledigt. Mit dem Power Pack 3 für den Home Server, das zum Redaktionsschluss noch nicht als finale Version vorlag, hält auch die volle Unterstützung für Windows 7 Einzug. Wer über den werksseitig gebotenen Leistungsumfang hinaus weitere Funktionen benötigt, kann aus einem großen Angebot von Add-Ins wählen und das System auf die eigenen Bedürfnisse anpassen. Lediglich eine Grenze lässt sich nicht aufheben, die Beschränkung auf zehn Benutzer. Und neigt sich der Arbeitstag dem Ende zu, empfiehlt sich der Scaleo Home Server dank der ebenfalls ab Werk integrierten Software "PVConnect" übrigens auch als Medienmanager, der Bild und Ton an die Clients streamt. *(dr)*

Der Autor dieses Artikels, Dipl.-Inform. (FH) Christian Knermann, ist stellvertretender Leiter des IT-Managements am Fraunhofer Institut für Umwelt-, Sicherheits- und Energietechnik UMSICHT in Oberhausen. Zugleich leitet er das Projekt "Competence Center Application Service Providing" der Fraunhofer Gesellschaft.

Produkt
Network Attached Storage (NAS) System für bis zu vier Festplatten.

Hersteller
Fujitsu Technology Solutions, www.fujitsu.com/de/

Preis
Rund 260 bis 300 Euro.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator *(max. 10 Punkte)*

Ein-/Ausbau von Festplatten	9
Bedienbarkeit der Admin-Konsole	8
Stromverbrauch	8
Client-Sicherung	9
Erweiterbarkeit	8

Dieses Produkt eignet sich

optimal für den Einsatz im Home Office und kleineren Büroumgebungen mit homogener Windows-Infrastruktur.

gut für Umgebungen mit maximal zehn Anwendern.

weniger für heterogene Umgebungen und Unternehmen mit mehr als zehn Usern.

Fujitsu Scaleo Home Server 2205

Links

[1] Scaleo Home Server 2205
http://de.ts.fujitsu.com/home/products/home_server/scaleo_homeserver.html

[2] Intel SS4200-E
www.intel.com/design/servers/storage/ss4200e/index.htm

[3] Home Server Team-Blog von Microsoft
http://windowsteamblog.com/blogs/windowshomeserver/default.aspx

[4] Deutschsprachiger Home Server-Blog
www.home-server-blog.de

[5] Deutschsprachige Seite zu WHS-Add-Ins
www.whsaddins.de

[6] Englische Seite zu WHS-Add-Ins
www.whsaddins.com

[7] Windows Home Server Disk Management
www.tentaclesoftware.com/whsdiskmanagement/

[8] Duplication Info
http://akiba.geocities.jp/duplicationinfo/

Im Kurztest: TeamViewer 4.1

Grenzenlose Zusammenarbeit

von Sandro Lucifora

Zusammenarbeit in Unternehmen bedeutet heutzutage nicht nur für Administratoren, komplexe Themen am Computer telefonisch oder per E-Mail erklären zu müssen. Eine optimale Lösung hierfür ist natürlich die Möglichkeit, seinem Gegenüber das Problem oder ein Produkt direkt am Bildschirm zu zeigen. TeamViewer ist eine Software, die Fernwartung, Präsentationen und Zugriffe auf entfernten Windows- und Mac-Computern ermöglicht. Dabei sind Probleme mit geschlossenen Ports in Firewalls passé, denn das Tool nutzt den normalen Weg ins Internet.

Insgesamt besteht die Lösung aus drei Komponenten: Der TeamViewer als Master oder Slave und der Sitzung-Server des Herstellers. Die Software gibt es in unterschiedlichen Funktionspaketen:

- Die All-in-One Vollversion: Sie bietet nach dem Start sowohl die Master- als auch die Slave-Funktion; diese ermöglichen, sich entweder aktiv mit einem Computer zu verbinden oder erlauben den passiven Zugriff.
- Das QuickSupport Kundenmodul muss nicht installiert werden und wird nur als Slave direkt auf dem Computer gestartet; dieses schlanke Programm findet seinen Einsatz im Kundensupport und kann zudem mit einem eigenen Logo und Begrüßungstext gestaltet werden.
- Zusätzlich gibt es noch den TeamViewer Host, der den Zugriff auf unbeaufsichtigte Rechner herstellt: Das Hostmodul läuft als Systemdienst und ermöglicht die Verbindung zum Server, den eigenen PC zu Hause oder beliebige sonstige Systeme – inklusive Login/Logout und Remote-Reboot.

Wenn Sie unterwegs sind, keinen TeamViewer griffbereit haben und unbedingt mal auf einen Computer zugreifen müssen, ist "TeamViewer Web" die Lösung. Hierbei handelt es sich um die TeamViewer-Lösung in HTML und Flash.

Verbindungsaufbau nicht fehlerfrei

Nachdem TeamViewer gestartet wurde, müssen sich die Parteien einigen, welcher Computer Slave und welcher Master ist. Der Slave bekommt automatisch eine Sitzungs-ID und ein Kennwort angezeigt. Diese Daten müssen dem Master mitgeteilt werden. Für die ID und das Kennwort ist der Sitzungs-Server des Herstellers zuständig: Der Slave-Computer "bucht" sich auf diesem Server eine Sitzung. Wenn der Master nun die Sitzungs-ID und das Kennwort des Slave einträgt, können sich beide Software-Komponenten verbinden. Hier hat sich im Test eine einzige Schwäche gezeigt: Wenn der Sitzungs-Server des Herstellers nicht erreichbar ist, kann TeamViewer keine Sitzungen aufbauen; das ist uns im Testzeitraum zwei Mal passiert.

Der Master-Computer legt die Art der Verbindung fest. Zur Auswahl steht die klassische Fernwartung, um zum Beispiel Probleme auf einem entfernten Computer zu beheben oder sich etwas zeigen zu lassen. Der Präsentationsmodus zeigt dem Slave-Computer seinen eigenen Bildschirm. Dazu muss nicht der ganze Desktop gezeigt werden. Es lässt sich auch nur ein einzelnes Fenster zur Übertragung festlegen. Die Dateiübertragung öffnet einen Dateimanager, mit dem Dateien zwischen beiden Computern übertragen werden können. Eine VPN-Verbindung zwischen den Computern ist ebenso möglich. Hierzu muss zuvor der TeamViewer VPN-Adapter auf den Computern installiert sein.

Fazit

TeamViewer bietet eine Menge hilfreicher Funktionen für sein Geld. Nicht nur innerbetriebliche, sondern auch externe Problemfälle und -analysen lassen sich durch die einfache Remote-Bedienung einfacher lösen. Probleme mit geblockten Ports der Firewall existieren nicht mehr. Zudem kann auf verschiedene Computer hinter einer Firewall mit nur einer IP zugegriffen werden; bisher musste für eine Fernwartung der RPC-Port auf den zu wartenden Computer geroutet werden. So war von außerhalb über eine IP der Zugriff auf mehrere Server nicht möglich. Dass der eigene Bildschirm oder gezielte Fenster anderen gezeigt werden können, erleichtert die Zusammenarbeit enorm. *(jp)*

Produkt
Software zur Fernwartung und Zusammenarbeit.

Hersteller
TeamViewer GmbH, www.teamviewer.de

Preis
Für Privatanwender ist TeamViewer kostenlos;
Eine Lifetime-Lizenz ist ab 499 Euro erhältlich.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator *(max. 10 Punkte)*

Umsetzung	8
Handhabung	10
Aufwand der Konfiguration	9
Zuverlässigkeit	8
Kosten/Nutzen	8

TeamViewer 4.1

NETWORK computing AWARDS 2009 – SERVICE MANAGEMENT PRODUCT OF THE YEAR – WINNER

best business AWARDS Winner 2009

PC PRO 2009 AWARDS FINALIST

Desktop Management- und Helpdesk-Software

Effektive Verwaltung und Support für Ihre wichtigsten Anlagegüter

Seit 1989 unterstützen die marktführenden Softwarelösungen von NetSupport zahlreiche Unternehmen bei der Verwaltung und Wartung ihrer IT-Infrastruktur.

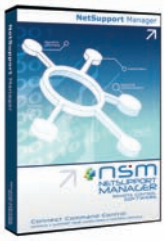
Die für alle relevanten Bereiche perfekt aufeinander abgestimmten Lösungen von NetSupport ermöglichen Ihrem Unternehmen eine noch bessere Nutzung der IT-Kapazitäten.

NetSupports Desktop-Verwaltungs- und Fernwartungssoftware schafft Transparenz über die laufenden IT-Kosten und spart durch deutlich kürzere Supportzeiten bares Geld.

Management der IT-Infrastruktur und Internet-basierender Anwendersupport

Das modular aufgebaute NetSupport DNA ist ein herausragendes System zur Verwaltung von Hardware- und Software-Installationen und bietet ein umfassendes Lizenzmanagement – wichtige Grundlage zur exakten Bedarfsermittlung bei neu anstehenden IT-Investitionen. Die integrierten NetSupport DNA-Komponenten, wie die Überwachung des Energieverbrauchs, den Werkzeugen zur Messung der Software- und Internetnutzung und zur Ferninstallation von Software, sowie ein Internet-basierender Anwendersupport mit fortschrittlichem Ticket-Management, bieten Ihrem Unternehmen ein wertvolles Instrument zur Einsparung von Zeit und Geld.

Weitere Informationen und eine kostenlose Testversion erhalten Sie unter: ***www.netsupportdna.com***



Zukunftsweisende Fernwartung und Desktop-Verwaltung

Durch die Kombination aus modernstem Desktop-Management und einer leistungsfähigen plattformübergreifenden PC-Fernwartungslösung bietet NetSupport Manager heute einen der schnellsten ROIs auf dem Markt. Egal ob Windows, Mac, Linux und mobile Geräte, Fernwartung und interaktive Schulungen oder die gleichzeitige Überwachung und Verwaltung vieler Systeme – mit NetSupport Manager haben Sie alle Herausforderungen sicher im Griff, zuverlässig und schnell über LAN und Internet und ganz ohne umständliche Firewall-Konfigurationen.

Weitere Informationen und eine kostenlose Testversion erhalten Sie unter: ***www.netsupportmanager.com***

Weitere Informationen und eine kostenlose Testversion erhalten Sie unter

www.pci-software.de

PCIS

sales@pci-software.de +49 (0)89 550 508 -10 www.pci-software.de

Netbooks für den Administrator

Mobilität auf kleinstem Raum

von Sandro Lucifora

Mal eben das Passwort eines Users zurücksetzen, den Dienst auf einem Server prüfen oder neu starten, all das gehört zu den nicht planbaren Aufgaben des Administrators. Aber ist es wirklich nötig, am Wochenende vor dem Server zu sitzen, um bei einem Update zuzusehen, oder extra in den Betrieb zu fahren, um einen User anzulegen? Manchmal muss nur Enter gedrückt werden, damit alles weiterläuft. IT-Administrator hat für Sie überprüft, ob das Arbeiten mit einem Netbook für die Administration aus der Ferne praxistauglich ist.

Netbooks sind die neuen mobilen Begleiter: Klein, fein, leicht und mit einer enorm langen Akkulaufzeit – zumindest suggerieren das die Hersteller. Doch welche Möglichkeiten hat ein Administrator, der mit einem mobilen Computer seine IT verwalten will? Um diese Frage zu beantworten, haben wir uns Vertreter dieser Mini-PC-Klasse einmal näher angesehen und geprüft, wie sich deren Einsatz in der Praxis bewährt.

Hersteller wie ASUS, Samsung, Dell und einige mehr bieten unterschiedliche Netbook-Modelle an. Auf den ersten Blick sind die Unterschiede nicht auszumachen. Für Grafikanwendungen und Programmierarbeiten ist ein Netbook definitiv nicht geeignet. Dennoch bewegt sich die Preisspanne zwischen 300 und 700 Euro, teilweise noch höher. Wir können schon vorwegnehmen, dass sich die wirklichen Unterschiede erst auf den zweiten oder gar dritten Blick, und oft erst in der täglichen Arbeit, herausstellen.

Admin-Aufgaben für die Netbooks

Über mehrere Wochen haben wir administrative Arbeiten sowohl lokal als auch von extern mit dem Netbook durchgeführt. Dabei fiel die übliche Fernwartung, Updates auf Servern, Netzwerküberwachung, Rücksicherung von Backups et cetera an. Neben Windows-Servern hatten wir auch Linux-Geräte zu administrieren. Entsprechende Hilfsmittel und Tools wurden auf den Netbooks installiert und eingerichtet. Um auch unterwegs per E-Mail erreichbar zu sein, haben wir zudem Outlook als auch den David-Client über das Netbook betrieben.

Im Laufe der Zeit kristallisierten sich die Vorzüge und Nachteile der Netbooks für die Arbeiten des Administrators heraus und boten ein gemischtes Bild. Grundsätzlich ist zu sagen, dass es immer besser ist, ein Netbook mit den wichtigsten Tools unterwegs dabei zu haben, als seinen Urlaub oder freien Tag abzubrechen oder nachts in die Firma fahren zu müssen. Es ist nicht immer eine Freude, auf das kleine Gerät zu schauen, bietet jedoch eine neue Freiheit.

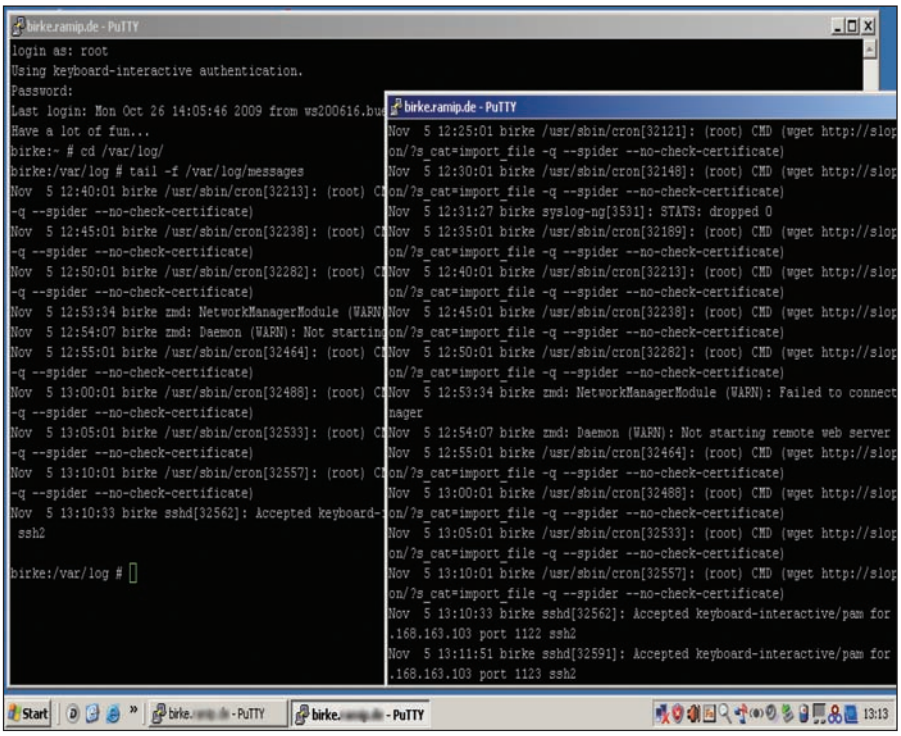
Um das Netbook überhaupt erst einmal betriebsbereit zu haben, muss der Administrator die erste Hürde des nicht vorhandenen optischen Laufwerks überwinden. Hier bieten die Geräte von Medion und Dell den großen Vorteil, über ein DVD-Laufwerk zu verfügen. Doch ob es sich lohnt, stets das Laufwerk mitzuschleppen, ist fraglich. Wenn das Netbook über kein CD/DVD-Laufwerk verfügt, ist die Alternative, ein im Netzwerk gemountetes Laufwerk zu nutzen oder sich ein USB-Laufwerk ins Regal zu stellen.

Grenzen der Netbooks

Mit das größte Manko ist das installierte Betriebssystem. Netbooks werden fast ausschließlich mit einer Windows Home-Edition ausgeliefert. Wir können davon ausgehen, dass ein Administrator im Umfeld eines Domänen-Netzwerks arbeitet. Bis auf das Vostro von Dell ist jedoch keines der vorgestellten Netbooks mit einer Windows Professional-Version erhältlich. Da mit den mitgelieferten Home-Versionen keine Domänen-Anmeldung möglich ist, bedeutet dies, mit Workarounds zu arbeiten oder das Netbook mit der gewünschten Professional-Lizenz neu zu installieren.

Die derzeit gängige Auflösung der Displays ist 1.024 x 600 Pixel. Um eine E-Mail zu lesen oder kurz remote einen Blick auf den Server zu werfen, reicht das aus. Doch im Test hat sich gezeigt, dass schon das Arbeiten mit zwei geöffneten SSH-Fenstern nebeneinander nicht praktikabel ist. Bei einer Remote-Verbindung konnten wir recht gut arbeiten, wenn das Fenster der RPC-Sitzung beim Öffnen auf maximal 1.000 x 550 Pixel eingestellt wird – ansonsten muss immer gescrollt werden.

Da meistens gerade dann keine Internetverbindung über WLAN verfügbar ist, wenn sie gebraucht wird, lohnt sich in jedem Fall der Einsatz eines Netbooks mit einem eingebauten UMTS-Modul. Alle Mobilfunk-Provider bieten ein solches Gerät zu einem günstigen Preis inklusive Vertrag an. Haben Sie ein Netbook ins



Mit einer Auflösung von 1.024 x 576 ist das Arbeiten schon möglich, wird nach einer längeren Zeit aber anstrengend

Auge gefasst, das nicht mit einem 3G-Modul oder nur mit einem Laufzeitvertrag erhältlich ist, bietet sich als gute Alternative ein USB-Surfstick an, die relativ günstig angeboten werden. Der Vorteil ist, dass die Internetnutzung nach tatsächlicher Zeit abgerechnet wird.

Fazit

Als Testergebnis lässt sich festhalten, dass ein Netbook für Administratoren in jedem Fall eine gute Ergänzung zum Arbeitsplatzrechner ist. Störend ist schon, dass die Auflösung relativ gering ist, was jedoch die logische Schlussfolgerung angesichts der Gesamtgröße ist. Wir können auf 10 Zoll nicht den Komfort eines 24-Zoll-Monitors erwarten. Ein Netbook bietet unterwegs für die administrativen Aufgaben eine neue mobile Freiheit. Die Leistung der üblichen Atom-CPUs reicht dabei aus, um die gängigsten Tools einzusetzen. Der Arbeitsspeicher sollte mindestens 2 GByte groß sein, da dann auch ein Groupware-Client recht schnell startet und sich große Logdateien flüssig betrachten lassen. VPN-Verbindungen, wie im Test zu einem LANCOM- und Netgear-Router, sind mit den dazugehörigen Clients problemlos möglich.

Um nicht allzu viele Kompromisse bei der Benutzung eingehen zu müssen, empfehlen wir ein Netbook zu wählen, das mindestens eine WXVGA-Auflösung mit 1.366 x 768 Pixeln anbietet. Das daraus resultierende größere Gehäuse hat den positiven Nebeneffekt, dass auch die Tastatur mitwächst. Für die absolute Freiheit ist ein UMTS-Modul erforderlich. Da das Angebot der Netbooks am Markt mit diesem Zusatz begrenzt und dann meist an teure Laufzeitverträge geknebelt ist, greifen Sie am besten zu einem USB-Surfstick. Der Prozessor beeinflusst auch die Laufzeit des Akkus, daher ist eine Atom-CPU die erste Wahl.

Wenn Sie in Ihrem Netzwerk einen Domänencontroller einsetzen, kalkulieren Sie bei der Anschaffung eine Windows Professional-Lizenz mit ein – denn mit den Home-Editionen ist zwar auch die Arbeit im Domänen-Netzwerk möglich, doch artet das eher zu einem Krampf als zu einem sinnvollen Arbeiten aus, sobald Sie auf Netzwerkressourcen zurückgreifen wollen. *(jp)*

	Eee PC 1005 HGo	Eee PC 1101 HA	N 140-anyNet N270 BNBT21
Hersteller	ASUS	ASUS	Samsung
Web	www.eee-pc.de	www.eee-pc.de	www.samsung.de
Gewicht	1.270 Gramm	1.380 Gramm	1.270 Gramm
Mobilfunk	GSM Quadband	Nein	Nein
Connectivity	UMTS / HSDPA / HSUPA	Nein	Nein
Kommunikation	Bluetooth, WLAN b/g, Ethernet 10/100 MBit/s	Bluetooth, WLAN b/g/n, Ethernet 10/100 MBit/s	Bluetooth, WLAN b/g/n, Ethernet 10/100 MBit/s
Schnittstellen	3x USB 2.0, 1x VGA Out, 1x Audio in, 1x Audio Out, RJ-45, Card Reader	3 x USB 2.0, 1 x VGA Out, 1 x Audio in, 1 x Audio Out, RJ-45, Card Reader	3 x USB 2.0 (1 x mit Ladefunktion), 1 x VGA Out, 1 x Audio in, 1 x Audio Out, RJ-45, Card Reader
Webcam	0,3 Megapixel	0,3 Megapixel	0,3 Megapixel
Prozessor	1,66 GHz Intel Atom N280	1,33 GHz Intel Atom Z520	1,6 GHz Intel Atom N270
Speicher	1024 MByte	2048 MByte	1024 MByte
Festplatte	160 GByte	250 GByte	160 GByte
Display	10,1" WSVGA	11,6" WXVGA	10,1" WSVGA
Auflösung	1.024 x 600	1.366 x 768	1.024 x 600
Betriebssystem	Microsoft Windows XP Home	Microsoft Windows 7 Home Premium	Microsoft Windows XP Home
Besonderheit	–	LED Backlight, ASUS WebStorage: 500GB	SuperBright Matt LED Backlight Display; Festplatten-Passwortschutz
Beschreibung	Der Eee PC 1005 HGo ist das einzige Netbook im Test, das derzeit nur mit einem Mobilfunkvertrag erhältlich ist. Das GSM Quadband-Modul bietet auch netzwerkunabhängigen Zugriff auf die Daten im Unternehmen. Die Einschränkungen der geringen Auflösung haben wir im Artikel erläutert. Die Webcam reicht aus, um hier und da eine Videotelefonie via Skype durchzuführen. Die Akkulaufzeit konnte mit knapp 7 Stunden – ohne eingeschaltetes WLAN- und GSM-Modul – überzeugen.	Der Eee PC 1101 HA lässt derzeit ein GSM-Modul vermissen, würde es dieses Netbook doch zum unabhängigen Wegbegleiter machen. Mit 11,6" und WXVGA 1.366 x 768 bietet das Netbook den besten Kompromiss zwischen Displaygröße und Auflösung. Mit knapp 400 Euro, 2 GByte Arbeitsspeicher und einer 250 GByte Festplatte fehlt dem 1101 HA für unsere Zwecke nichts. Der kostenlose Eee PC-WebStore ist eine gute Möglichkeit, wichtige Daten für Dritte oder sich selber im Netz zwischenzuspeichern.	Das Samsung N 140 ist mit einer Akkulaufzeit von knappen 11 Stunden – ohne eingeschaltetes WLAN-Modul – das Gerät mit der längsten Ausdauer. Der Festplatten-Passwortschutz schützt die Daten, sollte das Netbook in falsche Hände geraten. Das Display ist sehr gut entspiegelt, nur ist die WSVGA-Auflösung eine Bremse für die halbwegs gute Arbeit. Das preiswerteste Gerät im Vergleich bietet mit der Samsung Recovery Solution III eine individuell einstellbare Wiederherstellung. Es hat sich gezeigt, dass dies sehr hilfreich ist, um nach einer problematischen Softwareinstallation oder einem Update das System problemlos wiederherzustellen.
Preis mit Mobilfunkvertrag	T-Mobile: 4,95 Euro inkl. MwSt.	–	–
Netto-Preis	–	335 Euro	293 Euro

	X 120	AKOYA E3211	Vostro 1220
Hersteller	LG	Medion	Dell
Web	www.lge.com/de/	www.medion.de	www.dell.de
Gewicht	1.260 Gramm	1.700 Gramm	1.520 Gramm
Mobilfunk	3G HSDPA Modul	Nein	Nein
Connectivity	UMTS / HSDPA / HSUPA	Nein	Nein
Kommunikation	Bluetooth, WLAN b/g, Ethernet 10/100 MBit/s	WLAN b/g, Ethernet 10/100/1000 MBit/s	Bluetooth, WLAN b/g/n, Ethernet 10/100 MBit/s
Schnittstellen	3 x USB 2.0, 1 x VGA Out, 1 x Audio in, 1 x Audio Out, RJ-45, Card Reader	3 x USB 2.0, 1 x VGA Out, 1 x Audio in, 1 x Audio Out, RJ-45, Card Reader	3 x USB 2.0, 1 x VGA Out, 1 x Audio in, 1 x Audio Out, RJ-45, Card Reader
Webcam	1,3 Megapixel	1,3 Megapixel	Nein
Prozessor	1,6 GHz Intel Atom N270	1,2 GHz Intel Celeron 723	2,2 GHz Intel Core 2 Duo T6670
Speicher	1024 MByte	2048 MByte	4096 MByte
Festplatte	160 GByte	500 GByte	250 GByte
Display	10,1" WSVGA	13,3" WXVGA	12,2" WXGA
Auflösung	1.024 x 576	1.366 x 768	1.280 x 800
Betriebssystem	Microsoft Windows XP Home	Windows Vista Home Premium	Windows 7 Professional (32 Bit)
Besonderheit	–	Integrierter 8x Multi-Standard DVD-/CD-Brenner mit DVD-RAM und Dual-Layer Unterstützung	Integrierter 8x Multi-Standard DVD-/CD-Brenner
Beschreibung	Das LG X 120 ist das Fliegengewicht und bietet mit seinem 3G-Modul (UMTS) mobile Freiheit par excellence. Unabhängig von Netzwerken können damit auch auf der grünen Wiese administrative Arbeiten erledigt werden. Doch auch hier stört die relativ geringe Auflösung. Für die Akkulaufzeit konnten wir, auch hier ohne eingeschaltetes WLAN- und GSM-Modul, gute sechseinhalb Stunden stoppen.	Die Grenzen zwischen Netbook und Notebook sind ineinander fließend. Mit 13,3" ist das Medion AKOYA E3211 ein Wanderer zwischen den Grenzen und bietet bei einem zwei Zoll größeren Display die selbe gute WXVGA-Auflösung wie der Eee PC 1101. Das einzige Gerät mit Windows Vista setzt auf einen Intel Pentium Ultra Low Voltage-Prozessor und liefert eine entsprechend höhere Wärmeentwicklung wie die Atom-Prozessoren. Dass die Pentium-Klasse, auch mit Ultra Low Voltage, nicht zu den ausdauernsten Geräten gehört, zeigt die vergleichsweise geringste Akkulaufzeit von unter vier Stunden. Der DVD-Brenner tut sein Übriges für das Schwergewicht im Vergleich.	Das Vostro 1220 von Dell liefert auf 12,2" und WXGA das Mittelmaß in der Auflösung. Die Ausstattung ist üppig: Mit 4.096 MByte Arbeitsspeicher und einer 250 MByte Festplatte ist für Administratoren Leistung satt vorhanden. Der 2.2 GHz Intel Core 2 Duo-Prozessor ist hier nur, ebenso wie bei dem Medion-Gerät, ein unnötiger Stromfresser. Da sich bei Dell alle Geräte individuell zusammenstellen lassen, wäre es wünschenswert, wenn wir auf einen DVD-Brenner verzichten könnten. Das teuerste Gerät in der Übersicht ist auch das einzige, dass eine Windows-Professional-Version hat und somit der Domänen-Login im Netzwerk problemlos möglich ist.
Preis mit Mobilfunkvertrag	–	–	–
Netto-Preis	419 Euro mit, 335 Euro ohne HSDPA-Modul	461 Euro	544 Euro

VPN-Tunnel zu Windows-PCs mit freeSSHd

Marke Eigenbau

von Christian Knermann

Der Weg zur sicheren Kommunikation mit dem Unternehmensnetz besteht meist darin, auf dem entfernten Host die Remote-Software eines Drittanbieters einzusetzen oder einen VPN-fähigen Router mit separater Authentifizierung vorzuschalten. Beides erfordert aber in der Regel die Installation einer zusätzlichen Software-Komponente auf dem Client. Dieser Workshop zeigt auf, wie Sie mit dem frei verfügbaren SSH-Server freeSSHd einen durch öffentliche und private Schlüssel abgesicherten Zugriff auf Windows-Systeme in Eigenregie realisieren.

Neben der Server-Software freeSSHd [1] ist auf der Client-Seite lediglich der ebenfalls frei verfügbare Telnet- und SSH-Dienst PuTTY [2] erforderlich, der nicht installiert werden muss und sich so beispielsweise auch von einem USB-Stick starten lässt. Für unseren Workshop verwendeten wir freeSSHd in der Version 1.2.4, die wir auf einem Windows 7 System installierten.


Quelle: Karl-Heinz Laube – pixelio.de

Flinke Installation

Das Setup des Dienstes ist denkbar schnell erledigt. Der Assistent fragt zunächst nach dem Installationspfad. Wir akzeptierten den Standard "C:\Program Files\freeSSHd". Im nächsten Schritt bietet sich scheinbar die Gelegenheit, die zu installierenden Komponenten auszuwählen. Es handelt sich dabei jedoch offensichtlich um eine rhetorische Frage, denn beim Expandieren des Dropdown-Feldes zeigt sich, dass mit der "Full Installation" genau ein Eintrag angeboten wird. Dies machte uns die Wahl entsprechend einfach. Der nächste Dialog gilt dem gewünschten Startmenü-Ordner. Wir beließen es auch hier beim Standard "freeSSHd". Der Assistent fasst die gewählten Optionen noch einmal zusammen, woraufhin mit einem Klick auf "Install" eben dieser Prozess beginnt. Im Verlauf der Installation bietet die Setup-Routine an, RSA-/DAS-Schlüssel für den SSH-Server zu erzeugen, was wir mit "Ja" bestätigten. Ebenso stimmten wir der Frage zu, ob FreeSSHd als Systemdienst eingerichtet werden soll.

Damit ist die Installation abgeschlossen. Ein Blick in die Computerverwaltung zeigt anschließend, dass der Dienst "FreeSSHDService" mit dem Starttyp "Automatisch" eingerichtet und bereits

Kurze Schlüssel

Die Schlüssel, die während der Installation automatisch erzeugt werden, sind lediglich 1.024 Bit lang. Möchten Sie stattdessen für höhere Sicherheit 2.048 Bit lange Schlüssel verwenden, können Sie nach der Installation über die Einstellungen des Dienstes neue generieren.

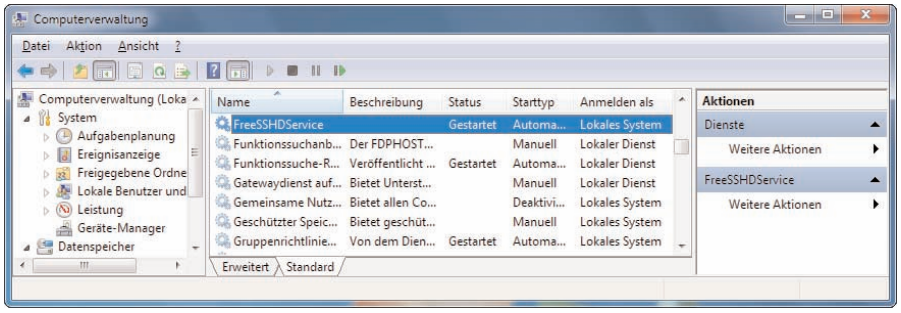


Bild 1: freeSSHd registriert sich als Systemdienst

erfolgreich gestartet wurde. Verbindungen zum Server sind allerdings an diesem Punkt noch nicht möglich. Dazu ist der Dienst zunächst zu konfigurieren. Der erste Schritt hierzu führt in die Konfiguration der Windows Firewall, wo der TCP-Port 22 freizugeben ist. Dies geschieht unter Windows XP und Vista jeweils auf der Registerkarte "Ausnahmen" der Firewall-Einstellungen. In den Einstellungen der im Funktionsumfang deutlich umfangreicheren Firewall von Windows 7 ist der entsprechende Eintrag in den erweiterten Einstellungen unter "Eingehende Regeln" vorzunehmen.

Basiskonfiguration

Starten Sie anschließend die Konfiguration von freeSSHd über das gleichnamige Desktop-Icon. Das freeSSHd-Symbol verankert sich daraufhin im Systemtray der Startleiste. Rufen Sie mit einem Rechtsklick auf dieses Symbol die "Settings…" auf. Die erste Registerkarte der Konfiguration mit dem Titel "Server status" könnte sogleich Verwirrung stiften, vermeldet sie doch unter Windows 7 im Gegensatz zur vorherigen Ansicht der Computerverwaltung, dass sowohl Telnet- als auch SSH-Server nicht in Betrieb seien. Diese Meldung ist jedoch insoweit missverständlich, als sich die Anzeige lediglich auf den Status der Dienste bezieht, soweit diese interaktiv im Kontext des angemeldeten Benutzers gestartet werden. Dass der Server bereits im Hintergrund als Systemdienst läuft, findet hier schlicht keine Berücksichtigung. Versuchen Sie, den SSH-Server manuell zu starten, wird dies entsprechend mit einer Fehlermeldung quittiert, dass der Port bereits in Benutzung sei.

Insbesondere wenn Sie Windows 7 als Host einsetzen, sollte der erste Schritt darin bestehen, auf der Registerkarte "Automatic updates" sowohl die Option "Show info messages…" als auch "Check for new version…" zu deaktivieren. Hintergrund ist, dass der im Systemkontext laufende Dienst ansonsten versucht, Meldungen in der Session des angemeldeten Benutzers anzuzeigen. Dies erfolgt aber unter Windows 7 auf einem separaten, privilegierten Desktop und rief in unserem Testaufbau als unschönen Nebeneffekt den Abbruch von RDP-Sitzungen hervor. Eine weitere Möglichkeit, dem Dienst dieses Verhalten abzugewöhnen, finden Sie in den Eigenschaften des Dienstes in der Computerverwaltung. Deaktivieren Sie dazu dort auf der Registerkarte "Anmelden" die Option "Datenaustausch zwischen Dienst und Desktop zulassen".

SSH-Verbindung vorbereiten

Zu einem ersten Test der SSH-Verbindung fehlt nun nur noch ein Account, den Sie im Konfigurationsprogramm von freeSSHd auf der Registerkarte "Users" über die Schaltfläche "Add" anlegen können. Tragen Sie den gewünschten Benutzernamen im Feld "Login" ein und wählen Sie eine Art der Authentifizierung aus der Dropdown-Box darunter. Zur Wahl stehen NT-Anmeldung, Passwort oder öffentlicher Schlüssel. Im ersten Fall muss der Login mit dem Namen des Windows-Benutzers übereinstimmen. Erzeugen Sie hier beispielsweise einen Benutzer mit Passwort und aktivieren Sie unter "User can use:" die Shell. Verlassen Sie anschließend den Dialog, übernehmen Sie die Änderungen mit der gleichnamigen Schaltfäche und beenden Sie die freeSSHd-Konfiguration. Der "FreeSSHDService" verlangt nun noch nach einem Neustart über die Computerverwaltung, bevor die geänderte Konfiguration aktiv ist.

Mittels PuTTY (*putty.exe*) können Sie nun Verbindung zum freeSSHd-Host aufnehmen. Beim Erstkontakt werden Sie aufgefordert, den RSA-Schlüssel des Hosts zu bestätigen, den Sie mit "Ja" permanent speichern können. Geben Sie nun Namen und Passwort des zuvor erzeugten Benutzers ein, so erhalten Sie eine Kommandozeile im Verzeichnis "C:\WINDOWS\system32". Damit funktioniert der verschlüsselte Zugriff via SSH bereits. Die

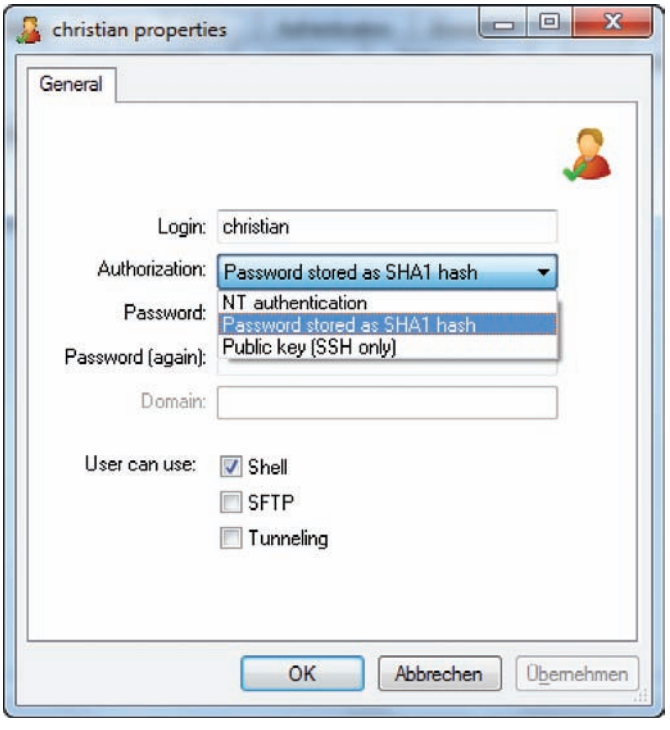


Bild 2: freeSSHd verfügt über eine eigene Benutzerverwaltung

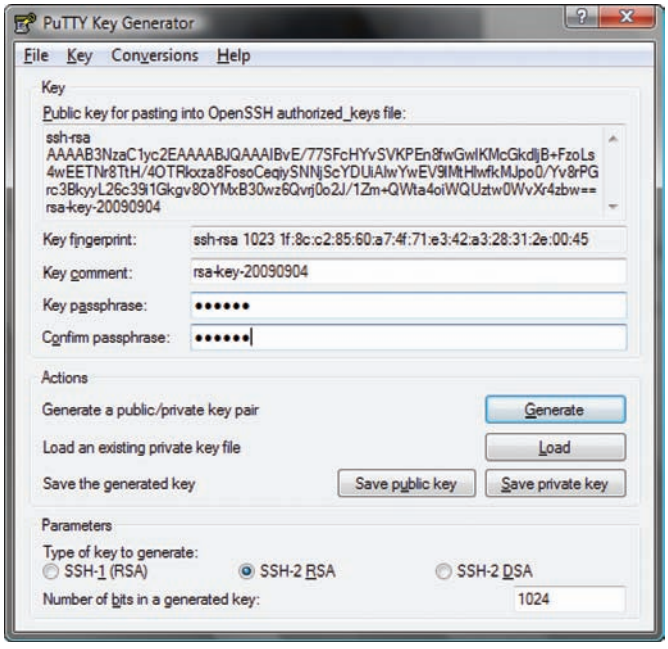


Bild 3: Der PuTTY Key Generator erzeugt öffentliche und private Schlüssel

Anmeldung erfolgt aber nach wie vor per Passwort und der Befehl *whoami* enthüllt, dass die Kommandozeile noch dazu im Kontext des freeSSHd-Dienstes, also des Systemkontos, läuft.

Schlüsselverteilung

Widmen wir uns zunächst der ersten Aufgabe, indem wir die Anmeldung auf ein Paar, bestehend aus öffentlichem und privatem Schlüssel, umstellen. Dies bewerkstelligen Sie mit dem PuTTY Key Generator (*puttygen.exe*) über die Schaltfläche "Generate". Der Generator fordert Sie auf, durch willkürliche Mausbewegungen ein Zufallsmuster zu erzeugen, aus dem schließlich das Schlüsselpaar generiert wird. Vergeben Sie eine Passphrase und speichern Sie den privaten Schlüssel über die Schaltfläche "Save private key". Schlüssel und Passphrase werden später auf dem Client benötigt, um die Verbindung herzustellen und sind entsprechend sicher aufzubewahren. Der öffentliche Schlüssel wird auf dem Server hinterlegt und ist in diesem Fall eigentlich das Schloss, das mit dem privaten Schlüssel geöffnet wird, um einen bildlichen Vergleich zu bemühen. Speichern Sie den öffentlichen Schlüssel nun jedoch nicht über die Schaltfläche "Save public key". Dies würde in einem für unseren Anwendungsfall unpassenden Dateiformat resultieren. Markieren Sie stattdessen den kompletten Inhalt des mit "Public key for pasting into OpenSSH" betitelten Feldes. Kopieren Sie den Key anschließend über die Zwischenablage in eine Textdatei, die Sie mit dem Namen des SSH-Benutzers ohne Dateiendung abspeichern.

Legen Sie die Datei anschließend auf dem Server, beispielsweise im Verzeichnis "C:\Programme\freeSSHd\keys", ab und konfigurieren Sie diesen Pfad in den Einstellungen des freeSSHd-Dienstes auf der Registerkarte "Authentication" als "Pu-

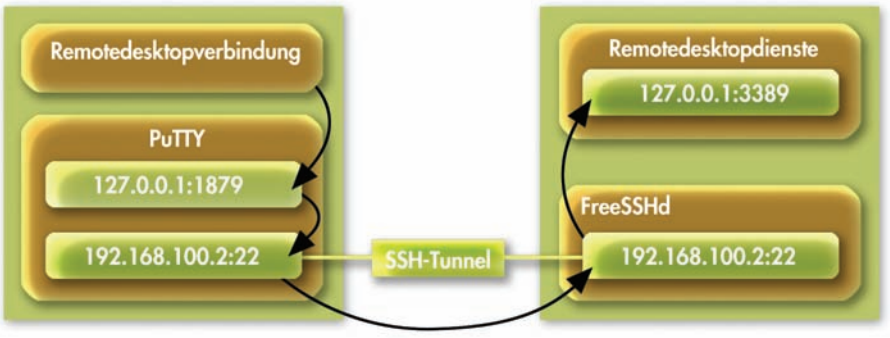


Bild 4: freeSSHd und PuTTY verbinden RDP-Server und -Client mittels SSH

blic key folder". Ändern Sie zudem die Passwort-Anmeldung auf "Disabled" und die Anmeldung per öffentlichem Schlüssel auf "Required". Wechseln Sie daraufhin die Art der Anmeldung für den Testbenutzer von "Password…" auf "Public Key (SSH only)" und starten Sie den Dienst neu. Weiter geht es auf dem Client, wo Sie PuTTY starten und unter "Connection\SSH\Auth" den privaten Schlüssel laden. Bauen Sie nun die Verbindung zum freeSSHd Server auf, werden Sie zur Eingabe der Passphrase aufgefordert, woraufhin Sie wiederum Zugriff auf die Kommandozeile erhalten. Diese ist aber auf einem Windows-System von geringem Nutzwert und birgt zudem großes Potenzial, das System zu beschädigen, da das zu Grunde liegende Systemkonto über umfassende Zugriffsrechte verfügt.

Tunnelbau

Rufen Sie daher erneut die Konfiguration des freeSSHd-Dienstes auf und aktivieren Sie auf der Registerkarte "Tunneling" die Option "Allow local port forwarding", gefolgt von der Option darunter, die Zugriffe auf die lokale Loopback-Adresse des Servers beschränkt. Dies reicht für unser Vorhaben aus. Ändern Sie anschließend die Eigenschaften des Testbenutzers, indem Sie die Shell deaktivieren und stattdessen als einzige Option auch dort das "Tunneling" aktivieren. Serverseitig haben wir damit nach dem obligatorischen Neustart des Dienstes die Voraussetzungen geschaffen, um lokale Ports des Servers durch die SSH-Verbindung zu tunneln und somit vom Client verschlüsselt darauf zuzugreifen.

Dies erfordert nun nur noch eine entsprechende Einstellung im SSH-Client. Laden Sie dazu in PuTTY zunächst erneut unter "Connection\SSH\Auth" den privaten Schlüssel des Benutzers. Den Zugriff auf Ports des Servers konfigurieren Sie daraufhin unter "Connection\SSH\Tunnels". Geben Sie unter "Source port" einen beliebigen, ungenutzten Port auf dem Client ein, in diesem Beispiel 1879. Verwenden Sie als Ziel die Adresse "127.0.0.1:3389" und übernehmen Sie den neuen Tunnel mittels "Add". Dieser verweist nun nicht, wie zu vermuten wäre, auf die lokale Loopback-Adresse des Clients. Die Adresse 127.0.0.1 wird vielmehr erst am entfernten Ende des SSH-Tunnels aufgelöst und bezieht sich somit auf den Server, der wiederum auf dem TCP-Port 3389 auf RDP-Verbindungen wartet. Somit verbindet der auf diese Weise konfigurierte Tunnel den RDP-Port des Servers mit dem lokalen TCP-Port 1879 des Clients.

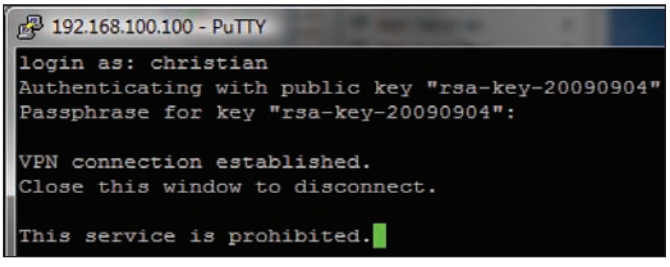


Bild 5: Die Shell ist deaktiviert. PuTTY dient nur noch als Hilfsmittel für den SSH-Tunnel

Tragen Sie abschließend den Namen des Zielhosts ein, vergeben Sie einen Namen für die Sitzung unter "Saved Sessions", um zukünftig einfach auf die Einstellungen zurückgreifen zu können, und speichern Sie die Konfiguration mittels "Save" ab. Stellen Sie nun die Verbindung her, begrüßt Sie nach Eingabe der Passphrase nicht die Kommandozeile, sondern lediglich der Hinweis "This service is prohibited". Dieser Hinweis bezieht sich selbstredend nur auf den Shell-Zugriff. Der SSH-Tunnel wurde im Hintergrund etabliert und besteht, solange das PuTTY-Fenster geöffnet bleibt. Um auf diesen Sachverhalt hinzuweisen, bietet es sich an, in der Konfiguration des freeSSHd-Dienstes auf der Registerkarte "SSH" eine Textdatei mit einem entsprechenden Hinweis als "Banner message" zu konfigurieren, die wiederum nach einem Neustart des Dienstes im PuTTY-Fenster angezeigt wird.

Ist nun auf diese Weise die verschlüsselte SSH-Verbindung zum Zielhost etabliert und der entfernte RDP-Server mit dem lokalen Port verbunden, können Sie über die Remotedesktopverbindung auf dem Umweg über die Adresse "localhost:1879" Verbindung zum entfernten System aufnehmen. Nach der üblichen Windows-Anmeldung steht Ihnen der Desktop des Zielsystems in gewohnter Weise zur Verfügung. Auch das Verbinden lokaler Laufwerke und somit der Datenaustausch funktionieren. So gerüstet können Sie Ihr System nun unbesorgt auf dem TCP-Port 22 freigeben. Wer nicht über einen passenden privaten Schlüssel sowie die zugehörige Passphrase zu einem auf dem Server hinterlegten öffentlichen Schlüssel verfügt, bleibt außen vor. *(dr)*

Links

[1] Webseite zu freeSSHd
www.freesshd.com

[2] PuTTY-Download
www.chiark.greenend.org.uk/~sgtatham/putty/download.html

CompTIA-Studie:

IT-Profis setzen auf Security-Zertifizierungen

Eine aktuelle Studie des IT-Branchenverbandes CompTIA zeigt, dass Zertifizierungen im Bereich IT-Sicherheit der Renner unter den Weiterbildungsangeboten für IT-Profis bleiben: 37 Prozent der Befragten gaben an, in den nächsten fünf Jahren eine Sicherheits-Zertifizierung absolvieren zu wollen. Im selben Zeitraum streben 18 Prozent eine Zertifizierung zum Ethical Hacking und weitere 13 Prozent eine Zertifizierung im Bereich der digitalen Forensik an.

„Die IT-Sicherheit gewinnt angesichts der ständig gravierender und gefährlicher werdenden Angriffe sowie der Tatsache, dass kein Unternehmen vor diesen Angriffen gefeit ist, stetig an Bedeutung. Vor diesem Hintergrund ist der Entschluss, sich im Bereich der IT-Sicherheit weiter zu qualifizieren, ein sinnvoller und karrierefördernder Schritt", erklärt Bodo Vander, CompTIA Regional Director Deutschland, Österreich und der Schweiz.

Weit hinter den Zertifizierungen für die IT-Security rangieren die weiteren Qualifizierungsziele: So wollen sich die Befragten vorzugsweise in den Bereichen Green-IT (7%), Healthcare-IT (5%), mobile IT (5%) und Software-as-a-Service (2%) weiterbilden und zertifizieren lassen.

Die Motivation: höheres Gehalt und Karrieresprung

Die Hauptbeweggründe für den Erwerb einer Zertifizierung sind zum einen wirtschaftliche Erwägungen und zum anderen der Wunsch nach weiteren Schritten auf der Karriereleiter: 88 Prozent der Zertifizierungsinhaber geben an, eine Zertifizierung absolviert zu haben, um das Einkommen zu erhöhen. Ebenfalls 88 Prozent berichten, dass sie ihre Karrierechancen durch die Zertifizierung verbessern wollen.

IT-Profis nehmen Weiterbildung selbst in die Hand

Auffallend ist, dass die IT-Profis die Verantwortung für ihre Karriere selbst übernehmen. 50 Prozent gaben an, ihre Zertifizierung aus eigenen finanziellen Mitteln bestritten zu haben, bei 38 Prozent hat der Arbeitgeber zumindest unterstützt. Doch die IT-Profis sind nicht nur bereit, eigene finanzielle Mittel in die Weiterbildung zu stecken, sondern auch Freizeit: Im Durchschnitt verbringen Kandidaten 44,5 Stunden mit der Vorbereitung auf eine Zertifizierung. Rund jeder Dritte investiert sogar 60 Stunden und mehr. Die IT-Profis scheinen zu wissen, wofür sie diese „Opfer" bringen: 74 Prozent der befragten Zertifizierungsinhaber geben an, zufrieden oder sogar sehr zufrieden mit ihrem Job zu sein.

CompTIA (www.comptia.de):
Die Computing Technology Industry Association (CompTIA) ist das Sprachrohr der IT-Industrie. Zu den Mitgliedern des weltweit aktiven Verbandes zählen IT-Unternehmen und andere Branchenangehörige aus insgesamt 102 Nationen. Ziel von CompTIA ist die Förderung des weltweiten Wachstums der IT-Branche.

Zu den wichtigsten Aufgaben von CompTIA zählt die weltweit standardisierte Aus- und Weiterbildung von IT-Fachkräften. Hierfür hat CompTIA herstellerneutrale Zertifizierungen entwickelt. Diese bestätigen IT-Professionals nach international anerkannten Standards grundlegende IT-Kenntnisse zu Spezialgebieten wie PC-Support, IT-Sicherheit, Projektmanagement oder Netzwerk-Administration.

Die wichtigsten CompTIA-Zertifizierungen im Überblick:
CompTIA A+ (PC-Support)
CompTIA Network+
CompTIA Security+
CompTIA Server+
CompTIA CTT+ (Certified Technical Trainer)
CompTIA Project+ (Projektmanagement)
CompTIA PDI+ (Druck- und Kopiersysteme)
CompTIA CDIA+ (Dokumenten-Management)

Bodo Vander, Regional Director Deutschland, Österreich und der Schweiz bei CompTIA

Fit in Sachen IT-Sicherheit? Knowhow jetzt online testen!
Wer sein Security-Wissen testen möchte, kann dies bis Ende Dezember auf der Seite **http://www.it-administrator.de/comptia** tun. Dort gibt es einen Fragenkatalog, der an die Prüfungsfragen der herstellerneutralen Zertifizierung CompTIA Security+ angelehnt ist. Prüfen Sie, ob Ihr Wissen für das Erreichen der herstellerneutralen und weltweit anerkannten Zertifizierung ausreichen könnte!

Promotion-Aktion für Leser der it-administrator:
Die Leser der it-administrator können die CompTIA-Zertifizierungen CompTIA Security+, A+, Network+, Server+, PDI+, Project+ oder Linux+ mit 20 Prozent Rabatt auf den offiziellen Standardpreis absolvieren. Hierfür müssen sich die Leser bis zum 31.12.2009 entweder vor Ort in einem von VUE oder Prometric autorisierten Testcenter oder online unter www.vue.com oder www.prometric.com unter Angabe des Promotion-Code „ITAD09" für eine der Prüfungen registrieren. Das Angebot gilt für Testcenter in Deutschland, Österreich und der Schweiz und kann für mehrere Prüfungen in Anspruch genommen werden.

Exchange Server 2007

Mailversand im Namen anderer

von Robert Lindermeier

Immer wieder werden Exchange-Administratoren beauftragt, jemandem Zugriff auf das Postfach eines anderen Benutzers zu gewähren. Auf die Gründe hierfür, wie etwa Vertretung, Krankheit oder Ausscheiden eines Mitarbeiters, sowie die datenschutzrechtlichen Aspekte wollen wir an dieser Stelle nicht näher eingehen. Die Vergabe dieser Berechtigung an sich mag für den geübten Administrator unter Exchange 2007 kein Problem sein. Jedoch im Nachhinein die Send As- und Receive As-Berechtigungen im Überblick zu behalten, ist schon weitaus schwieriger.

Grundsätzlich ist die Verwaltung dieser Berechtigungen sowohl in der Exchange Managementkonsole als auch über die Verwaltungsshell möglich. Die zugehörigen Cmdlets sind *Add-MailboxPermission* und *Remove-MailboxPermission*. Über den entsprechenden Parameter "-AccessRights {FullAccess, SendAs,…}" kann das Recht vergeben oder entzogen werden. Um beispielsweise Send-As-Berechtigungen auf das Postfach ROBERTL für den User MARIAS zu vergeben, nutzen Sie den Befehl

```
Add-MailboxPermission -Identity
  robertl -AccessRights SendAs
  -User MARIAS
```

Mit dem folgenden Kommando entziehen Sie die Send-As-Berechtigungen auf das Postfach ROBERTL für den User MARIAS dagegen:

```
Remove-MailboxPermission -Identity
  robertl -AccessRights SendAs
  -User MARIAS
```

In diesem Workshop nutzen wir die Exchange Management-Shell, um alle Postfächer aufzulisten, bei denen diese speziellen Berechtigungen gesetzt wurden. Damit haben wir eine einfache Möglichkeit, eine aktuelle Liste zu führen und gegebenenfalls festzustellen, an welcher Stelle die eigentlich vorübergehend gedachten Berechtigungen noch gesetzt sind, um diese wieder zurückzusetzen.

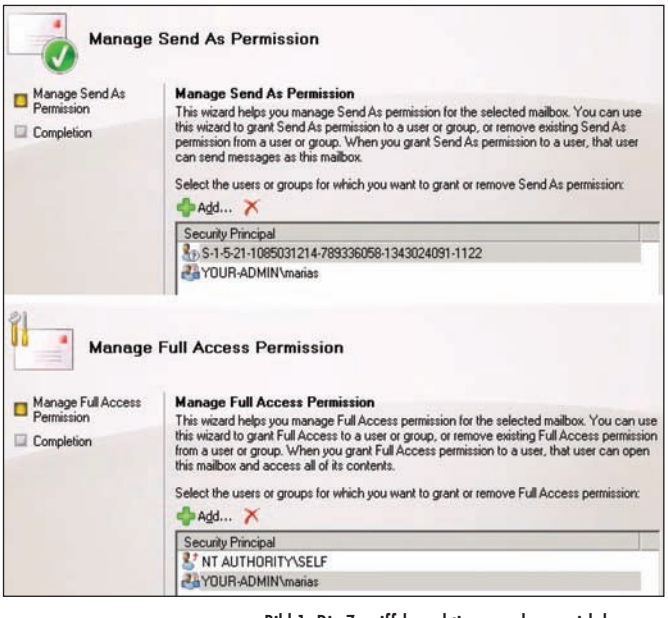


Bild 1: Die Zugriffsberechtigungen lassen sich bequem in der Exchange-Managementkonsole über einen Wizard einrichten

Dabei kommen folgende Exchange Management Shell-Commandlets zum Einsatz: *get-mailbox, get-ADPermission, where, ft*

Um nun alle Postfächer auszulesen, bei denen Sie Send-As-Berechtigungen gesetzt haben, geben Sie den Befehl

```
Get-Mailbox | Get-ADPermission |
  where {($_.ExtendedRights -like
  "*Send-As*")} | ft -Wrap
```

ein. Das Kommando *Get-Mailbox* gibt dabei eine Liste der aktuellen Postfächer auf dem Server aus. Möchten Sie hier nicht den lokalen Server abfragen, können Sie mit dem Parameter '-Server "{servername}"' explizit den Mailbox-Server abfragen.

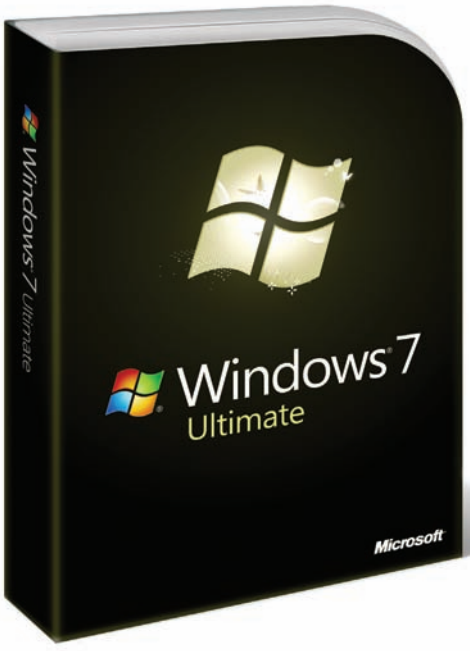
Der Befehl *Get-ADPermission* listet daneben alle Berechtigungen auf, die im AD zu dem betreffenden Postfach gespeichert sind, während *where* die Ausgabe filtert und nur die Zeilen ausgibt, bei denen ein Send-As eingetragen ist.

Da in der nun vorliegenden Liste auch die vererbten Berechtigungen und das SELF-Konto ausgegeben werden, bauen wir nun einen zusätzlichen Filter ein.

```
Get-Mailbox | Get-ADPermission |
  where {($_.ExtendedRights -like
  "*Send-As*") -and ($_.IsInherited
  -eq $false) -and -not ($_.User
  -like "NT AUTHORITY\SELF")} | ft
  -Wrap
```

Wenn Sie nun diese Liste in eine Datei ausgeben oder mit Hilfe des cmdlet *Export-CSV* eine CSV-Datei schreiben lassen, dann stehen Ihnen alle Möglichkeiten der professionellen Weiterverarbeitung zur Verfügung. *(dr)*

Robert Lindermeier ist Inhaber und Senior Consultant bei Your-Admin e.K.



Neuerungen in Windows 7

Hasta la Vista

von Dirk Srocke

Mit Windows 7 will Microsoft einen würdigen Vista-Nachfolger präsentieren. Anwender lockt das System mit hübscher GUI und besserer Performance; Administratoren dürften sich besonders für ausgefeilte Systemtools, VPN-Funktionen und die eng mit Windows 2008 R2 verzahnten Managementfeatures des Betriebssystems interessieren. IT-Administrator zeigt Ihnen, welche Neuerungen der Vista-Nachfolger mitbringt.

Evolution statt Revolution: Während Microsoft mit dem XP-Nachfolger Vista grundlegend an Kernel und Treiberarchitektur von Windows gefeilt hat, fällt der Versionssprung zu Windows 7 moderat aus. Wie auch Server 2008 R2 setzt das Betriebssystem auf der von Server 2008 und Vista bekannten Architektur auf. Netter Nebeneffekt: Sicherheitsupdates können gemeinsam für Clients und Server genutzt werden. Die Vista-nahe Architektur schlägt sich auch in der Versionierung nieder: Windows 7 gibt sich als Windows NT 6.1 aus. Der kleine Schritt wurde von Microsoft bewusst gewählt, um die Kompatibilität zu bestehenden Anwendungen zu gewährleisten und Versionskontrollen nicht zu verwirren. Letzte Sicherheit in Kompatibilitätsfragen soll das für Windows 7 angepasste Application Compatibility Toolkit [1] geben. Verglichen zum Vista-Check ist lediglich eine neue Prüfung hinzugekommen: Aufrufe zu Outlook Express. Auch Vista-Treiber sollten in aller Regel problemlos mit Windows 7 funktionieren – nach Microsoft-Lesart allerdings deutlich zuverlässiger und performanter.

Migrationshilfe für XP-Programme und -Daten

Als Migrationshilfe für XP-Umsteiger bietet Microsoft den XP-Mode an. Die für kleine und mittelständische Unternehmen gedachte Funktion ist als separater Download erhältlich und beinhaltet Windows Virtual PC. XP-Programme laufen dann in der virtuellen Umgebung nicht nur unter Windows 7, sondern werden auch in die Benutzeroberfläche des Wirtssystems integriert. Für Updates von XP und Vista gleichermaßen interessant ist das User State Migration Tool 4.0 (USMT). Mit dem Programm lassen sich Daten auf einem Netzwerk-Share sichern und auf Windows 7 zurückmappen.

Geschonte Ressourcen und höhere Energieeffizienz

Glaubt man Microsoft, geht Windows 7 um einiges schonender mit dem vorhandenen Arbeitsspeicher im System um. So habe bereits die Betaversion des Systems zwischen zehn und 30 Prozent weniger Arbeitsspeicher benötigt als der Vorgänger mit Service Pack 1. Damit eignet sich das System auch für schmalbrüstigere Hardware, wie aktuelle Netbooks. Die mobilen Geräte dürften auch von den erweiterten Stromsparfunktionen von Windows 7 profitieren. Microsoft hat den Befehl *powercfg* um den Parameter "/energy" erweitert. Die Option untersucht den Rechner über einen Zeitraum von 60 Sekunden und gibt einen per Browser darstellbaren "Energieeffizienzdiagnose-Bericht" aus.

Dort finden Sie Hinweise auf Konfigurationsfehler, die die Laufzeit eines batteriebetriebenen Systems verringern. Zudem gibt das Tool Informationen zur aktuellen Leistungsfähigkeit – und damit auch zur noch verbleibenden Lebensdauer – des verwendeten Akkus. Zudem listet die Analyse USB-Treiber auf, die verhindern, dass ohne Last laufende PCs in den Energiesparmodus (Suspend-Mode) wechseln.

Die verbesserten Energiesparfunktionen sind freilich nicht Microsofts Killerargument für den Umstieg auf Windows 7. Der Hersteller hat das Clientbetriebssystem zudem mit nützlichen Tools aufgewertet und eng mit dem ebenfalls neu veröffentlichten Serverbetriebssystem Windows 2008 R2 verzahnt.

VPN und Remote-Management

Im Zusammenspiel mit Windows Server 2008 R2 bietet Windows 7 etwa die Funktion DirectAccess an. Damit können mobile Endanwender zum einen auf das eigene Firmennetz zugreifen. Die Verbindung per Virtual Private Network (VPN) erfolgt dabei verschlüsselt und über beliebige Internet-Zugänge. Für Anwender geschieht das vollkommen transparent und nahtlos – das Aufrufen dedizierter Dialer entfällt.

DirectAccess ermöglicht es IT-Administratoren zudem, Systeme zu warten, wenn diese nicht direkt mit dem Unternehmensnetz verbunden sind. Somit lassen sich auch auf entfernten Notebooks Sicherheitspatches

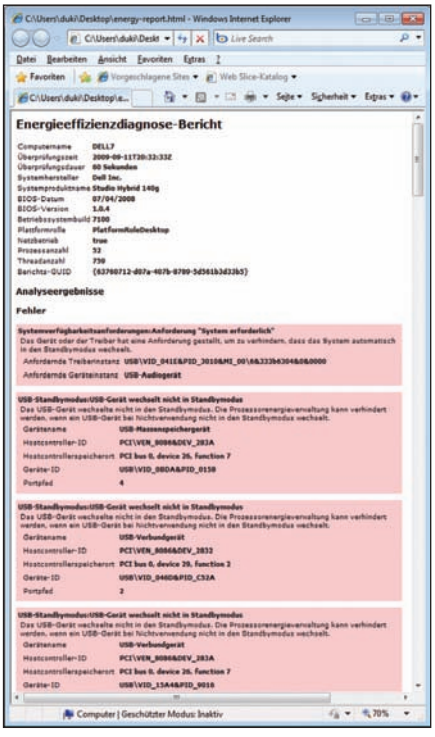


Bild 1: Der Energieeffizienzdiagnose-Bericht lässt sich per Webbrowser darstellen und zeigt, wie das untersuchte System effizienter mit Strom haushalten könnte

einspielen. Gleiches gilt für veränderte Konfigurationseinstellungen oder Gruppenrichtlinien. Dabei können Sie unterscheiden, ob sich Systeme aktuell im Unternehmensnetz befinden oder von außerhalb darauf zugegriffen wird. Remote agierende Rechner haben dabei beispielsweise direkten Zugang zum Internet, ohne unnötig über das Firmennetz geschleust werden zu müssen. DirectAccess funktioniert ausschließlich mit Windows 7, eine Rückportierung auf Vista ist nicht geplant. Voraussetzung ist zudem R2 des Windows Server 2008 sowie eine Implementierung von IPSec und IPv6. Als Verbindung eignet sich jedoch auch das herkömmliche Internet mit IPv4, da DirectAccess Daten per Tunnel transferieren kann.

Gesparte Bandbreite dank BranchCache

Mit BranchCache bieten Windows 7 und Server 2008 R2 eine weitere Funktion für Rechner außerhalb der Firmenzentrale an. Die Funktion soll niedrige WAN-Bandbreiten besser ausnutzen und redundante Datenübertragungen vermeiden. Von File- oder Webservern angeforderte Daten erhalten bei BranchCache einen Hashwert. Wird ein Dokument mehrmals per Wide Area Network angefordert, muss es lediglich einmal in die Zweigstelle übertragen werden. Bei größeren Installationen liefert ein zentraler Cache in der Zweigstelle dann die jeweilige Datei aus. In übersichtlicheren Infrastrukturen hingegen agieren verschiedene Windows-7-Systeme in einem Peer-to-Peer-Netz und tauschen Informationen untereinander aus. BranchCache baut auf Ende-zu-Ende-Verbindungen und unterstützt somit per SSL oder IPSec geschützte Kommunikationskanäle. Im Gegensatz zur bloßen Replizierung von Daten soll BranchCache die Koexistenz konkurrierender Dateiversionen verhindern.

Gemeinsam mit Windows 2008 R2 soll Windows 7 auch die Leistung von Virtual Desktop Infrastructures (VDI) steigern. Per Remote Desktop Protocol (RDP) lassen sich jetzt auch multimediale Inhalte mit akzeptabler Latenz und Geschwindigkeit übertragen, etwa Audio-Daten, Videos oder die Aero-GUI. Die beinahe erreichte "Full Fidelity Experience" mit Multi-Monitor-Support und Microphone Remoting ist nicht nur bloße Spielerei, sondern etwa für Callcenter interessant. Die können jetzt auf eine zentralisierte Desktop-Infrastruktur zugreifen, ohne auf Telefonie-Anwendungen auf den Clients verzichten zu müssen.

Management und Rollout

Mit Windows 7 will Microsoft das Management und die Verwaltung herkömmlicher Desktops weiter vereinfachen. Ein Weg hierzu ist etwa das Booten von Virtual Hard Disk (VHD). Damit lassen sich Images zentral und offline pflegen. Individuelle Einstellungen können per Differenz-VHD gestartet werden. Für die Pflege und Wartung stellen die Redmonder mit Windows 7 ein per "dism" aufrufbares Tool vor. DISM steht für "Deployment Image Servicing and Management" und wartet sowohl VHD- als auch WIM-Files (Windows Imaging Format Archive). Mit dem Werkzeug stellen Sie Systemabbilder bereit oder entfernen diese wieder. Zudem können Sie damit Windows-Features ein- oder ausschalten. Treiber und Pakete lassen sich mit "dism" aufzählen, hinzufügen oder entfernen.

Für einen beschleunigten Rollout sollen die aktualisierten Windows Deployment Services (WDS) sorgen. So hat Microsoft die Multicast-Funktion der Bereitstellungsdienste optimiert. Im Zusammenspiel mit Server 2008 R2 lassen sich Daten mit verschiedenen Geschwindigkeiten übertragen. Damit bestimmt nicht mehr der langsamste Client im Netz die maximale Geschwindigkeit beim Ausliefern von Daten. Mit Windows 7 stellen Sie Treiber darüber hinaus dynamisch bereit (Dynamic Driver Provisioning). Die Reduzierung der Treiber auf einzelnen Rechnern soll auch die Zahl möglicher Konflikte verringern.

Tools für Systemsicherung und Prozessanalyse

Einen besonderen Blick sind die mit Windows 7 ausgelieferten Systemwerkzeuge wert. So erlaubt das Betriebssystem jetzt nicht nur das Datenbackup, sondern bietet auch das Erstellen von Systemabbildern auf Festplatte, Netzwerkverzeichnis oder optischem Datenträger an. Der bereits mit Vista eingeführte Ressourcenmonitor wurde mit Features des Sysinternals-Tools aufgewertet. Nutzer können das Werkzeug direkt per Kommando *resmon* starten oder im Task-Manager unter dem Tab "Leis-

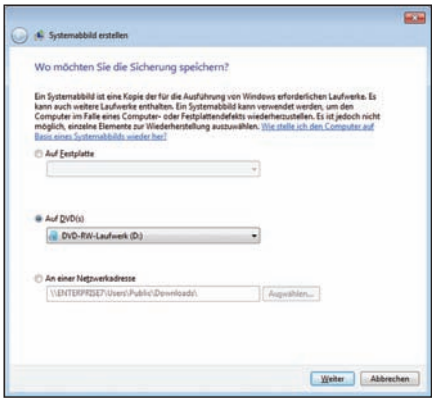


Bild 2: Mit Windows 7 können Anwender mit Bordmitteln ein Systemabbild ihres Rechners anfertigen

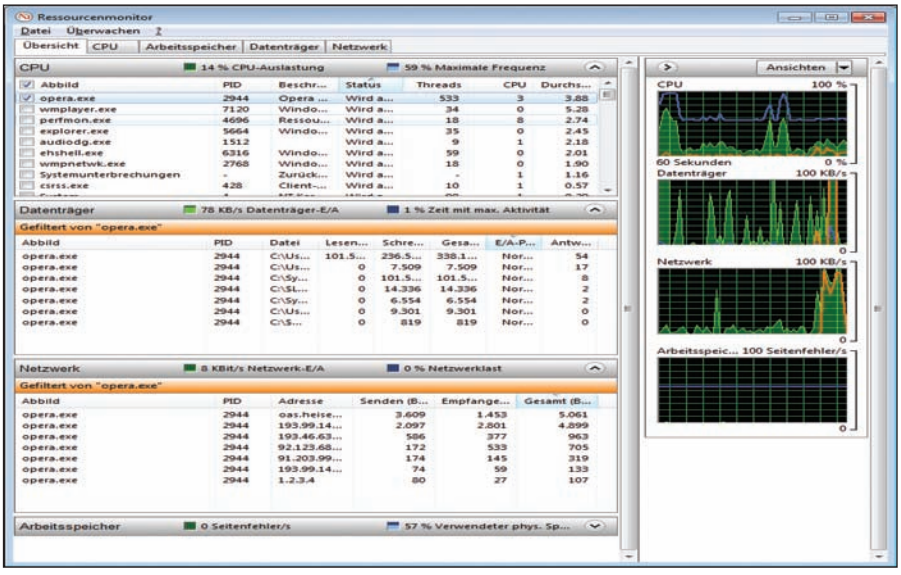


Bild 3: Microsoft hat den Ressourcenmonitor mit Windows 7 deutlich erweitert und Sysinternals-Tools eingebaut. Damit lassen sich Prozesse gezielt herausfiltern und beobachten.

tung" aufrufen. Die im Tab "Übersicht" integrierten "Process Monitor Features" erlauben beispielsweise, Prozesse gezielt zu filtern. Anwender wählen per Checkbox eine Anwendung von Interesse, der Ressourcenmonitor zeigt daraufhin Datenträger- und Netzwerkaktivitäten der jeweiligen Routine an.

Auf Karteikarte "CPU" beantwortet der Unterpunkt "zugeordnete Handles" die Frage nach geöffneten Dateien. Unter "Netzwerk" präsentiert sich der Ressourcen Monitor jetzt zudem als Alternative zum Kommandozeilenbefehl *netstat* und zeigt aktuelle TCP-Verbindungen und Überwachungsports – auch wieder per Checkbox filterbar.

Problemaufzeichnung erleichtert Helpdesk-Support

Für Supportanfragen beinhaltet Windows 7 den Kommandozeilenbefehl *psr*. Der "Problem Steps Recorder" – zu Deutsch "Problemaufzeichnung" – wird vom Endnutzer gestartet und zeichnet den Verlauf problematischer Applikationen auf. Das Werkzeug speichert Screenshots, Mausklicks sowie Bemerkungen des Anwenders in einer Zip-komprimierten MHT-Datei. Das Log kann dann direkt an den Helpdesk weitergeleitet werden. Per Webbrowser können Supportbeauftragte somit direkt nachvollziehen, bei welchem Programmpunkt Probleme aufgetreten sind.

Powershell mit GUI inklusive

Im Paket mit Windows 7 liefert Microsoft erstmals auch die Skriptumgebung PowerShell serienmäßig. Die aktuelle Version 2.0 ist wie gehabt als Befehlszeilenumgebung verfügbar und hilft, Routineaufgaben zu automatisieren. Einsteiger können jetzt jedoch auch mit einer grafisch aufbereiteten, intuitiven Benutzeroberfläche mit Editor und Debugger arbeiten. Die PowerShell 2.0 unterstützt aktuell zwei Arten des Remotings: Verwaltungsskripte lassen sich einerseits von einer Quelle an viele Ziele übermitteln (Fan-Out). Eine interaktive 1-zu-1-Remoteverbindung soll zudem die Problembehandlung für einzelne Rechner erleichtern.

Im Zusammenspiel mit der als Download angebotenen Gruppenrichtlinien-Verwaltungskonsole erleichtert die PowerShell 2.0 das Verwalten von Gruppenrichtlinienobjekten. Administratoren können das Gespann außerdem dazu nutzen, um registrierungsbasierte Gruppenrichtlinieneinstellungen zu erstellen oder zu bearbeiten.

Management und Sicherheit mit AppLocker

Die von Vista bekannten Richtlinien für Softwareeinschränkung (Software Restriction Policies) sind in Windows 7 nur noch aus Kompatibilitätsgründen vorhanden. Micrsosoft hat das Konzept mit AppLocker ersetzt. Systemverantwortliche können mit der Funktion unerwünschte Programme per Blacklist gezielt für festgelegte Einzelnutzer oder Anwendergruppen blockieren. Optional ist auch die Definition von Whitelists für erwünschte Applikationen möglich. Die Einstellung ist dabei sehr granular möglich. Anwendungen lassen sich auf mehrere Arten identifizieren. Bei signierten Anwendungen sollten Sie dabei die Option "Herausgeber" vorziehen. Mit dieser lassen sich etwa Regeln der folgenden Art definieren: alle Opera-Browser ab Version 10 mit dem Dateinamen *opera.exe*. Das schließt damit auch Updates ein und verringert den administrativen Aufwand bei der Pflege von Richtlinien.

Nicht signierte Anwendungen lassen sich einerseits per Pfad identifizieren, dabei sind

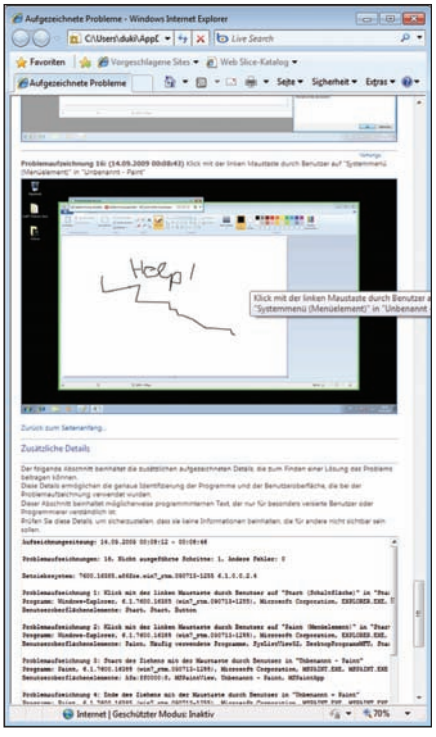


Bild 4: Die per "psr" aufrufbare Problemaufzeichnung unterstützt Supportabfragen mit einem grafisch aufbereiteten Log

jedoch Manipulationen durch das Kopieren von Dateien möglich. Die Option "Dateihash" umgeht dieses Risiko um den Preis eines höheren Wartungsaufwandes beim Einspielen von Updates. AppLocker ist über den lokalen Gruppenrichtlinien-Editor (*gpedit.msc*) verfügbar. Damit der Mechanismus funktioniert, muss der Service "Anwendungsidentität" laufen.

Verschlüsselung mit BitLocker To Go

Mit "BitLocker To Go" erweitert Microsoft das eigene Schutzwerkzeug gegen Datendiebstahl und -offenlegung. Die Verschlüsselungslösung lässt sich mit Windows 7 auch ohne Neupartionierung von Laufwerken nutzen. Damit können auch unbedarftere Anwender Daten auf mobilen Speicherlösungen, wie USB-Sticks oder portablen Festplatten, vor Datendieben schützen – ein Klick mit der rechten Maustaste genügt. Administratoren steuern mit "BitLocker To Go" außerdem, wie Wechselmedien in der jeweiligen Umgebung verwendet werden sollen und welche Schutzebene vorgeschrieben wird. So kann beispielsweise eine Verschlüsselung als zwingende Voraussetzung für einen Schreibzugriff auf mobile Datenträger festgeschrieben werden. Über Richtlinien können IT-Verantwortliche zudem geeignete Passwörter, Smartcards oder Anmeldeinformationen für Domänenbenutzer einfordern.

Mit "BitLocker To Go" verschlüsselte Daten lassen sich auch nach Verlust des Passworts wiederherstellen. Einzelanwender können hierfür den entsprechenden Wiederherstellungsschlüssel als Text speichern. In größeren Infrastrukturen kann der Wiederherstellungscode auch ins Active Directory eingebunden werden. Autorisierte Administratoren haben damit die Möglichkeit, verschlüsselte Daten jederzeit einzusehen. Auf die mit BitLocker chiffrierten, mobilen Datenträger ist dabei auch unter älteren Windows-Versionen der Zugriff möglich. Windows 7 speichert das hierzu nötige Tool automatisch auf den jeweiligen Datenträger. Der Komfort lässt allerdings noch ein wenig zu wünschen übrig: Ist Autorun aktiviert, startet das Leseprogramm zwar automatisch, die angezeigten Daten müssen jedoch erst auf das Zielsystem kopiert werden, bevor Anwender damit arbeiten können.

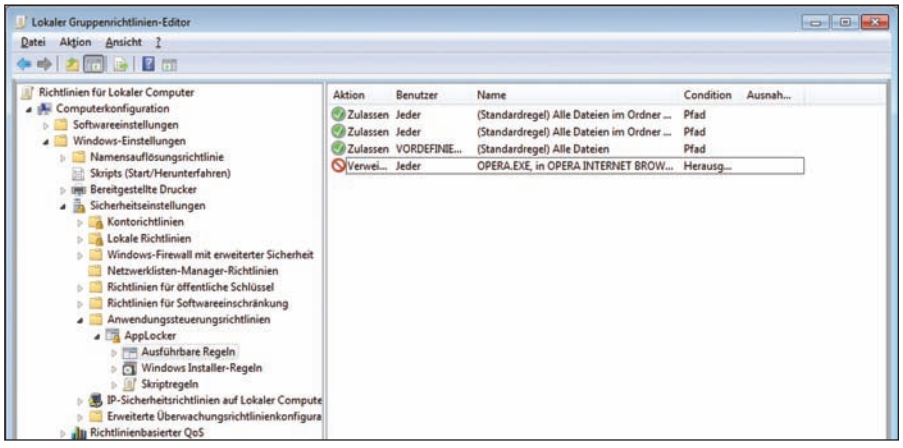


Bild 5: Mit AppLocker können Administratoren den Zugriff auf ungewünschte Anwendungen reglementieren. Windows 7 verweigert dann die Ausführung.

Überholte Taskleiste und prozessorientierte Benutzerführung

Mit Windows 7 hat Microsoft das Interface grundlegend überholt. Die Taskleiste ist zwar geblieben, nimmt nun aber deutlich mehr Raum ein und wurde umstrukturiert. Eine klassische Ansicht existiert jetzt nicht mehr und die klare Trennung zwischen den Icons für Schnellstart und laufende Programme wurde aufgehoben. Stattdessen lassen sich die Symbole beliebig anordnen. Ein rechter Mausklick auf die Symbole liefert jetzt so genannte "Jumplists" und damit Verweise auf die zuletzt von der jeweiligen Anwendung verwendeten Dokumente. Ein Verweilen des Mauszeigers auf der Taskleiste zeigt eine Miniaturansicht des geöffneten Programms. Bewegen Sie den Cursor hierauf, präsentiert Windows 7 eine komplette Voransicht. Fenster lassen sich jetzt besonders einfach für Breitbildschirme gruppieren: Ziehen Sie ein Fenster zu einer Bildschirmseite, nimmt die Anwendung genau die Hälfte des Bildschirms ein. Ein Ziehen des Fensters zum oberen Bildschirmrand führt zur Vollbilddarstellung. Die beschriebenen Reaktionen lassen sich auch per Shortcut mit Windows-Taste und Cursorblock provozieren. Klicken Sie auf die Titelleiste einer Anwendung und schütteln das Fenster per Mausbewegung, schließen sich alle anderen Fenster. Zudem ist Windows 7 für Touchscreens vorbereitet.

Preise und Verfügbarkeit

Windows 7 ist seit dem 22. Oktober im Handel verfügbar. Microsoft bietet das Betriebssystem wie üblich in verschiedenen Ausführungen an. Für den professionellen Einsatz kommen die Versionen Professional respektive Ultimate und Enterprise in Frage. Letztgenannte sind funktional identisch und unterscheiden sich voneinander lediglich in der Art und Weise der Lizenzierung. Die Enterprise-Version ist für Volumenlizenzkunden mit Software Assurance erhältlich und kann über unternehmenseigene KMS-Server aktiviert werden. Die im Artikel beschriebenen Funktionen BranchCache, DirectAccess, BitLocker, AppLocker sowie das Booten von VHD sind nur bei Enterprise/Ultimate verfügbar. Als Endkundenpreis für die Vollversion Windows 7 Ultimate nennt Microsoft 319 Euro. *(dr)*

Links

[1] Application Compatibility Toolkit
www.microsoft.com/downloads/details.aspx?FamilyId=24DA89E9-B581-47B0-B45E-492DD6DA2971&displaylang=en

WLAN-Netze in Unternehmen

Gesicherte Unabhängigkeit

von Thomas Bär

Wenn im deutschsprachigen Raum von WLAN gesprochen wird, ist zumeist ein lokales Funknetz gemäß dem Standard IEEE-802.11 gemeint. In anderen Ländern, insbesondere den USA, ist der Ausdruck "Wi-Fi" üblich. Ob WLAN oder Wi-Fi, Funknetzwerke als Ergänzung oder genereller Ersatz für kabelgebundene Netzwerke erfreuen sich sehr hoher Beliebtheit. Kommen WLANs in Unternehmen zum Einsatz, so gilt es, die Spezifikationen und Sicherheitsanforderungen im Überblick zu behalten. Ein zentrales Management erleichtert der Administration zudem die Bereitstellung. Wir erklären in diesem Artikel die technischen Grundlagen von Funknetzwerken und sagen Ihnen, worauf Sie beim Aufbau eines WLANs achten sollten.

Der Siegeszug des WLANs im privaten und heimischen Umfeld begann mit dem Angebot der meisten Internet-Provider, im Paket einen Router mit einer Funknetzwerkunterstützung anzubieten. Innerhalb weniger Jahre haben die WLANs in vielen Privathaushalten das traditionelle CAT-Kabel ersetzt. Gründe für den Einsatz gibt es sehr viele, und kaum jemand möchte auf die Annehmlichkeiten der freien Sitzplatzwahl mit dem Laptop verzichten.

Nicht selten kommt es in Unternehmen zu teils heftigen Debatten, warum am Arbeitsplatz kein Funknetzwerk eingeführt wird, was den Einsatz von Laptops deutlich vereinfachen würde. Es mag den vom heimischen Funknetz verwöhnten Benutzern unverständlich vorkommen, doch zu einem Unternehmenseinsatz gehört weit mehr als der Anschluss von Fritzbox und Co.

Besonders vor dem Hintergrund der jüngsten 802.11n-Freigabe durch das IEEE stieg das Interesse an WLAN noch einmal deutlich an, da Funknetzwerke erstmalig die magische 100 MBit-Fast-Ethernet-Grenze überwanden. Für den IT-Verantwortlichen ergeben sich für einen robusten Betrieb von Funknetzwerken in Unternehmen als Alternative zum Netzwerkkabel vier grundsätzliche Themenfelder: Zum einen sind grundlegende Aspekte kabelloser Übertragungstechniken zu beachten. Weiterhin muss das Ziel sein, eine größtmögliche Geschwindigkeit zu realisieren. Zudem gilt es gerade bei Funknetzwerken, eine größtmögliche Sicherheit zu garantieren. Letztendlich sollte sich ein solches Netzwerk natürlich effektiv administrieren lassen.

Betriebsmodi und Geschwindigkeiten

Funknetzwerke lassen sich prinzipiell in drei unterschiedlichen Ausprägungen nutzen. Im so genannten "Ad-Hoc-Modus" sind alle beteiligten Geräte gleichwertig, ohne dass einem Gerät eine zentrale Aufgabe zufällt. Gemäß dem Standard 802.11 können in einem Ad-Hoc-Netzwerk maximal zwei Gesprächspartner mit einer Geschwindigkeit von 11 MBit/s Daten austauschen. Durch den Einsatz zusätzlicher Protokolle, wie OSLR (Optimized Link State Routing), lässt sich die Anzahl auf maximal acht Teilnehmer erhöhen. Alle Teilnehmer in einem Ad-Hoc-Netzwerk sehen sich gegenseitig.

In dem deutlich erweiterten "Infrastruktur-Modus" übernimmt ein Access Point (AP) als zentrale Stelle die Organisation der über ihn in Verbindung stehenden Endgeräte. Werden Informationen zwischen Endgerät A und Endgerät B im Infrastruktur-Modus ausgetauscht, so senden/empfangen beide Geräte die Daten vom Access Point. Der dritte Betriebs-

modus ist für WLAN-Clients nicht nutz- und sichtbar - der "Point-To-Point"-Modus verbindet zwei APs miteinander.

Was die Übertragungsgeschwindigkeit betrifft, dürfte aktuell die Mehrzahl der WLANs gemäß der IEEE-Spezifikation 802.11g arbeiten. Dieser seit dem Jahr 2003 verfügbare Standard ermöglicht eine theoretische Brutto-Verbindungsrate von 54 MBit/s mit einer durchschnittlichen Reichweite von zirka 38 Metern in geschlossenen Räumen und rund 140 Metern im Freien. Der Netto-Durchsatz liegt mit zirka 19 MBit/s deutlich unter der theoretischen Brutto-Verbindungsrate.

Schon seit rund zwei Jahren sind WLAN-Router, Access Points und WLAN-Karten für den neuesten Standard 802.11n auf dem Markt – stets mit dem Hinweis "DRAFT" (Entwurf). Am 11.09.2009 wurde nach langer Diskussion der jüngste Funknetzwerkstandard 802.11n von der IEEE ratifiziert und einige wenige optionale Funktionen des Drafts festgeschrieben. Der Standard IEEE 802.11n beinhaltet zahlreiche neue Mechanismen, um die verfügbare Bandbreite zu erhöhen. Netzwerke nach 802.11n erzielen derzeit einen Brutto-Datendurchsatz von bis zu 300 MBit/s (netto in der Praxis zwischen 75 und 130 MBit/s). Die tatsächlich realisierbaren Geschwindigkeiten überschreiten somit zum ersten Mal den Fast-Ethernet-Standard mit 100 MBit/s in einem kabelgebundenen Netzwerk, was an den meisten PC-Arbeitsplätzen derzeit (noch) Standard ist. Neben der Erhöhung der Datendurchsatzrate bietet IEEE 802.11n zudem die Grundlage für eine zuverlässigere Funkabdeckung.

802.11n sendet über mehrere Antennen

Technisch betrachtet wurde für 802.11n das bereits bekannte OFDM-Verfahren (Orthogonal Frequency Division Multiplex) optimiert. Bei ODFM wird das Datensignal nicht auf einem einzelnen, sondern parallel auf mehreren Trägersignalen moduliert. Anstelle von 48 Trägersignalen, wie bei den Vorgängern 802.11 a/g, kommen maximal 52 Signale zum Einsatz. Das Verhältnis von Nutzdaten zu Prüfdaten hat sich seit der Entwicklung von 802.11 stetig verbessert, aktuell sind unter optimalen Bedingungen Verhältnisse von 5 zu 6 möglich, während die Vorgänger noch mit einem Verhältnis 1 zu 2 oder 3 zu 4 arbeiteten.

Die wichtigste Neuerung in 802.11n verbirgt sich hinter der Abkürzung MIMO (Multiple Input Multiple Output). MIMO benutzt mehrere Sender und mehrere Empfänger, um aktuell zwei parallele Datenströme auf dem gleichen Übertragungskanal zu übermitteln. In der Konzeption ist eine Erhöhung auf bis zu vier parallele Datenströme bereits eingeplant. Die Daten werden beispielsweise bei einem Access Point in zwei Gruppen aufgeteilt, die jeweils über separate Antennen, aber gleichzeitig zum WLAN-Client gesendet werden. Mit dem Einsatz von zwei Sende- und Empfangsantennen lässt sich also der Datendurchsatz verdoppeln. Bis zur Einführung von 802.11n galt eine solche Signalverteilung auf einem Kanal als unmöglich.

Trotz dieser Anpassungen ist IEEE 802.11n rückwärtskompatibel mit den bisherigen Standards IEEE 802.11a/b/g. Einige der Vorteile sind jedoch nur dann verfügbar, wenn neben den Access Points auch die WLAN-Clients die Verfahren von 802.11n nutzen. Um die Co-Existenz von WLAN-Clients nach 802.11 a/b/g zu ermöglichen (hier als "Legacy-Clients" bezeichnet), bieten die 802.11n-Access Points besondere Betriebsarten für den gemischten Betrieb an, in denen jedoch die Performance-Steigerungen gegenüber den Vorgängern geringer ausfallen. Nur in reinen 802.11n-Umgebungen kommt der so genannte "Greenfield-Modus" zur Anwendung, in dem alle Neuerungen nutzbar sind. Der neueste Standard 802.11n ist für den Betrieb in Unternehmen mit Blick auf Geschwindigkeit und Verfügbarkeit somit bestens gerüstet. Bezüglich der Verschlüsselung bleibt bei 802.11n alles beim Alten.

Verschlüsselung im Unternehmenseinsatz

Die Abkürzungen WEP, WPA und WPA2 sind jedem geläufig, der bereits einen WLAN-Internetrouter aus dem SOHO-Umfeld eingerichtet hat. Hinter den Abkürzungen verbergen sich unterschiedliche Verschlüsselungsmethoden, um einen unbefugten Zugriff auf das Funknetzwerk zu verhindern. WEP (Wired Equivalent Privacy) basiert auf RC4 und auf der Methodik, dass beim Einbuchen in das Netzwerk ein zuvor definierter Schlüssel eingegeben werden muss. Auch wenn es Implementierungen von Schlüssellängen mit bis zu 256 Bit gibt, gilt WEP als unsicher, da im Internet kostenlose Programme zur Verfügung stehen, die nach einer gewissen, meist

Verschlüsselung

Unabhängig von der verwendeten Verschlüsselungstechnik erschwert ein verschlüsseltes Netzwerk lediglich den Zugriff durch Dritte. Die Verschlüsselungen WEP und WPA sind bereits erfolgreich geknackt worden und gelten somit als unsicher.

Ausblenden der SSID

Die Deaktivierung des sichtbaren "Service Set Identifier" (SSID) senkt das Risiko, dass ein Funknetzwerk entdeckt wird. Spezielle Tools, so genannte WLAN-Sniffer, entdecken jedoch auch WLANs ohne SSID. Das Ausblenden des SSID kann sinnvoll sein, macht allein aber noch kein sicheres WLAN.

MAC-Adressenfilter

Durch die Begrenzung des Zugriffs durch einen MAC-Adressen-Filter lassen sich unerwünschte Teilnehmer ausschließen. Eigentlich dürfte jede 48-Bit lange MAC-Adresse weltweit nur ein einziges Mal existieren. Es gibt jedoch Programme, welche die Manipulation der eigenen MAC-Adresse ermöglichen. Als einziges Schutzsystem ist somit auch die MAC-Adressen-Filterung ungeeignet, insbesondere dann, wenn Kunden oder Mitarbeiter laufend externe Geräte in das Netzwerk einbringen.

Ausschalten, wenn nicht benötigt

Wird das Funknetzwerk nicht benötigt, beispielsweise über das Wochenende oder in der Nacht, so empfiehlt es sich, das WLAN auszuschalten. Dies senkt den Stromverbrauch, mindert das Risiko einer Hacker-Attacke und reduziert die Menge an elektromagnetischen Emissionen.

WLAN-Sicherheitsempfehlungen

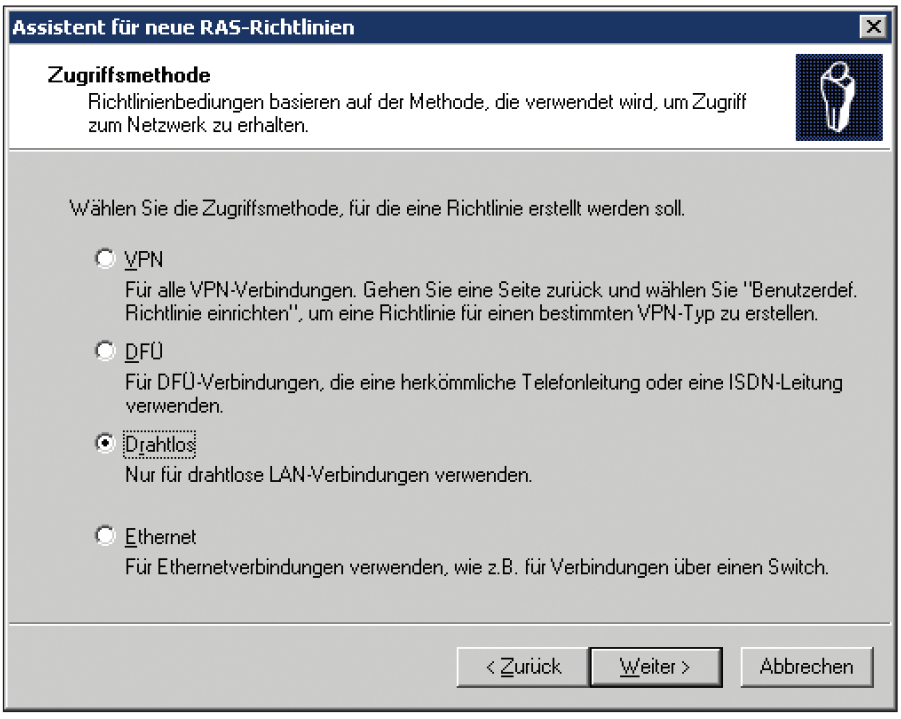


Bild 1: Mit Windows-Bordmitteln ist der Aufbau einer überschaubaren und über das Active Directory gesteuerten WLAN-Umgebung mit Hilfe des IAS Internetauthentifizierungsdienstes möglich

recht kurzen Protokollierungszeit den WEP-Schlüssel ermitteln können.

WPA (Wi-Fi Protected Access) ergänzt das Konzept um einen dynamischen Schlüssel. Zur Datenverschlüsselung nutzt WPA das Protokoll TKIP (Temporal Key Integrity Protocol) und für die Nutzeranmeldung EAP (Extensible Authentication Protocol). In der im SOHO-Umfeld gebräuchlichen Variante "Personal" wird der dynamische Schlüssel manuell auf jedem Endgerät eingetragen. Der dynamische Schlüssel ist somit weit weniger dynamisch und wird als "Passphrase" oder "Pre Shared Key" bezeichnet. Im Unternehmensumfeld, in den Auswahlfeldern der Software häufig als "Enterprise Mode" betitelt, kommt ein separater Authentifizierungsserver, beispielsweise Radius, zum Einsatz. Dieser prüft die Echtheit des Nutzers und gibt die Sitzung frei. WPA steht aktuell in der Version 2 zur Verfügung, welche als Verschlüsselungsmechanismus AES (Advanced Encryption Standard) verwendet.

Benötigt ein Unternehmen nur wenige Access Points und eine Handvoll Endgeräte, die auf das WLAN zugreifen, so steht einer traditionellen Bereitstellung mit WPA2-PSK im Prinzip nichts im Wege. Schwierig wird es erst dann, wenn die Passphrase aus Sicherheitsgründen geändert werden soll. Dies hat einen manuellen Aufwand für die Administration zur Folge. Die Administratoren müssen alle Access Points und Wireless Clients mit dem neuen Schlüssel ausstatten. Im Sinne einer erhöhten Betriebssicherheit sollte die neue Passphrase dem Benutzer nicht auf einem Papierausdruck mitgeteilt werden. Da nicht alle Anwender einen solchen Ausdruck korrekt vernichten, ist die Umstellung aller Notebooks und anderer Wireless Clients durch die EDV-Abteilung der sinnvollere Weg.

Ohne einen Authentifizierungsserver sollte in jedem Fall der Netzwerkschlüssel deutlich länger als die Mindestlänge von acht Zeichen sein und über Ziffern und Sonderzeichen verfügen. Kurze oder einfache Netzwerkschlüssel lassen sich bei WPA-PSK mittels Brute-Force oder Wörterbuch-Attacken erraten. Es verwundert somit kaum, dass Microsoft auf einer TechNet-Seite schreibt, dass "WPA-PSK aufgrund des Schlüsselhandlings nur für sehr

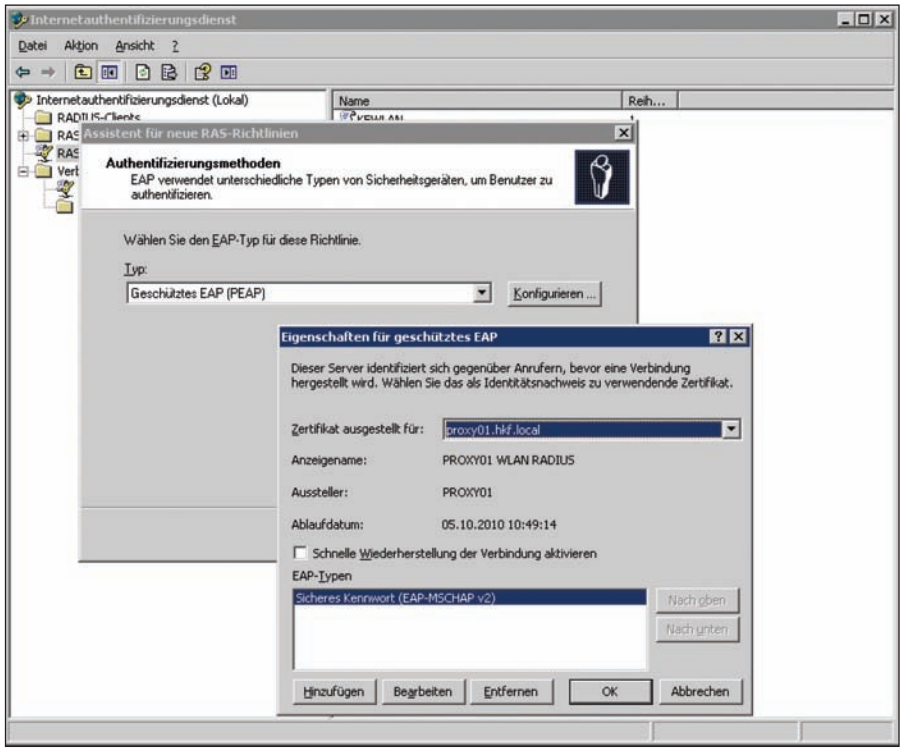


Bild 2: Um Microsoft Windows IAS nutzen zu können, ist eine Zertifizierungsstelle zwingende Voraussetzung

kleine Unternehmen oder Heimanwender geeignet ist".

Zentrales Management mit Windows-Bordmitteln

Windows bietet mit dem Internetauthentifizierungsdienst (IAS) die Möglichkeit, eine Authentifizierung der Wireless Clients sowie eine Verschlüsselung und Integrität der übertragenen Daten sicherzustellen. In dem TechNet-Dokument "10 Schritte zum Absichern eines WLAN in Windows-basierten Netzwerken" [1] geht Autor Denis Holtkamp auf diese Bereitstellung näher ein. In einer Test-Umgebung gelang die Umsetzung in rund zwei Stunden. Eine Bedingung für die Verwendung des Internetauthentifizierungsdienstes von Windows ist eine bereits installierte Zertifizierungsstelle im Active Directory. Unabhängig davon, ob im späteren Verlauf Zertifikate auf Benutzerebene genutzt werden sollen oder nicht, ist für die Anbindung des IAS selbst in jedem Fall die Zertifizierungsstelle eines Windows-Servers erforderlich. Die Konfiguration geschieht in sieben Schritten:

- Schritt 1: Installation des IAS Internetauthentifizierungsdienstes auf einem Active Directory Member Server.
- Schritt 2: Server im Active Directory registrieren.
- Schritt 3: Computerzertifikat für den IAS-Server anfordern.
- Schritt 4: Eine neue RAS-Richtlinie auf dem IAS-Server einrichten. Dieser Vorgang ist Assistenten-gestützt und beschränkt sich auf die Eingabe des Richtliniennamens, die Auswahl der Zugriffsmethode "drahtlos", die Verknüpfung mit einem Benutzer oder einer Gruppe aus dem Active Directory und die abschließende Auswahl "Geschütztes EAP (PEAP)". PEAP nutzt die normalen Domänen-Benutzer und das Passwort zur Authentifizierung.
- Schritt 5: Die Access Points als RADIUS-Clients eintragen.
- Schritt 6: In der Verwaltungsoberfläche der Access-Points den IAS-Server als Radius-Server angeben.
- Schritt 7: Einstellung auf dem Wireless-Client vornehmen (am sinnvollsten per Gruppenrichtlinie).

Als weiterführende Information sei auf das "Einrichtungshandbuch - Sichern von Wireless LANs mit Zertifikatsdiensten" [2], ebenfalls aus dem Microsoft TechNet, hingewiesen.

Zentrales Management durch WLAN-Controller

Mit Windows ist zwar die Bereitstellung eines zentralisierten WLAN-Managements generell möglich, jedoch mit einigen Einschränkungen. Sollen Gastzugänge angeboten, Firmware-Verteilungen realisiert oder Funkfeld-Optimierungen durchgeführt werden, so ist ein universelles Betriebssystem mit diesen Aufgabenstellungen überfordert. Zudem ist ein effektives Reporting über die Nutzung der WLANs ohne den Einsatz einer zusätzlichen Software kaum möglich. Spezielle Appliances, so genannte WLAN-Controller, bieten sich für ein zentralisiertes Management in größeren Umgebungen an. Ein solcher Controller übernimmt die Steuerung aller Access Points und WLAN-Router im Netzwerk und bildet zudem die Funktion eines RADIUS/EAP-Dienstes ab.

Dabei sind viele Geräte nicht auf ein WLAN begrenzt und können die einzelnen Funknetzwerke pro SSID auch einem VLAN zuweisen. Der Ausfall des Controllers geht nicht unbedingt mit einem Zusammenbruch des Funknetzwerks einher. Es obliegt dem Administrator, eine Einstellung zu wählen, die den Access Points einen autarken Weiterbetrieb beim Ausfall des Controllers ermöglicht. Viele Hersteller unterstützen dabei ausschließlich Access Points und WLAN-Router aus dem eigenen Hause. Dem Wunsch nach einem zentralen Management sollte somit eine genaue Geräteauswahl vorangehen. *(ln)*

Links

[1] TechNet: 10 Schritte zum Absichern eines WLANs
www.microsoft.com/germany/technet/sicherheit/mvp/wlan.mspx

[2] TechNet: Sichern von WLANs mit Zertifikatsdiensten
www.microsoft.com/germany/technet/datenbank/articles/900160.mspx

Prozessoptimierung durch Logon-Skripte (1)

Automatisch besser

von Sascha Giebelhausen

Bevor ein Logon-Skript erstellt wird, sollte die Infrastruktur des Unternehmens sehr genau analysiert werden, da Fehler bei der Planung von Logon-Skripten nach deren Implementierung häufig weitergeführt werden. Zum Beispiel zählen zu solchen Fehlern, dass die Skripte bei vielen Unternehmen nicht durch Abfragen des Active Directory gesteuert werden, es jedoch für jede Abteilung beziehungsweise jedes Fachteam ein eigenes Logon-Skript für die Verbindung von Netzwerkdruckern und Netzlaufwerken gibt. Wäre dies jedoch der Fall, muss bei einer Änderung an einer zentralen Netzwerkressource nur ein Active Directory integriertes Skript angepasst werden. Im ersten Teil unserer Workshopserie zeigen wir auf, wie Logon-Skripte durch das Lesen von Daten aus dem Active Directory Prozesse automatisieren.

Da Logon-Skripte häufig aus einer Not heraus erstellt werden, automatisieren diese meist nur die offensichtlichen Aufgaben des Benutzers, welche bei der ersten Anmeldung direkt durch den Administrator oder einen Mitarbeiter des Supports manuell durchgeführt werden müssen. Zu diesen gehören zum Beispiel die Begrüßung des Benutzers, das Zuordnen von Netzlaufwerken oder das Verbinden von Netzwerkdruckern. Je nach örtlicher Gegebenheit sollte der Standarddrucker anhand der Raum- oder Etagennummer festgelegt werden. Was jedoch meist nicht zur Umsetzung kommt, ist das Laufwerksmanagement über die Mitgliedschaft des Benutzerkontos in Gruppenobjekten des Active Directory oder die Umbenennung der Netzlaufwerke. Weiterhin lassen sich natürlich auch Mailsignaturen für Microsoft Outlook benutzerspezifisch generieren (mehr dazu im zweiten Teil dieser Workshopserie).

Microsoft Script Editor

Der Microsoft Script Editor ist seit Office XP verfügbar und wird hauptsächlich für die Erstellung beziehungsweise Anpassung von Macros in den Office-Anwendungen genutzt. Den wenigsten Administratoren ist jedoch bekannt, dass sich diese Anwendung auch gesondert von Excel, Access oder Word starten lässt. Mit Office 2007 wurde der Microsoft Skript Editor unter "\Program Files\Common Files\Microsoft Shared\OFFICE12" abgelegt.

Arten von Logon-Skripten

Alle in diesem Artikel erwähnten Logon-Skripte basieren auf der Programmiersprache VB-Skript. Es gibt auch die Möglichkeit, die Logon-Skripte auf der Basis von Batch- oder CMD-Dateien aufzubauen. Dies ist jedoch nur so lange interessant, wie keine Abfragen über das Active Directory oder über die Registrierung des Clients durchgeführt werden, da dies nur über VB-Skript möglich ist. Diese Abfragen können zum Beispiel folgende Informationen ausgeben:

- Gruppenmitgliedschaften
- IP-Adressen
- Adress-Attribute des Nutzers
- Kontaktinformationen, etwa aus einem Benutzer-Objekt des Service Desks
- Betriebssysteminformationen
- Typ und Service Pack

Es gibt zwei Möglichkeiten zur Zuweisung von Logon-Skripten. Einerseits können Sie diese direkt im Benutzerkonto im Active Directory eintragen. Diese Methode ist gut geeignet für kleine und mittelständische Unternehmen mit einer einfachen Struktur. Sollte die Struktur jedoch größer werden, besteht ebenfalls die Möglichkeit, die Logon-Skripte über Gruppenrichtlinienobjekte zuzuweisen. Diese Methode ist jedoch erst praktikabel, wenn die Infrastruktur des Unternehmens mehrere Logon-Skripte voraussetzt oder die Anzahl der Anwender zu groß wird.

Aufgaben von Logon-Skripten

Alle Informationen aus dem Active Directory können Sie mehr oder weniger einfach via VB-Skript auslesen. Die gängigsten Attribute sind etwa Vorname (givenname), Nachname (sn), Benutzername (samaccountname), Mailadresse (mail) et cetera. Diese Attribute lesen Sie zum Beispiel mit dem Skript (Listing 1) aus und geben sie in einer MSG-Box aus.

Überprüfung von Active Directory-Attributen

Da in vielen mittelständischen Unternehmen die Pflege des Active Directory ma-

```
Set objSysInfo = CreateObject("ADSystemInfo")
strquery = "LDAP://" & objSysInfo.Username
Set objuser = GetObject(strquery)

strfirstname = objuser.givenname
strname = objuser.sn
straccount = objuser.samaccountname
strmail = objuser.mail
strcompany = objuser.Company
strphone = objuser.TelephoneNumber

msgbox ("Name: " & strfirstname & vbCrLf &_
   "Benutzerkonto: " & straccount & vbCrLf &_
   "Mailadresse: " & strmail & vbCrLf &_
   "Firma: " & strcompany & vbCrLf &_
   "Telefon: " & strphone & vbCrLf)
```

Listing 1: Auslesen von Attributen

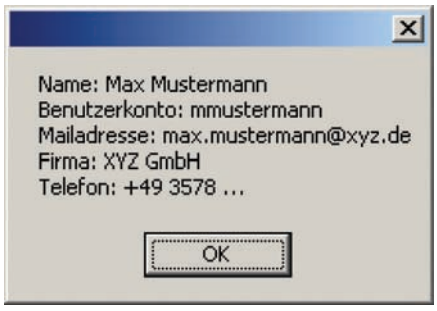


Bild 1: Die Ausgabe des Skripts aus Listing 1

nuell durch einen IT-Administrator erfolgt, müssen diese Informationen natürlich auch geprüft werden. Dies wird umso notwendiger, wenn die Signaturen von Outlook auf Attributen des Active Directory basieren. Diese Signatur wird bei jeder Neuanmeldung generiert und könnte durch fehlerhafte Informationen verfälscht werden. Deshalb sollte diese Abfrage mindestens überprüfen, ob die folgenden Active Directory-Attribute enthalten sind: Nachname, Vorname, Anmeldename, Mailadresse, Firma, Telefonnummer, Faxnummer, Büro, Straße, PLZ, Stadt und Webseite.

Natürlich können Sie aufgrund dieser Abfrage auch die Konsistenz der Informationen prüfen. Es lassen sich zum Beispiel die Domains der Mailadressen, die allgemeinen Adressinformationen oder auch das Attribut "Webseite" mit einer Liste freigegebener Informationen abgleichen.

Die Skript-Bausteine dieses Workshops wurden auf der Basis von Windows XP und Office 2003 (11.0) erstellt. Sie können diese jedoch auch einfach für die Betriebssysteme Windows Vista und Windows 7 oder für Office 2007/2010 verwenden. Zur Anpassung werden die Signaturen (Teil 2 dieser Workshopserie) in folgenden Pfaden abgelegt:

Windows XP
C:\Dokumente und Einstellungen\{username}\Anwendungsdaten\Microsoft\Signatures\{Signaturname}

Windows Vista
C:\Benutzer\{username}\AppData\Roaming\Microsoft\Signatures
C:\Benutzer\{username}\AppData\Roaming\Microsoft\Signatures\{Signaturname}

Windows 7
C:\Benutzer\{username}\AppData\Roaming\Microsoft\Signatures
C:\Benutzer\{username}\AppData\Roaming\Microsoft\Signatures\{Signaturname}

Natürlich gibt es auch bei den Officeversionen unterschiede. Dafür werden jeweils die folgenden Registrykeys genutzt:

Office 2003 (Version 11.0)
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\{MAILBOX-PROFILNAME}\9375CFF0413111d3B88A00104B2A6676\{ALLE_SCHLÜSSEL}\New Signature

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\{MAILBOX-PROFILNAME}\9375CFF0413111d3B88A00104B2A6676\{ALLE_SCHLÜSSEL}\Reply-Forward Signature

HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\MailSettings\NewSignature

HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\MailSettings\ReplySignature

Office 2007 (Version 12.0)
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\{MAILBOX-PROFILNAME}\9375CFF0413111d3B88A00104B2A6676\{ALLE_SCHLÜSSEL}\New Signature

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\{MAILBOX-PROFILNAME}\9375CFF0413111d3B88A00104B2A6676\{ALLE_SCHLÜSSEL}\Reply-Forward Signature

Office 2010 (Version 14.0)
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\{MAILBOX-PROFILNAME}\9375CFF0413111d3B88A00104B2A6676\{ALLE_SCHLÜSSEL}\New Signature

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\{MAILBOX-PROFILNAME}\9375CFF0413111d3B88A00104B2A6676\{ALLE_SCHLÜSSEL}\Reply-Forward Signature

Einzelheiten zu den Systemvoraussetzungen

Versenden von E-Mails an IT-Administratoren

Existiert innerhalb der Infrastruktur ein Microsoft Exchange-Server, so kann direkt eine E-Mail mit allen oder auch nur den fehlenden/fehlerhaften Informationen generiert und an die verantwortlichen Administratoren versandt werden (Listing 2). Weiterhin ist es natürlich auch möglich, eine Mail mit allen vorgenommenen Einstellungen zu versenden.

Logging der Änderungen des Skriptes

Ebenfalls ist es möglich, Log-Dateien auf einer zentralen Netzwerkressource über das Logon-Skript zu befüllen. Dies spart Ihnen zum Beispiel beim Troubleshooting viel Zeit. Kommt diese Lösung zum Einsatz, sollte das Logon-Skript bei der Anmeldung jede Änderung am System dokumentieren. Dazu müssen Sie natürlich sowohl die neuen als auch die alten Einstellungen festhalten. Hierbei ist jedoch zu beachten, dass gegebenenfalls der Betriebsrat über dieses Logging informiert werden muss und diese Log-Datei nicht im Netlogon-Verzeichnis abgelegt ist. Den Skript-Baustein aus Listing 3 können Sie für das Logging der Anmeldungen zum Troubleshooting nutzen.

Gruppengesteuertes Laufwerks-Mapping

Das Laufwerks-Mapping kann über zwei Methoden erfolgen. Sie können einerseits neue Gruppen alleine für das Mapping anlegen oder Sie nutzen die bestehenden Gruppen. Keine der beiden Methoden hat dabei entscheidende Vor- oder Nachteile. Sollten bereits Gruppen ohne einheitliche Syntax (im SamAccountName) für eine Netzwerkressource vorhanden sein, so würde es sich anbieten, das Mapping vorerst über gesonderte Gruppen zu managen.

Weiterhin besteht auch die Möglichkeit, den UNC-Pfad zu der Freigabe der Ressource in das Gruppenobjekt zu integrieren. Dafür sollten Sie die Felder "Beschreibung" oder "Anmerkung" nutzen. Dann lässt sich die Abfrage anschließend

relativ einfach für ein anderes Active Directory-Attribut anpassen. Das folgende Beispiel zeigt die Verbindung des Netzlaufwerks "T:" (\\Server\Temp), falls der Anwender Mitglied der Gruppe mit dem Namen "grp_temp" ist.

```
Set objSysInfo = CreateObject
  ("ADSystemInfo")
strquery = "LDAP://" &
  objSysInfo.Username
Set objuser = GetObject(strquery)
Set WSHNetwork = WSkript.
  CreateObject("WSkript.Network")
strmemberof = objuser.MemberOf
For Each objuser in strmemberof
  If instr(1,lcase(objuser),"cn=
       grp_temp,") >0 Then
       WSHNetwork.MapNetworkDrive
  "T:", "\\Server\Temp"
  End If
Next
```

Vereinfachung der Laufwerksbeschreibung

Um dem User die Arbeit mit den eingerichteten Netzlaufwerken zu vereinfachen, können Sie diese durch das Logon-Skript umbenennen. Hierfür sollten Sie jedoch innerhalb eines Active Directory-Konzeptes festlegen, dass diese Laufwerksbuchstaben nicht durch abteilungsabhängige Software oder andere Skripte genutzt werden dürfen. Sollte jemand zum Beispiel vor der Ausführung des Logon-Skripts eine externe Festplatte oder einen USB-Stick mit dem System verbinden, kann es sein, dass dieser Datenträger einen im Logon-Skript festgelegten Laufwerksbuchstaben erhält und die Beschreibung dieses Datenträgers geändert wird. Wenngleich dies im Normalfall keinen Datenverlust zur Folge hat, kann es trotzdem für einige Verwirrung auf Seiten des Users sorgen.

Zur Umbenennung der Netzlaufwerksbezeichung fügen Sie den folgenden Quelltext in das Logon-Skript ein:

```
Set objSysInfo = CreateObject("ADSystemInfo")
strquery = "LDAP://" & objSysInfo.Username
Set objuser = GetObject(strquery)

strfirstname = objuser.givenname
strname = objuser.sn
straccount = objuser.samaccountname
strmail = objuser.mail
strcompany = objuser.Company
strphone = objuser.TelephoneNumber
strfax = objuser.FaxNumber
straddress = objuser.streetaddress
strzip = objuser.postalcode
strcity = objuser.l
strmobile = objuser.TelephoneMobile
strweb = objuser.wwwhomepage
stroffice = objuser.physicaldeliveryofficename

strmessagetxt= "Hallo IT-Administrator," & vbCrLf & _
            vbCrLf & _
            "bei dem Account von " & strfirstname & " " & strname & " wurden leider nicht alle erforderlichen
            Attribute gepflegt." &vbCrLf & _
            vbCrLf & _
            "Nachnamen: " & strname & vbCrLf & _
            "Vorname: " & strfirstname & vbCrLf & _
            "Anmeldename: " & straccount & vbCrLf & _
            "Mailadresse: " & strmail & vbCrLf & _
            "Firma: " & strcompany & vbCrLf & _
            "Telefonnr.: " & strphone & vbCrLf & _
            "Faxnr.: " & strfax & vbCrLf & _
            "Büro: " & stroffice & vbCrLf & _
            "Straße: " & straddress & vbCrLf & _
            "PLZ: " & strzip  & vbCrLf & _
            "Stadt: " & strcity & vbCrLf & _
            "Mobil: " & strmobile  & vbCrLf & _
            "Webseite: " & strweb

set objMessage = CreateObject("CDO.Message")
objMessage.From = "wunsch@domain.de"
objMessage.To = "empfaenger.mailadresse@domain.de"
objMessage.Subject = "AD-Attribute fehlen für Signatur"
objMessage.TextBody = strmessagetxt

objMessage.Configuration.Fields.Item ("http://schemas.microsoft.com/cdo/configuration/sendusing") = 2
objMessage.Configuration.Fields.Item ("http://schemas.microsoft.com/cdo/configuration/smtpserver") = "Eigener
   Mailserver"

objMessage.Configuration.Fields.Item ("http://schemas.microsoft.com/cdo/configuration/smtpserverport") = 25

objMessage.Configuration.Fields.Update

objMessage.Send
set objMessage = Nothing
```

Listing 2: Versand einer E-Mail aus MS Exchange

```
Set objSysInfo = CreateObject("ADSystemInfo")
strquery = "LDAP://" & objSysInfo.Username
Set objuser = GetObject(strquery)
Set objFSO = CreateObject("Skripting.
   FileSystemObject")
strComputer = "."
Set objWMIService = GetObject("winmgmts:" _
 & "{impersonationLevel=impersonate}!\\" &
   strComputer & "\root\cimv2")

Set colOSes = objWMIService.ExecQuery("Select *
   from Win32_OperatingSystem")
For Each objOS in colOSes
   strhostname = objOS.CSName
Next

strmemberof = objuser.MemberOf

straccount = objuser.samaccountname
strfirstname = objuser.givenname
strname = objuser.sn

strdate = Date() &" "&Time()

Set objFSO = CreateObject("Skripting.
   FileSystemObject")
Set readfile = objFSO.OpenTextFile("\\Domäne\
   NETLOGON\signaturhistory.csv", 1)

Inhalt =""

Do Until readfile.AtEndOfStream
   Zeile = readfile.ReadLine
   Inhalt =   Inhalt & Zeile & vbCrLf
Loop

Set writefile =
   objFSO.OpenTextFile(("\\Domäne\NETLOGON\
   signaturhistory.csv", 2)

writefile.Write Inhalt
writefile.Write strdate & ";" & straccount & ";" &
   strname & ";"& strfirstname & ";" & strhostname
writefile.Close
```

Listing 3: Logging der Anmeldungen

```
Dim oShell
Set oShell = CreateObject("Shell.
  Application")
oShell.NameSpace("h:\").Self.Name =
  "Home"
```

Druckermapping via Logon-Skript

Das grundsätzliche Verbinden aller Netzwerkdrucker kann in vielen Unternehmen automatisch erfolgen. Dabei sollten Sie jedoch darauf achten, dass nicht zu viele Drucker pro Anwender verbunden werden. Bei mehr als 15 Druckern nimmt die Übersichtlichkeit enorm ab. Dies können Sie jedoch durch eine gut durchdachte Namenskonvention für die Bezeichnung der Netzwerkdrucker wieder ausgleichen.

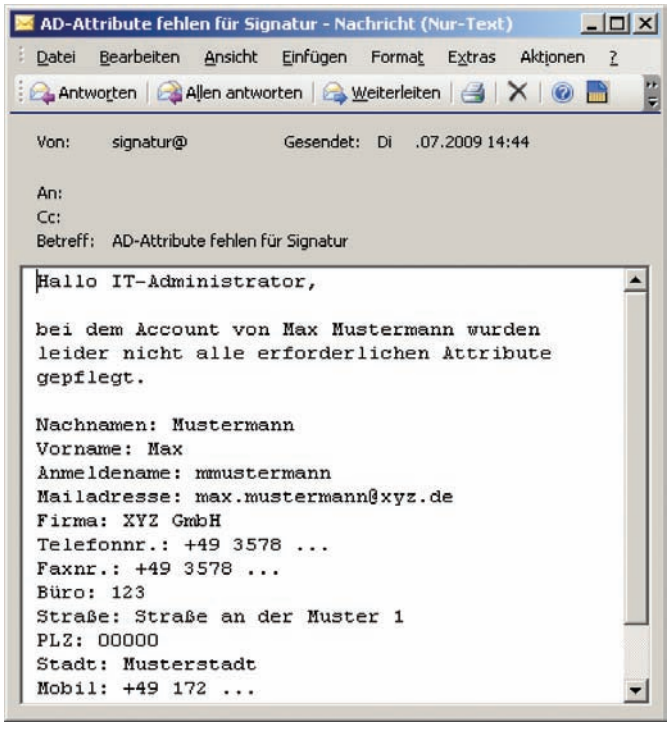


Bild 2: Die E-Mail aus dem Skript informiert den Administrator über fehlende Attribute

```
Set WSHNetwork = WScript.
  CreateObject("WScript.Network")
WshNetwork.AddWindowsPrinter
  Connection "\\Printserver\" +
  "Druckername"
```

Natürlich ist es durch die Vereinheitlichung der Druckernamen auch möglich, veraltete Drucker bei Anmeldung am System zu entfernen. Dafür nutzen Sie folgende Befehle:

```
Set WSHNetwork = WScript.
  CreateObject("WScript.Network")
WshNetwork.RemovePrinterConnection
  "\\Printserver\" + "Druckername"
```

Im Normalfall ist der Standarddrucker immer der Drucker, welcher zuerst verbunden wird. Häufig reicht die Zuordnung eines Standarddruckers jedoch nicht aus. Diese Herausforderungen tauchen jedoch meist erst nach der eigentlichen Implementierung des Logon-Skripts auf.

Zu guter Letzt gibt es dann natürlich auch noch die Mitarbeiter mit einem Drucker auf der Etage oder einem eigenen Drucker am Platz. Hier muss die Zuordnung des Standarddruckers über eine Abfrage des Active Directory-Attributs Büro oder über einen Vergleich der Adresse mit einer vorher festgelegten Liste durchgeführt werden. Das erste Beispiel ändert diese Zuordnung des Standarddruckers aufgrund der ersten zwei Stellen der Raumnummer, da diese häufig in den Raumkonzepten als Angabe der Etage genutzt wird.

```
Set objSysInfo = CreateObject("AD-
  SystemInfo")
strquery = "LDAP://" &
  objSysInfo.Username
Set objuser = GetObject(strquery)
Set WSHNetwork = WScript.CreateOb-
  ject("WScript.Network")

stroffice = objuser.physicaldeli-
  veryofficename

If left(stroffice,2)="1." then
  WshNetwork.SetDefaultPrinter
  "\\Printserver\" + "Drucker Etage
  1"
```

Dieses zweite Beispiel ordnet den Standarddrucker direkt dem Vorgesetzten mit der Raumnummer 122 zu.

```
Set objSysInfo = CreateObject("AD-
  SystemInfo")
strquery = "LDAP://" &
  objSysInfo.Username
Set objuser = GetObject(strquery)
Set WSHNetwork = WScript.CreateOb-
  ject("WScript.Network")

stroffice = objuser.physicaldeli-
  veryofficename

If stroffice="122" then
  WshNetwork.SetDefaultPrinter
  "\\Printserver\" + "Drucker Vorge-
  setzter"
```

Fazit

Der Vorteil von Logon-Skripten auf der Basis von VB-Skript ist, dass diese Skripte eine kostenlose Alternative zu kostenpflichtiger Software von Drittanbietern ist. Weiterhin können diese Skripte sehr viele Aufgaben von Administratoren und Anwendern übernehmen oder wenigstens vereinfachen, wodurch die Mitarbeiter den Fokus auf ihre eigentlichen Aufgaben richten können. Natürlich können alle hier enthaltenen Beispieltexte, die in Textdateien abgelegt wurden, auch datenbankbasiert verwaltet werden - der Einfachheit halber wurde in diesem Artikel darauf verzichtet.

Im zweiten Teil der Workshopserie zeigen wir auf, wie Sie über Logon-Skripte E-Mail-Signaturen erzeugen und den Anwendern zuweisen. *(jp)*

Sascha Giebelhausen ist Infrastrukturberater bei der adMERITia GmbH aus Langenfeld.

Bestellen Sie jetzt

das IT-Administrator

Sonderheft I/2010!

180 Seiten Praxis-Know-how

rund um das Thema

Windows Server 2008 R2 und Windows 7 + Tools-CD

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

**IT-Administrator Abonnenten erhalten das Sonderheft I/2010 für € 24,90.*
Nichtabonnenten zahlen € 29,90.

Liefertermin:
Ende März 2010

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

www.it-administrator.de/kiosk/sonderhefte/

---

administrator
Das Magazin für professionelle System- und Netzwerkadministration

Einfach kopieren und per Fax an den Leserservice IT-Administrator senden: 06123/9238-252

☐ **Ja**, ich bin IT-Administrator Abonnent mit der Abonummer (falls zur Hand) _____
und bestelle das IT-Administrator Sonderheft I/2010 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

☐ **Ja**, ich bestelle das IT-Administrator Sonderheft I/2010 zum Preis von **€ 29,90** inkl. Versand und 7% MwSt.

Der Verlag gewährt mir ein Widerrufsrecht. Ich kann meine Bestellung innerhalb von 14 Tagen nach Bestelldatum ohne Angaben von Gründen widerrufen.*

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____

Kto.: _____ BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

* Zur Fristwahrung genügt die rechtzeitige Absendung einer E-Mail an leserservice@it-administrator.de oder einer kurzen postalischen Mitteilung an Leserservice IT-Administrator, 65341 Eltville.

ITA 1209

So erreichen Sie unseren Vertrieb, Abo- und Leserservice:

Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville
Tel: 06123/9238-251
Fax: 06123/9238-252
leserservice@it-administrator.de

Diese und weitere Aboangebote finden Sie auch im Internet unter www.it-administrator.de

E-BOOK SYSTEMS
Abos und Einzelhefte gibt es auch als E-Paper

Heinemann Verlag
Leopoldstraße 85
D-80802 München
Tel: 089-4445408-0
Fax: 089-4445408-99
Geschäftsführung:
Anne Kathrin Heinemann
Matthias Heinemann
Amtsgericht München HRB 151585

Informationsschutz durch Kennworte

Sicher wie in Abrahams Schoß

von Hagen Will

Mit dem gestiegenen Sicherheitsbedürfnis in der Informationstechnik ist auch die Frage nach einem effektiven Kennwortschutz aktuell wie nie zuvor. Kennworte schützen Informationen nicht nur, vielmehr sind sie die sensibelsten Bestandteile eines Systems, das Informationszugriffe auf Benutzerebene regelt und loggt. Die Herausforderung an jeden Administrator lautet, den Anwendern Möglichkeiten aufzuzeigen, Kennworte sicher und dennoch merkbar zu wählen. IT-Administrator entschlüsselt in diesem Beitrag die wichtigsten Fakten.

Vor jeder Kennworterstellung steht die Frage nach dem Schutzbedürfnis: welcher Aufwand ist angemessen, den Zugriff auf einen Informationssatz einzuschränken? Die Anforderungen an das Kennwort für einen Gastzugriff sind zweifelsfrei niedriger anzusetzen als jene für ein Netzwerkadministrator-Kennwort. Ab Windows XP ist bei Wahl eines leeren Kennwortes übrigens kein Netzwerkzugriff über das betroffene Konto mehr möglich: eine Möglichkeit, den Netzwerkverkehr für eine lokal sichere Umgebung einzudämmen.

Dagegen gilt für Hochsicherheitsumgebungen das Vier-Augen-Prinzip: Hier sollten Sie dafür Sorge tragen, dass Kennworte bei der Eingabe aus mehreren Teilen zusammengesetzt werden,

Bild 1: Die Inhalte von Kennwortfeldern sollten immer maskiert dargestellt werden

die jeweils verschiedenen Administratoren bekannt sind. So vermeiden Sie administrative Alleingänge.

Objekt- und benutzerbezogener Schutz

Haben Sie Ihr Schutzbedürfnis definiert, stellt sich die Frage nach dem Zugriffsmodell, das den Schutz gewährleistet. Grob unterteilt existieren zwei Kategorien: der objektbezogene und der benutzerbezogene Ansatz. Wird ein Informationssatz objektbezogen geschützt, bedeutet dies, dass für den Zugriff auf diesen ein Kennwort vonnöten ist. Hier liegt der Schwerpunkt ganz klar auf der Differenzierung zwischen befugten und unbefugten Anwendern (weitere Unterscheidungen treffen wir an dieser Stelle zugunsten der Überschaubarkeit nicht). Praktisch umgesetzt findet sich dieses Modell auf einem PC, auf dem nur ein Benutzerkonto existiert, unter dem alle Anwender arbeiten, insofern sie das Kennwort kennen.

Beim benutzerbezogenen Schutzmodell existiert für jeden Benutzer, der auf ein Objekt zugreift, ein eigenes Konto und somit auch ein separates Kennwort. Hierdurch entsteht zunächst ein höherer Verwaltungsaufwand, der jedoch durch die Anforderung Nachvollziehbarkeit gerechtfertigt ist. Immer dann, wenn es Ihnen wichtig ist, wer etwas ausgelöst hat und diese Information geloggt wird, müssen Sie den Benutzer anhand seines Kontos eindeutig identifizieren können. Ein weiterer Zweck in der Unterscheidung verschiedener Benutzerkonten liegt in der unterschiedlichen Rechtevergabe. Wenn Benutzer A die Dateien eines Ordners lesen und ändern können soll, muss er im Regelfall über ein anderes Konto zugreifen als Benutzer B, der diese nur lesen können soll. Der benutzerbezogene Ansatz ist der in Firmenumgebungen am häufigsten anzutreffende.

Wahl der passenden Kennwortart

Wie Sie ein Kennwort eingeben lassen, sollte vom Sicherheitsbedürfnis des Systems und vom Arbeitskomfort des Anwenders abhängen. Ein hochsicheres Schutzsystem, bedient durch einen frustrierten Anwender, wird in der Regel daran scheitern, dass dessen Motivation und/oder Verantwortungsbewusstsein für die Sicherheit auf Dauer sinkt.

Neben der klassischen Texteingabe existiert die Möglichkeit der Authentifizierung über Smartcard und PIN. Diese Zwei-Faktor-Authentifizierung hält eine Kombination aus einem physikalischen Sicherheitstoken und einer bekannten Information als Schlüssel bereit. Dreh- und Angelpunkt ist hierbei jedoch meist der Einsatz einer Public Key Infrastruktur (PKI), welche weiteres Know-how erfordert, denn viele Smartcards funktionieren über hinterlegte digitale Zertifikate. Smart-

Bild 2: PINs sind ausschließlich dem Besitzer der zugehörigen Karte bekannt

card-Verfahren sind als sicherer als textbasierte Verfahren einzustufen, bedingen allerdings einen höheren Verwaltungs- und Kostenaufwand. Die Nutzerakzeptanz hält sich mit der ersteren Methode die Waage, da die Anwender hier zwar zwei Dinge vergessen können, die PIN jedoch meist einfacher als ein Kennwort zu merken ist.

Biometrie als Schlüssel zur Sicherheit und Nutzerakzeptanz ist eine Medaille mit zwei Seiten. Ein körperliches Merkmal, eine biologische Eigenschaft, die sich nicht vergessen lässt und die weitaus komplexer als jedes alphanumerische Kennwort ist, wird erfasst. Hierbei kommen Fingerabdrücke, Pupillenscanner, Handabdrücke (hier ist das venöse Geflecht entscheidend), Stimm- und Schrifterkennung sowie Hybridverfahren zum Einsatz. In der Praxis hat sich gezeigt, dass die Eingabe der Schlüsselinformation indes einfacher ist, da in der Tat keine Notwendigkeit mehr besteht, sich etwas zu merken. Ebenso wird dem Komplexitätsaspekt beim Abgleich von erkannten Merkmalen mit den Referenzdaten genüge getan. Es sei jedoch darauf verwiesen, dass hier nur die etablierten Hersteller durch Praxistauglichkeit überzeugen. In Vergleichsstudien fielen diverse Low-Cost-Produktserien durch ungenügende Fehlertoleranz oder mangelnde Beachtung des Datenschutzes bei der Speicherung von Referenzmaterial durch.

Verbreitete Sorten von Kennwörtern
- Textkennwort beziehungsweise -passwort
- Handy-PIN
- EC-PIN, TAN
- Biometrisches Merkmal
- Zertifikatsschlüssel (etwa auf Smartcards)
- Parole

Beispiele für Kennworte

Erstellung, Pflege und Verwahrung

Die Frage nach der Wahl des Kennwortes stellt sich nur bei der klassischen zeichenbasierten Eingabeform. Insofern möglich, sollten Anwenderkennworte nur dem Anwender selbst bekannt sein. Es besteht keine Notwendigkeit für die Kenntnisnahme seitens der Administration oder gar Geschäftsleitung. Notwendige Arbeiten unter dem Kontext des Benutzers können unter Anmeldung mit Initialkennworten, die der Anwender abschließend ändert, vorgenommen werden. Generell ist eine hohe Motivation des Anwenders vonnöten, um ihn nicht durch Komplexitätsanforderungen abzuschrecken. Die meisten Kennwortscanner, die beispielsweise bei der Brute-Force-Attacke alle möglichen Kombinationen ausprobieren, scheitern nicht an der Komplexität, sondern an der Länge eines Kennwortes. Außerdem gilt: je länger das Kennwort, desto länger kann es gültig bleiben. Lange Kennworte können Passphrasen sein, kurze verbale Ausdrucksformen wie "Wie geht's uns 2?".

Diese gelten unter Zugrundelegung moderner Methoden als besonders resistent gegen Angriffe. Das rhythmische Ändern von Kennworten gehört ebenso wie die sichere Verwahrung zur Kennwortpflege. Je nach Sicherheitsbedarf gelten wieder unterschiedliche Richtwerte für Mindestlängen von Kennworten und deren Gültigkeitsdauer. Eine Bankinfrastruktur wird eine mindestens monatliche Änderung der Kennworte in Verbindung mit Mindestlängen von 10 oder gar 12 Zeichen erfordern. Hier sei noch einmal darauf verwiesen, dass sicherheitsunbewusste Anwender erfahrungsgemäß Wege finden, um durch geschickte Modifikationen Kennworte zu wiederholen.

Auch hier existieren Hybridverfahren, wie die Kombination eines permanenten Kennwortes mit einem weiteren, verfallenden Einmal-Kennwort, wie beim PIN/TAN-Verfahren. Üblicherweise empfiehlt es sich, ein Kennwort etwa halbjährlich zu ändern und eine Mindestlänge von acht Zeichen vorzugeben. Durch Zuschaltung von Komplexitätsanforderungen können Sie Zahlen und Sonderzeichen erzwingen. Fordern Sie Ihre Anwender auf, die Kennwörter regelmäßig zu ändern, ist neben der Angabe einer maximalen Gültigkeitsdauer auch die einer minimalen nötig. Ansonsten ändern manche Anwender ihr Kennwort solange an einem Stück, bis die Chronik wieder den ursprünglichen Wert zulässt. Dieses Verhalten lässt sich unterbinden, wenn ein Kennwort zum Beispiel mindestens zwei Tage gilt. Stark anwenderbezogene Daten wie Name, Geburtstag, die Namen Verwandter oder einfache Zeichenfolgen dürfen in Kennworten aufgrund des leichten Erratens bekannterweise nicht verwendet werden.

Die sichere Speicherung beziehungsweise Verwahrung von Kennworten ist ebenso möglich wie das Sichmerken, allerdings weniger fehlerbehaftet. Es empfehlen sich Tresore oder Kennwortdatenbanken. Auch hier ist es nicht sinnvoll, alle Anwenderkennworte in einer Datenbank abzulegen. Bei Verwendung kann eine zentrale Lösung angestrebt werden, die beispielsweise über eine verschlüsselte Weboberfläche jedem Anwender – egal ob Administrator oder Endbenutzer – die Möglichkeit bietet, seine Kennworte sicher zu hinterlegen. Vorsicht ist geboten bei der Wahl des Master-Keys für den Zugriff auf eine solche Oberfläche. Da Ketten bekannterweise nur so stark sind wie ihr

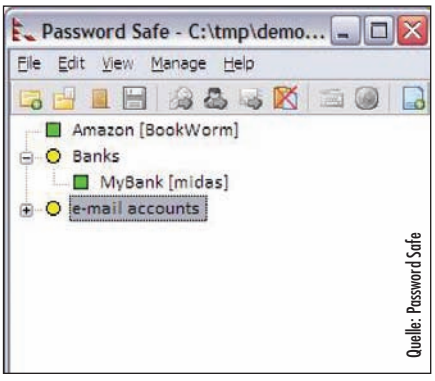


Bild 3: Die grafische Oberfläche der Kennwortdatenbank-Freeware Password Safe

schwächstes Glied, müssen Sie hier ein zum Inhalt vergleichsweise sicheren Wert wählen. Viele digitale Kennwortdatenbanken laufen als Dienst im Hintergrund des Betriebssystems mit und können bei entsprechender Konfiguration Kennworte automatisch eingeben oder zur Aufnahme neuer auffordern.

Authentifizierung und Verschlüsselung

Ein entscheidender Moment beim Einsatz passwortgestützter Zugriffskontrollsysteme ist der Abgleich des eingegebenen Kennwortes mit dem hinterlegten Prüfwert. Das Szenario basiert auf dem Server/Client-Prinzip, wobei der Client die kennworteingebende – also Informationen anfordernde – und der Server die Information haltende Funktion innehat. Der Abgleich des Kennwortes durch den Server ist als Verifizierungsversuch der vom Client behaupteten Identität zu verstehen. Bei diesem Vorgang authentisiert sich der Client am Server, wobei der Server bei positivem Abgleich den Client authentifiziert. Bei der Verarbeitung und Speicherung von Kennworten kommen standardmäßig Verschlüsselungsalgorithmen wie AES oder Twofish zum Einsatz. Das in Windows-Netzen verbreitete Kerberos-Authentifizierungssystem arbeitet zusätzlich aufgrund von Vertrauensstellungen und Tickets. Schon lange werden praktisch keine Klartextwerte, sondern Hashes zum Abgleich des eingegebenen Kennwortes durch den Server zum Vergleich herangezogen. Dies sind durch mathematische Streuwertfunktionen erzeugte Werte aus einer Teilmenge der Kennwortzeichen. Somit wird sichergestellt, dass das Kennwort selbst zum Vergleich nirgendwo steht und somit auch nicht ausgelesen werden kann. Doch es gibt neben diversen Hashalgorithmen wie MD5 oder SHA auch Angriffsmethoden; hier sei besonders auf den Kollisionsangriff verwiesen, bei dem zwei differente Ausgangswerte denselben Hashwert erzeugen.

10 Tipps für sichere Kennworte

1. Mindestens 8 Zeichen
2. Mindestens eine Zahl und ein Sonderzeichen
3. Eher lang als komplex (Passphrase)
4. Mindestens halbjährlich ändern
5. Sicher verwahren
6. Nicht weitergeben
7. Keine Kennworte wiederholen
8. Einfache Zeichenfolgen wie Namen und persönliche Daten vermeiden
9. Einfache Kurzbegriffe wie "Passwort" oder "qwertz" vermeiden
10. Anwender sensibilisieren

Alternative Ansätze

Es existieren Ansätze, um Sicherheitssysteme ohne Kennwortobjekte wie Textfolgen, Fingerabdrücke oder ähnlichem zu etablieren. Der bekannteste Ansatz ist die Kette des Vertrauens, bei der ein vertraulicher Datensatz nur zwischen Entitäten kommuniziert wird, die sich einander vertrauen. Die Sicherheit dieses Ansatzes gründet sich auf der Annahme, dass keine Instanz Informationen von einer anderen, nicht als vertrauenswürdig eingestuften Instanz annehmen würde. Ein Beispiel für angewendete Vertrauensketten in einem Hybridverfahren findet sich im Schlüsselsystem von PGP.

Fazit

Kennworte haben sich als Schlüssel zu vertraulichen Daten über Jahrhunderte bewährt und sind heute in digitaler Form präsenter denn je. Umso wichtiger ist der sorgsame Umgang mit diesen, der in erster Linie von der Einstellung des Anwenders zur Vertraulichkeit und Verantwortlichkeit hierbei abhängt. Sie sollten Sensibilisierung und Awareness vor jeder produktiven Einführung kennwortbasierter Zugriffskontrollsysteme auf Anwenderseite erneut hinterfragen. Die Form des Kennwortschutzes unterscheidet sich durch Anforderungen an Nachvollziehbarkeit und Berechtigungstiefe zwischen objekt- und benutzerbasierten Systemen.

Die Wahl der Eingabemethode hängt ebenso vom Sicherheits- und Komfortbedürfnis ab wie vom Kostenfaktor, denn Sicherheit und Komfort finden sich für biometrische Verfahren nur mit Aufpreis. Wer sich öfter Kennworte ausdenken muss, sollte auf eine bewährte Methode zur Generierung zurückgreifen, hier bieten sich Passphrasen an. Die regelmäßige Änderung und das absolut sichere Vermerken des Kennwortes runden dessen Pflege ab. Technisch werden Kennworte durch verschlüsselte Verarbeitung vor Ausspähung geschützt. Eine absolute Sicherheit wird es auch unter Zugrundelegung vertrauensbasierter Systeme nicht geben. Kryptografieexperte Bruce Schneier nennt den Weg als Ziel: "Sicherheit ist kein Produkt. Sicherheit ist ein Prozess". *(jp)*

Links

[1] Microsofts Tipps für sichere Kennworte
www.microsoft.com/germany/protect/yourself/password/create.mspx

[2] Webbeitrag zu sicheren Kennworten unter Linux
www.linux-fuer-alle.de/doc_show.php?docid=169&catid=16

[3] Website zu Macintosh Security
www.securemac.com

[4] Hagen Will zur Frage "Was darf der Admin wissen?"
www.datenschutz-praxis.de/fachwissen/fachartikel/was-darf-der-admin-wissen/

[5] Website des Sicherheitsexperten Bruce Schneier
www.schneier.com

Gemeinsame Benutzerverwaltung in Windows- und Linux-Netzwerken (2)

Der andere Weg

von Thorsten Scherf

Der erste Teil dieser Workshopserie befasste sich damit, Linux-Benutzer mit Hilfe von Winbind an einem zentralen Windows-Domänenkontroller zu authentifizieren. Nun wenden wir uns dem umgekehrten Weg zu, indem wir Windows-Benutzer an einem Linux-Server anmelden und so auf die gewohnte Umgebung zugreifen lassen. Dazu verwenden wir das Samba-Programmpaket und OpenLDAP.


Quelle: Jürgen Treiber, Pixelio.de

Zu dem umfangreichen Samba-Programmpaket [1] zählt etwa der im ersten Workshopteil vorgestellte Winbind-Dienst. Bekannter ist jedoch der SMB-Server, der Dateien und Drucker auf Basis des SMB-Protokolls im Netzwerk freigibt. Benutzer greifen so über das SMB-Protokoll auf die Daten eines Linux-Servers zu. Daneben bietet Samba weitere Funktionen an, die sonst nur von Windows-Servern bekannt sind:

- So kann Samba beispielsweise als NT4 PDC oder BDC agieren, also Anmeldefunktionen für Windows-Clients zur Verfügung stellen.
- Daneben ist es mittels WINS auch möglich, Samba als Namensserver einzusetzen oder
- die Stabilität der Windows-Netzwerkumgebung zum Durchsuchen von Freigaben zu erhöhen, indem Samba als Computersuchdienst agiert.

Mit all diesen Funktionen ist es Samba möglich, eine komplette Windows-Domäne zu verwalten. An dieser Stelle sei natürlich auch erwähnt, dass Samba in der aktuellen Version 3 keinen Active Directory-Domänencontroller ersetzen kann. Diese Funktion wird aber mit Erscheinen des nächsten Release (Version 4) in das Programm-Paket aufgenommen.

Vorteile von Samba

Der ein oder andere stellt sich nun vielleicht die Frage, wieso er überhaupt einen Samba-Server einsetzen soll, schließlich erledigen bestehende Windows-Server die notwendigen Aufgaben ja anscheinend auch problemlos. Zum einen spielt hier die Kostenfrage eine große Rolle, denn Samba steht unter der GNU General Public License (GPL) und ist somit kostenfrei zu haben. Hierbei fallen keinerlei Lizenzgebühren an, weder für den Server selbst noch für Client-Zugriffe auf den Server.

Daneben ist Samba sehr performant. Für jeden Client-Zugriff wird ein eigener smb-Prozess gestartet, das ist gerade für Multi-Core-Maschinen interessant, bei denen sich Prozesse auf einzelne CPUs verteilen lassen, um die anfallende Last aufzuteilen. Möchten Sie bestehende Windows-Server konsolidieren, so bietet Samba die Installation von unterschiedlichen Instanzen auf einem einzelnen System an. Auch was die Konfiguration und Verwaltung anbelangt, hat Samba Vorteile, da die Konfiguration über eine einzige Konfigurationsdatei stattfindet. Diese lässt sich sehr leicht auch aus der Ferne editieren und anpassen.

In Sachen Fehlersuche sind die Log-Dateien eines Samba-Servers eindeutig auskunftsfreudiger als die Ereignisanzeige von Windows-Servern und Fehler lassen sich leichter finden und somit Zeit einsparen. Dass zudem der Quellcode von Samba offenliegt und jeder die Funktionsweise der eingesetzten Software nachvollziehen kann, mag für manche Administratoren auch ein entscheidender Vorteil im Vergleich zu einer rein Windows-basierten Lösung sein.

Unter der Haube der Benutzerverwaltung

Bevor es an die Konfiguration des Samba-Servers geht, ist ein kleiner Ausflug in die interne Benutzerverwaltung auf Windows- und Linux-Systemen notwendig. Bereits im letzten Artikel erwähnten wir, dass Windows Benutzerkonten anders verwaltet als ein Linux-Server. Verwendet Linux eine einfache numerische User-ID (uid), um einen Benutzer zu identifizieren, so kommt unter Windows eine so genannte Security ID (SID) zum Einsatz. Diese SID ist, anders als die uid unter Linux, in der ganzen Windows-Domäne eindeutig. Das ist deshalb so, weil diese SID aus zwei Komponenten besteht: einer 98 Bit langen Domänenkennung und einer relativen ID (RID).

Zur Rechtevergabe kommt neben der angesprochenen SID und der uid natürlich auch noch die Gruppenmitgliedschaft eines Benutzers zum Tragen, wenn es darum geht, Zugriffsentscheidungen zu treffen. Genauso wie Benutzer-IDs verwaltet Windows auch seine Gruppen mit Hilfe dieser Security-IDs. Bei einer Anmeldung am System bekommt ein Benutzer dann ein so genanntes Security-Token ausgestellt, dieses enthält eine Liste mit sämtlichen SIDs, die diesem Benutzer zugeordnet sind. Mit dem Tool "rpcclient" lässt sich bei Interesse aus einer numerischen SID der eigentliche Benutzer- und Gruppenname ableiten. Somit ist es auch relativ sinnlos, den Administrator-Account auf einer Windows-Maschine umzubenennen, da sich dieser anhand der SID immer eindeutig identifizieren lässt (die SID dieses Kontos endet stets auf 500). Das Tool zeigt auch sehr schön an, ob es sich bei der angegebenen SID um einen Benutzer oder eine Gruppe handelt, dies ist ansonsten so ohne weiteres nicht ersichtlich. Aus den SIDs im Security-Token ergeben sich dann die tatsächlichen Zugriffsrechte für den Benutzer.

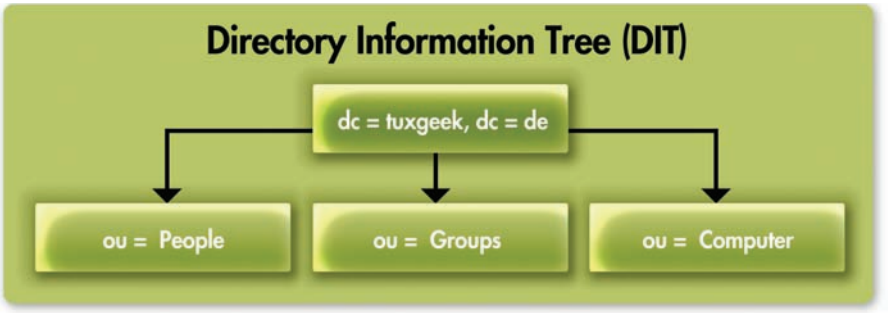


Bild 1: Samba speichert alle Account-Informationen in einem LDAP-Baum

Unter Linux besitzt jede Gruppe eine Gruppen-ID, die so genannte gid. Welcher Gruppe ein Benutzer angehört, steht in der Datei */etc/group*. Das Linux-Kommando *id* zeigt sämtliche Mitgliedschaften für einen Benutzer an. Beim Zugriff auf eine Datei ist auch hier die Kombination aus User-ID und Gruppen-IDs verantwortlich dafür, welche Rechte der Benutzer an dieser Datei besitzt.

Linux speichert Benutzerinformationen üblicherweise in der Datei */etc/passwd* ab; diese Datei ist vergleichbar mit dem Windows Security Account Manager (SAM). Damit nun auch Linux-Konten nicht nur auf einem einzelnen System eindeutig sind, sondern sich auch problemlos netzwerkweit einsetzen lassen, sind diese an zentraler Stelle zu speichern. Da wir in dieser Workshopserie die Konsolidierung von Linux- und Windows-Konten behandeln, bietet es sich an, die Benutzerkonten in einem LDAP Directory-Server abzulegen. Fügen Sie diesen Konten dann noch die notwendigen Windows-Attribute hinzu, so lässt sich mit Hilfe von Samba auch von Windows-Clients auf diese Konten zurückgreifen.

Die beiden Samba Standard-Backends "smbpasswd" und "tdbsam" eignen sich für diesen Fall nicht, da diese lediglich mit Samba-Benutzern umgehen können und außerdem auch keine Form der Replikation zwischen mehreren Samba-Servern anbieten. Diese Probleme existieren mit dem ldapsam-Backend von Samba nicht. Hier bezieht Samba, genau wie auch Linux-Anwender, Benutzer- und Gruppeninformationen aus dem LDAP-Server. Somit besteht nur noch ein zentraler Server zur Verwaltung sämtlicher Accounts. In größeren Umgebungen, in denen die Last auf mehrere Domänenkontroller verteilt wird, kommen Sie um den Einsatz eines LDAP-Servers als Backend sowieso nicht herum, da Samba über keinen eigenen Replikationsmechanismus zwischen dem Primary- (PDC) und dem Backup-Domänenkontroller (BDC) verfügt. Sie können mit einem Verzeichnisdienst, wie beispielsweise OpenLDAP [2], die Benutzerdatenbanken mehrerer Domänenkontroller dank der Replikationsfähigkeit des Verzeichnisdiensts synchron halten.

Neben den Benutzerkonten selbst muss ein Domänenkontroller noch einige weitere Informationen verwalten. Zum einen sind hier die Heimat-Verzeichnisse der Benutzer zu nennen, also "C:\Dokumente und Einstellungen \ Benutzername". Zum anderen existieren die beiden Ordner "Profiles" und "Netlogon". Der Profiles-Ordner enthält üblicherweise spezifische Einstellungen für einen Benutzer, also beispielsweise dessen Desktop-Einstellungen (*ntuser.dat*) und bestimmte Teile der Registry. Dieser Ordner kann Teil des Heimatverzeichnisses sein, lässt sich aber auch an jeder anderen Stelle

im Dateisystem ablegen. Im Ordner Netlogon befinden sich Skript- oder Batch-Dateien, die nach einem Login eines Benutzers ausgeführt werden. Des Weiteren finden sich hier Systemrichtlinien (*NTConfig.pol*). Diese sind nicht mit den Gruppenrichtlinien eines Active Directory-Servers zu verwechseln.

Die Konfiguration nehmen Sie in der Datei */etc/openldap/ slapd.conf* vor.

Schema Dateien für den Server

```
include     /etc/openldap/schema/corba.schema
include     /etc/openldap/schema/core.schema
include     /etc/openldap/schema/cosine.schema
include     /etc/openldap/schema/duaconf.schema
include     /etc/openldap/schema/dyngroup.schema
include     /etc/openldap/schema/inetorgperson.schema
include     /etc/openldap/schema/java.schema
include     /etc/openldap/schema/misc.schema
include     /etc/openldap/schema/nis.schema
include     /etc/openldap/schema/openldap.schema
include     /etc/openldap/schema/ppolicy.schema
include     /etc/openldap/schema/collective.schema
include     /etc/openldap/schema/samba.schema
```

Root-DN und Admin-Account

```
suffix      "dc=tuxgeek,dc=de"
rootdn      "cn=Manager,dc=tuxgeek,dc=de"
rootpw      redhat
```

Datenbank-Settings

```
database  bdb
checkpoint  1024 15
directory /var/lib/ldap
```

Indizes für bessere Performance

```
index objectClass
   eq,pres
index ou,cn,mail,surname,givenname
   eq,pres,sub
index uidNumber,gidNumber,loginShell
   eq,pres
index uid,memberUid
   eq,pres,sub
index sambaSID
   eq,pres
```

Logdatei

```
logfile /var/log/ldap
loglevel 256
```

Access Control-Einträge

```
access to attrs=userPassword,sambaLMPassword,sam-
   baNTPassword
by self write
by * auth

access to *
by * read
```

Listing 1: Konfigurationsdatei für den OpenLDAP-Server

Aufbau des LDAP-Servers

Nach soviel grauer Theorie nun in die Praxis. Als Test-Installation dient ein Fedora 11-System. Alle Beispiele lassen sich aber problemlos auch auf jeder anderen Linux-Distribution nachvollziehen. Unter Fedora gelingt eine Installation der Samba-Pakete aus dem Standard Software-Repository heraus. Als LDAP-Server kommt hier OpenLDAP zum Einsatz, Sie können jedoch auch auf jeden anderen LDAP-Server zurückgreifen, solange dieser LDAPv3-konform ist. Zur Installation der Pakete sieht der entsprechende yum-Aufruf unter Fedora wie folgt aus:

```
yum install samba samba-common
  openldap openldap-servers
  openldap-clients
```

Als Erstes konfigurieren Sie den Directory-Server. Dieser lässt sich recht einfach über die Datei */etc/openldap/ slapd.conf* (Listing 1) einrichten. Die Werte passen Sie natürlich entsprechend Ihrer Umgebung an (weitere Informationen zu den diversen Parametern finden Sie in der Manpage *slapd.conf*).

Im nächsten Schritt erzeugen Sie nun die Container, welche später die Benutzer-, Gruppen- und Maschinenkonten aufnehmen sollen. Hierzu verwenden Sie im einfachsten Fall die LDIF-Datei aus Listing 2. Als Directory-Server-Administrator ist diese dann in die LDAP-Datenbank zu importieren:

```
ldapadd -x -D "cn"Manager,dc=tuxge-
  ek,dc=de" -f /tmp/samba.ldif -w
  redhat
```

Ein abschliessendes *ldapsearch* bestätigt, dass der Server die Daten korrekt empfangen hat:

```
ldapsearch -x -h localhost -b
  "dc=tuxgeek,dc=de" -D \
"cn=Manager,dc=tuxgeek,dc=de" -W
```

Um dabei nicht ständig eine Vielzahl von Optionen an *ldapsearch* oder andere LDAP Client-Anwendungen übergeben zu müssen, lassen sich diese in einer zentralen Konfigurationsdatei namens */etc/openldap/ldap* speichern:

```
host tiffy.tuxgeek.de
base dc=tuxgeek,dc=de
binddn cn=Manager,dc=tuxgeek,dc=de
bindpw redhat
```

LDAP Client-Anwendungen greifen beim Verbindungsaufbau zum Directory-Server auf diese Konfigurationsdatei zurück. Somit sparen Sie sich unnötige Tipparbeit. Schließlich sind dem Directory-Server noch die notwendigen LDAP-Attribut- und Objekt-Definitionen aus dem Samba-Paket zu übergeben. Unter Fedora befindet sich im Samba-Dokumentationsordner eine Datei mit dem Namen *samba.schema*. Diese kopieren Sie einfach in das Schema-Verzeichnis von Open-LDAP und starten den Server im Anschluss neu:

Die LDIF-Datei */tmp/samba.ldif* erzeugt im Directory-Server ein Grundgerüst für die späteren Einträge.

```
dn: dc=tuxgeek,dc=de
objectClass: top
objectClass: dcObject
objectClass: organization
o: tuxgeek.de
dc: tuxgeek

dn: ou=users,dc=tuxgeek,dc=de
objectClass: top
objectClass: organizationalUnit
ou: users

dn: ou=groups,dc=tuxgeek,dc=de
objectClass: top
objectClass: organizationalUnit
ou: groups

dn: ou=idmap,dc=tuxgeek,dc=de
objectClass: top
objectClass: organizationalUnit
ou: idmap

dn: ou=computers,dc=tuxgeek,dc=de
objectClass: top
objectClass: organizationalUnit
ou: computers
```

Listing 2: LDIF-Datei

```
cp /usr/share/doc/samba-
  3.4.1/LDAP/samba.schema
service ldap restart
```

Wichtig ist, dass diese Schema-Datei in der eigentlichen Konfigurationsdatei *slapd.conf* auch mit einem include-Statement eingelesen wird, ansonsten sind dem LDAP-Server sämtliche Samba-Attribute unbekannt. Abschließend erzeugen Sie die Standard-Gruppen und -Benutzer, die Samba benötigt, um die Funktion als PDC korrekt ausführen zu können:

```
net sam provision
Checking for Domain Users group.
Adding the Domain Users group.
Checking for Domain Admins group.
Adding the Domain Admins group.
Check for Administrator account.
Adding the Administrator user.
  Checking for Guest user.
Adding Guest user.
  Checking Guest's group.
Adding the Domain Guest group.
```

Mit Hilfe von *pdbedit* lässt sich das Ergebnis, beispielsweise anhand des Administrator-Kontos, überprüfen. Dieses ist nun bereits in der LDAP-SAM vorhanden und lässt sich entsprechend abfragen. Natürlich können Sie das Tool auch dazu verwenden, bestimmte Eigenschaften eines Benutzers zu verändern.

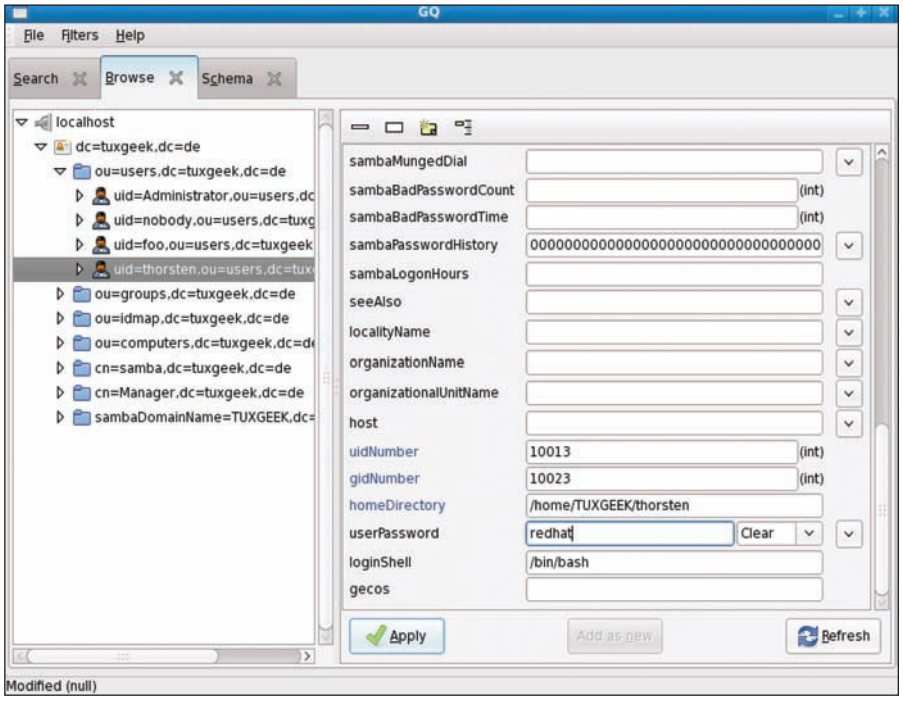


Bild 2: Mit Hilfe des grafischen LDAP-Browsers GQ lassen sich LDAP-Verzeichnisse komfortabel abfragen und verändern

Konfiguration von Samba

Nachdem wir den LDAP-Server eingerichtet haben, steht im nächsten Schritt die Konfiguration des eigentlichen Samba-Servers über die Datei */etc/samba/smb.conf* an. Interessant ist, dass neue Versionen von Samba (ab 3.3) zusätzlich eine Registry-basierte Konfiguration über das Tool "net registry" anbieten. Somit haben Sie die Möglichkeit, von einem Windows-System über den Registrierungseditor die Linux-basierte Konfiguration des Samba-Servers zu verändern. Mit diesem Thema befassen wir uns im letzten Teil der Serie ausführlich.

Die Konfigurationsdatei gliedert sich in zwei Abschnitte – "Global" und "Shares". Über die Sektion "Global" definieren Sie beispielsweise die Funktion des Servers, in diesem Fall also die des Primary Domain Controllers (PDC). Eine einfache Konfiguration für diese Sektion könnte wie folgt aussehen:

```
[global]
workgroup = TUXGEEK
security = user domain
logons = yes domain
master = yes
```

Hiermit definieren wir den Samba-Server als primären Domänen-Controller in der TUXGEEK-Domäne. Daneben agiert der Server noch als Master Browse-Server, dass heisst, er ist dafür zuständig, die Informationen, aus denen sich die Netzwerkumgebung zusammensetzt, von den einzelnen lokalen Browse-Servern aus den einzelnen Subnetzen zu verarbeiten und entsprechend auszuwerten. Als Nächstes teilen Sie dem Server mit, welches Backend er verwenden soll. Da wir in diesem Beispiel von einer replizierten Benutzerdatenbank ausgehen, legen wir sämtliche Account-Informationen in einem LDAP-Verzeichnis ab. Die notwendige Konfiguration finden Sie in Listing 3.

Seit Samba 3.0.25 ist der Server selbst in der Lage, die Benutzer- und Gruppen-Konten in die LDAP-Datenbank zu schreiben. In älteren Versionen mussten Administratoren hierfür auf einige Hilfs-

LDAP Backend-Konfiguration

```
passdb backend = ldapsam:ldap://tiffy.tuxgeek.de
ldap admin dn = cn=Directory Manager
ldap suffix = dc=tuxgeek,dc=de
ldap user suffix = ou=users
ldap group suffix = ou=groups
ldap machine suffix = ou=computers
ldap idmap suffix = ou=idmap
ldapsam:trusted = yes
ldapsam:editposix = yes
```

Winbind-Konfiguration (Samba benötigt diese, wenn mittels *smbpasswd* neue Benutzer und Gruppen anzulegen sind):

```
idmap uid = 10000 - 19999
idmap gid = 10000 - 19999
template shell = /bin/bash
```

Home-, Profile- und Netlogon-Definitionen

```
logon drive = H:
logon path = \\%N\profiles\%U\%a
logon script = login.bat
```

Listing 3: Ablage der Accountdaten im LDAP-Verzeichnis

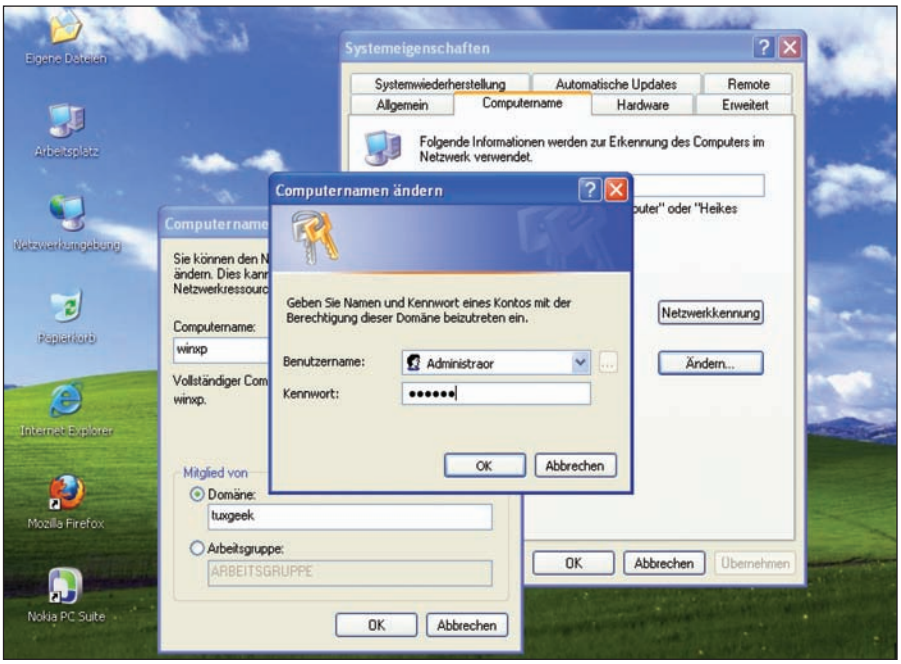


Bild 3: Mit Hilfe eines Administrator-Kontos des Samba-Servers lässt sich eine Windows-Maschine in die neue Domäne aufnehmen

Applikationen zurückgreifen [3][4]. Damit Samba nun auch mit dem LDAP-Backend kommuniziert, ist natürlich das Passwort des "LDAP Admin Users" in der Samba-Konfig mittels *smbpasswd -W* zu hinterlegen.

Wie bereits erwähnt, besteht die Aufgabe eines Domänencontrollers aber noch aus anderen Aufgaben, als lediglich Account-Informationen bereitzustellen. Benutzer möchten beim Login auch Zugriff auf Ihre Homeverzeichnisse erhalten, einmal geänderte Desktop-Einstellungen sollen wieder geladen werden und andere Netzlaufwerke sollen auch direkt nach dem Login zur Verfügung stehen, ohne diese erst manuell einbinden zu müssen. Genau hierfür sind die letzten drei Anweisungen aus der "Global-Sektion" zuständig. Sie definieren jeweils den Laufwerksbuchstaben für Homeverzeichnisse und legen fest, wo die Benutzerprofile zu speichern sind und welches Login-Script bei einer Benutzeranmeldung auszuführen ist. Damit dies funktioniert, muss Samba die passenden Ordner natürlich auch freigeben, so dass Benutzer Zugriff hierauf erhalten. Freigaben erzeugen Sie in der "Share-Sektion". Die drei Standard-Freigaben für einen Domänenkontroller sind im Folgenden aufgeführt:

```
[homes]
writable = yes
[profiles]
path = /var/lib/samba/profiles
writeable = yes
[netlogon]
path = /var/lib/samba/netlogon
```

Natürlich lassen sich noch jede Menge weiterer Optionen in der Datei hinterlegen. Das ist für einen performanten und sicheren Betrieb auch zwingend anzuraten, für eine grundlegende PDC-Konfiguration reichen die aufgeführten Beispiele jedoch vollkommen aus.

Abschließend erzeugen Sie nun noch mit Linux Bordmitteln ein Benutzerkonto mit allen notwendigen Samba-Attributen. Damit dies funktioniert und Samba nicht über einen fehlenden Linux-Benutzer mit den notwendigen Posix-Attributen meckert, konfigurieren Sie schließlich noch den Name Service Switch (NSS). Dieser kümmert sich darum, Benutzer- und Gruppen-Informationen aus unterschiedlichsten Datenquellen zu beziehen. Eine oft gestellte Frage an dieser Stelle ist, ob im Vorfeld nun also ein Linux-Konto mit Posix-Attributen anzulegen ist. Die Antwort lautet: "Nein, es ist nicht notwendig". Der Clou bei der vorgestellten Konfiguration ist nämlich, dass einem mit dem Tool *smbpasswd* erzeugten neuen Samba-Konto sowohl Samba-Attribute als auch – durch die Informationen für den Winbind-Daemon aus der *smb.conf* – die notwendigen Posix-Attribute (beispielsweise uid, gid und Heimat-Verzeichnis) zugewiesen werden. Damit der NSS diese Informationen aber auch findet, ist dieser anzuweisen, auf den LDAP-Server zurückzugreifen. Diese notwendigen Informationen stehen in der NSS-Konfigurationsdatei */etc/nsswitch.conf*:

```
grep ldap /etc/nsswitch.conf
passwd:     files ldap
group:      files ldap
```

Möchten Sie dem System nun einen neuen Benutzer mit Samba- und Posix-Attributen hinzufügen, so rufen Sie hierfür einfach *smbpasswd* wie folgt auf:

```
smbpasswd -a thorsten
New SMB password:
Retype new SMB password:
Added user thorsten.
```

Oftmals ist es wünschenswert, einzelne Attribute des Benutzers im LDAP zu verändern oder neue Attribute hinzuzufügen. Zum einen gelingt dies manuell über eine LDIF-Datei, die Sie dann mittels *ldapadd* in den Server importieren oder Sie greifen auf grafischen Frontends wie beispielsweise GQ [5] zurück. Möchten Sie beispielsweise den eben eingerichteten Benutzer zum Domänen-Administrator befördern, so ändern Sie im LDAP die Attribute uidNumber, gidNumber und sambaSID entsprechend. Die sambaSID eines Administrator-Kontos endet immer auf 500, die uid ist auf 0 zu setzen und die Gruppe der Domänen-Administratoren hat die Nummer 10024.

Eine ldapsearch-Abfrage bestätigt, dass das Konto nun wirklich im LDAP-Server vorhanden ist und die manuell vorgenommenen Änderungen sind ebenfalls zu erkennen. Auch die Anmeldung über den Samba-Server funktioniert nun einwandfrei, wie der folgende Aufruf zeigt:

```
smbclient //tiffy/thorsten
  -U thorsten
Enter thorsten's password:
Domain=[TUXGEEK] OS=[Unix]
  Server=[Samba 3.4.1-0.41.fc11]
  smb: \>
```

Nun wird es Zeit, den ersten Rechner in die neue Domäne aufzunehmen. Auf einem Windows-Client gelingt dies durch einen Rechtsklick auf das Arbeitsplatz-Symbol. Unter dem Reiter "Computername" klicken Sie dann auf den Button "Ändern", um der Domäne beizutreten. Als Benutzername geben Sie ein Konto des Samba-Servers an, welches Sie zuvor der Gruppe der Domänenadministratoren hinzugefügt haben und welches über root-Rechte auf der Linux-Maschine verfügt.

Bild 4: Beim Login kann sich der Anwender entweder mit seinem lokalen oder einem Domänen-Konto an der Maschine anmelden

Eine weitere Möglichkeit besteht darin, dem Windows-User, der die Maschine in die Domäne aufnehmen soll, mittels *net rpc* dieses Recht zu gewähren. Somit besteht nicht mehr die Notwendigkeit, dass dieser Benutzer zwingend die uid 0 besitzen muss:

```
net -U Administrator rpc rights
  grant Administrator
SeMachineAccountPrivilege
```

Noch einfacher geht es von einer Linux-Maschine aus. Hier reicht der folgende Befehl, um den gewünschten Rechner sozusagen remote in die Domäne aufzunehmen – sogar ein remote Reboot gelingt von hier aus:

```
$ net dom join -S WINXP -U
  WINXP\\Administrator
        domain=tuxgeek \
  account=root password=redhat reboot
Enter WINXP\Administrator's
  password:
Enter WINXP\Administrator's
  password:
Shutdown of remote machine
  succeeded
```

Anders als bei den Benutzer-Konten, liegt das Maschinen-Konto nun im Container ou=computers und endet auf ein Dollarzeichen. Damit ist die Konfiguration des PDCs abgeschlossen. Verwalten lässt sich der Server nun, wie gezeigt, sowohl mit Linux-Bordmitteln oder aber mit den bekannten Windows-Tools.

Im nächsten Teil der Artikel-Serie geht es dann darum, dem PDC einen Backup-Domänencontroller mit einer replizierten Benutzerdatenbank zur Seite zu stellen. Auch die Konfiguration von Linux-Systemen, so dass diese von den Informationen im LDAP profitieren und diese zur Anmeldung verwenden können, ist Thema des nächsten Artikels. Abschließend kommen einige erweiterte Konfigurationsmöglichkeiten zur Sprache, beispielsweise wie sich die Kommunikation zwischen dem LDAP-Server und den Clients mittels SSL/TLS schützen lässt oder wie Sie die komplette Samba-Konfiguration mit Hilfe des Registrierungseditors von einer Win-dows-Maschine aus erledigen. *(jp)*

Links

[1] Samba-Homepage
www.samba.org

[2] OpenLDAP-Homepage
www.openldap.org

[3] IDX-smbldap-Tools
http://sourceforge.net/projects/smbldap-tools/

[4] GOsa-Tools
http://alioth.debian.org/projects/gosa

[5] Grafischer LDAP-Browser GQ
http://sourceforge.net/projects/gqclient/

In jeder Ausgabe präsentiert Ihnen IT-Administrator Tipps, Tricks und Tools zu den aktuellen Betriebssystemen und Produkten, die in vielen Unternehmen im Einsatz sind. Wenn Sie einen tollen Tipp auf Lager haben, zögern Sie nicht und schicken Sie ihn per E-Mail an tipps@it-administrator.de. Für jeden Tipp, der veröffentlicht wird, bedanken wir uns mit einem Gutschein über 20 Euro für den Internetshop getDigital.de.

Tipps & Tricks ohne Gewähr

Bei der **Installation von Windows XP auf einem aktuellen Notebook** habe ich das Problem, dass der Installationsvorgang beim Lesen der Windows-CD mit einem Blue Screen und der Stop-Meldung "0x0000007B" abbricht. Laut Fehlermeldung scheint es **Schwierigkeiten mit der Festplatte beziehungsweise dem Festplatten-Controller** zu geben. Windows Vista und 7 kommen seltsamerweise problemlos mit der verbauten Festplatte zurecht. Warum funktioniert die XP-Installation nicht und gibt es hierfür einen Workaround?

Wenn Sie einen Blick auf das Datenblatt des wohl recht neuen Notebooks werfen, werden Sie feststellen, dass im Rechner eine SATA-Festplatte verbaut ist. Windows XP bringt jedoch von Haus aus keinen Treiber für SATA-Platten mit und kann den Magnetspeicher aus diesem Grund auch nicht ansteuern. Zwar besteht während des Installationsvorgangs die Möglichkeit, die nötigen Treiberdaten über eine Diskette auf den Rechner zu spielen, allerdings verfügt so gut wie kein neues Notebook mehr über ein Floppy-Laufwerk. Über USB angeschlossene Laufwerke erkennt XP während des Bootvorgangs ebenfalls nicht. Der einfachste Weg, diese Hürde zu überwinden, besteht darin, im BIOS den "Compatibility Mode" für den SATA-Controller zu aktivieren. Je nach BIOS kann dieser Modus unterschiedlich heißen, "ATA" oder "ATA Mode" sind hier die gebräuchlichsten Bezeichnungen. Diese Einstellung bewirkt, dass sich der SATA-Controller als normaler IDE-Controller ausgibt. XP kommt in diesem Fall mit der am Controller angeschlossenen Festplatte zurecht. Je nach Chipsatz kann es außerdem nötig sein, im BIOS die Option "AHCI" zu deaktivieren und / oder auf "IDE" zu setzen. Nun müsste die Installations-CD die Harddisk erkennen und einer Bespielung mit Windows XP steht nichts mehr im Wege. Der Nachteil dabei ist jedoch, dass Sie dann auch nicht mehr auf spezielle Features von SATA zurückgreifen können oder sogar eventuell vorhandene externe SATA-Anschlüsse nicht mehr funktionieren. Zudem kann es sein, dass Ihr Notebook aus Gründen der Boot-Performance nur noch ein abgespecktes BIOS an Bord hat. In diesem Fall ist es möglich, dass sich die nötigen Einstellungen zur Aktivierung des Schein-IDE-Controllers nicht vornehmen lassen. Sollte dies so sein, bleibt Ihnen nur noch, eine eigene, angepasste XP-Installations-CD mit integriertem SATA-Treiber zu erstellen. Dazu greifen Sie am besten auf die Programme "nLite" oder "Winfuture XP ISO Builder" zurück. Bei diesem Workaround handelt es sich um einen längeren Vorgang, der den Rahmen dieser Rubrik sprengen würde. Wenn Sie jedoch nach einem der beiden oben genannten Programme zusammen mit den Begriffen "XP" und "SATA" googeln, finden Sie diverse Anleitungen, wie Sie eine XP-Installations-CD mit SATA-Treiber erstellen. *(ln)*

Bereits Windows Vista verfügte als Bordmittel in der Systemsteuerung ja über ein Feature, das den **Aufbau des Netzwerkes in einer recht übersichtlichen grafischen Ansicht** verdeutlicht hat. Auch bei Windows 7 gibt es diese Möglichkeit. Leider funktioniert es weder bei Vista noch bei 7, dass diese topologische Ansicht die **im Netzwerk vorhandenen XP-Rechner** anzeigt. Kann ich diesen Umstand irgendwie ändern?

Daran, dass die XP-Rechner in der Netzwerkübersicht unsichtbar bleiben, trägt weder Windows Vista noch 7 eine Schuld. Vielmehr fehlt es XP am LLTD-Protokoll, das für die automatische Netzwerkerkennung nötig ist. Um auch die PCs mit älteren Betriebssystemen in der grafischen Übersicht abzubilden, müssen Sie ein Paket namens "Verbindungsschicht-Topologieerkennungs-Antwortprogramm" auf den XP-Clients nachrüsten. Dieses Programm lässt sich auf der Webseite von Microsoft herunterladen – auf einen

Link verzichten wir an dieser Stelle, da Sie die Erweiterung nach Eingabe des Namens-Ungetüms in einer Suchmaschine leicht finden werden. *(ln)*

Wenn man sich erst einmal an die **neue Taskleiste in Windows 7** gewöhnt hat, möchte man einige der Features nicht mehr missen. Besonders praktisch finde ich die Funktion, dass bei einem Verweilen des Mauszeigers über dem Programm-Symbol in der Taskleiste eine **Mini-Vorschau der jeweiligen Anwendung** eingeblendet wird. Allerdings erscheint dieser Thumbnail immer erst mit einer gewissen Verzögerung. Kann ich irgendwo einstellen, dass die praktische Vorschau sofort auf dem Monitor erscheint?
Von Haus aus hat Microsoft dem Vorschau-Fenster aus der Taskleiste heraus eine gewisse Latenzzeit verpasst. Wenn Sie dieser überdrüssig sind und die Thumbnails ohne Verzögerung einsehen wollen, können Sie dies nach Ausführen des Kommandos "regedit" in der Registrierungsdatenbank ändern. Navigieren Sie hierzu zum Verzeichnis "HKEY_CURRENT_USER \ Control Panel \ Mouse" und doppelklicken Sie auf den Eintrag "MouseHoverTime". Ändern Sie den dortigen Wert (die Zahl steht für Millisekunden) einfach auf "0" und die Mini-Vorschau erscheint sofort, wenn der Mauszeiger über die Taskleiste gehalten wird. *(ln)*

Ich arbeite oft mit der **Eingabeaufforderung**. Dabei nervt mich ziemlich, dass sich das **Fenster nicht beliebig skalieren** lässt, sondern der rechte Rand feststehend ist. Gerade bei umfangreichen Ausgaben verschwindet dann ein Teil der Zeile im Nirvana. Kann ich denn nicht auch dieses eine Fenster flexibel gestalten?
Leider ist es nicht möglich, die Eingabeaufforderung bei jedem Start beliebig mit der Maus zu skalieren. Der Grund für die feste Fensterbreite liegt darin, dass Windows XP die Bildschirmzeilen auf DOS-Ebene puffert. Mit einem einfachen Trick können Sie den Bildschirmbereich aber generell vergrößern und die abgeschnittenen Zeilen so aus dem unsichtbaren Puffer zurückholen. Dafür müssen Sie lediglich die Zahl der gepufferten Zeilen in den Eigenschaften des Konsolenfensters unter dem Reiter "Layout/Höhe" festlegen. Die Standardeinstellung von 300 Zeilen sollten Sie je nach Bildschirmgröße erhöhen, um frühere Arbeitsschritte oder Ergebnisse von DOS-Sitzungen besser prüfen zu können. Soll unabhängig von diesen Einstellungen das Fenster den kompletten Bildschirm einnehmen, erreichen Sie dies durch die Tastenkombination [ALT+EINGABE]. Verlassen können Sie den Vollbildschirm-Modus mit dem gleichen Shortcut.

Ich möchte **Postfachdaten aus einem Exchange-Konto direkt** in eine PST-Datei exportieren. Am liebsten über einen einfachen Befehl in der Exchange-Verwaltungsshell. Welche Möglichkeiten habe ich hier?
Wie Sie bereits erkannt haben, bietet die Exchange-Verwaltungsshell eine komfortable Möglichkeit, um aus Postfachdaten aus einem Exchange-Konto eine PST-Datei zu erstellen. Verwenden Sie dazu folgendes Cmdlet:

```
Get-Mailbox | Export-Mailbox -
  PSTFolderPath {Zielpfad}
```

Die gleiche Vorgehensweise funktioniert natürlich auch in die andere Richtung:

```
Get-Mailbox | Import-Mailbox -
  PSTFolderPath {Pfad der zu impor-
  tierenden PST-Datei}
```

So können Sie PST-Dateien auch in Exchange-Postfächer importieren, indem Sie das Cmdlet "Import-Mailbox" nutzen. *(ln)*

Ich würde gerne eine **Gruppe von Objekten konfigurieren, die ähnliche Identitäten besitzen**. Welche Cmdlets und Befehle kommen unter der **Exchange-Verwaltungsshell** hierzu in Frage?
Sie können auf Platzhalterzeichen mit dem Parameter "Identity" zurückgreifen, wenn Sie ein Get-Cmdlet verwenden und die Ausgabe mittels Pipelining an ein Set-Cmdlet umleiten. Geben Sie dazu Folgendes ein:

```
Get-Mailbox *John* | Set-Mailbox -
  ProhibitSendQuota 100MB
```

Dieser Befehl ermittelt alle Postfächer mit dem Namen "John" in der Identität des Postfachs und legt den Parameter "ProhibitSendQuota" auf 100 MByte fest. *(ln)*

Ich muss einen **Benutzer verwalten**, der zwar über Netzwerkzugriff verfügt, jedoch auch ein **externes E-Mailkonto außerhalb unserer Exchange-Organisation** besitzt. Wie kann ich mit Exchange Server 2007 E-Mail-aktivierte Benutzer erstellen, die reguläre Active Directory-Konten sind, sich aber auch als E-Mail-aktivierte Kontakte verhalten?
Mithilfe des Cmdlets "Enable-MailUser" können Sie jedem vorhandenen Active Directory-Benutzer, der nicht bereits ein Postfach auf einem Server mit Exchange besitzt, E-Mail-Kontaktattribute hinzufügen. Geben Sie dazu Folgendes ein:

```
Enable-MailUser -Identity {Active
  Directory Alias}
-ExternalEmailAddress {SMTP Ziel-Ad-
  dresse}
```

Anschließend sind die Benutzer in Ihrer Exchange-Organisation in der Lage, E-Mailnachrichten an das externe E-Mailkonto dieses Benutzers zu senden. *(ln)*

Tools

Microsoft **Exchange Server** ist vermutlich eines der Monitoring-intensivsten Serverprodukte. Es ist für den Administrator eine nicht immer ganz leichte Aufgabe, die zahlreichen Parameter im Blick zu behalten. Denn wenn der Exchange-Server erst einmal steht, klingeln die Telefone dafür umso intensiver. Umso nützlicher ist ein **Monitoring-Werkzeug**, das der Exchange-Verantwortliche schnell im Zugriff hat, um die Gesundheitsdaten seines Servers komfortabel abzulesen.

Die freie Software **Exchange Monitor** von Solarwinds ermöglicht eine Desktop-basierte Überwachung von Exchange 2003. Das Werkzeug überwacht den Server ununterbrochen und liefert dem Verantwortlichen Echtzeitdaten zu den Exchange-Diensten, der E-Mail-Queue-Größe und dem Exchange-Host. Über das schon aus dem VM Monitor bekannte Ampelprinzip signalisiert die Software den Zustand verschiedener Parameter von Exchange. So lassen sich schnell Probleme erkennen, die zu einem Ausfall des Servers oder zu großen Leistungseinbrüchen führen können, wie etwa Transportprobleme, Ausfälle der Internetverbindung oder Virusaktivitäten. Hostseitig überwacht das Tool Werte wie zum Beispiel den Plattenplatz, CPU-Auslastung und die Nutzung des Arbeitsspeichers. Nach einer kurzen Registrierung beim Hersteller steht die Software zum Download bereit, die zwar nicht mit Exchange 2007 arbeitet und zudem nur einen Exchange-Server überwachen kann, ansonsten jedoch ein überzeugendes Feature-Set für eine kostenlose Software bietet. *(jp)*

Quelle:http://www.solarwinds.com/products/freetools/exchange_monitor.aspx

Datenverluste sorgten in den vergangenen Monaten immer wieder für Schlagzeilen. Damit der Verlust beispielsweise eines USB-Sticks oder einer DVD nicht sofort für neue Horrormeldungen sorgt, ist als Basisschutz zumindest die **Verschlüsselung der mobilen Daten** anzuraten. So hat derjenige, dem die abhandengekommenen Daten in die Hände fallen, zumindest eine Hürde zu überwinden, ehe ihm Interna des betroffenen Unternehmens zur Kenntnis gelangen. Das freie Verschlüsselungstool **Sophos Free Encryption** schützt Daten, ohne dass die Anwender ihr gewohntes Arbeiten anpassen müssen.

Das kostenfreie "Sophos Free Encryption" verschlüsselt Dateien und ganze Ordner mittels 128- oder 256-Bit-AES

Sophos Free Encryption bietet gegenüber anderen Produkten, wie Dateipackern mit einfachem Passwortschutz für Dateien oder Verzeichnisse, den Vorteil einer starken Verschlüsselungstechnologie (AES). Das Werkzeug zeichnet sich besonders durch seine einfache Bedienung aus: Die Installation erfolgt über den Windows Installer; das Programm integriert sich automatisch in das Kontextmenü von Windows und in Standard-E-Mailclients wie Microsoft Outlook oder Lotus Notes. Die Software komprimiert zudem die ausgewählten Files und bietet die Option, selbstentpackende Archive zu erstellen. Der Hersteller hat die Lösung zudem mit einem Schutz gegen Brute Force-Angriffe gegen das vergebene Passwort versehen, indem sich der Zeitraum zwischen zwei Passworteingaben von Versuch zu Versuch verlängert. Das Verschlüsselungstool ist lauffähig unter Windows Vista, XP und 2000 sowie für Windows 7getestet. *(jp)*

Quelle:http://www.sophos.com/products/free-tools/sophos-free-encryption.html

Auf der Homepage des IT-Administrator-Magazins stellen wir jede Woche für Sie ein praktisches Tool zum Download bereit. Neben einer Kurzbeschreibung finden Sie Systemvoraussetzungen und alle weiteren wichtigen Informationen auf einen Blick. Und können so gezielt Werkzeuge für Ihren täglichen Administrationsbedarf herunterladen.

www.it-administrator.de/downloads/software/

Download der Woche

802.11n als Dualband Wireless

Mit zwei Kanälen auf der Überholspur

von Dominik Fritzsche

Nach Angaben der Marktforscher von ABI Research werden rund 45 Prozent aller 2009 verkauften WLAN-Produkte den Standard 802.11n unterstützen. Bis 2012 soll der Anteil auf 65 Prozent steigen. Im Gegensatz zu Heimanwendern zögerten Kunden im Enterprise-Umfeld bislang, die drahtlose Technologie weiträumig in ihre Netze zu integrieren. Dabei ist eine höhere Bandbreitenkapazität durchaus erforderlich. Am 11. September 2009 – und damit sechs Jahre nach dem ersten Entwurf und insgesamt elf Versionen später – erfolgte die Ratifizierung des WLAN-Standards 802.11n durch die IEEE-Gremien. Als besonders nutzbringend sollen sich die Bandbreitenbündelung von Funkkanälen und das parallele Senden auf zwei Frequenzen erweisen.

Wo früher unterschiedliche Frequenzen in verschiedenen Standards genormt waren – wie beispielsweise 2,4 GHz in IEEE 802.11g oder 5 GHz in IEEE 802.11a – erlaubt der jüngst verabschiedete Standard IEEE 802.11n zugleich die Verwendung des 2,4 sowie des 5 GHz-Frequenzbandes. Demnach werden Daten mit 300 MBit/s im Parallelbetrieb übertragen, wovon insbesondere sensible Datenströme wie High-Definition-Videoübertragungen und Voice-over-IP-Anwendungen profitieren. Außerdem bietet das duale Funken den Anwendern eine Alternative zu stark frequentierten 2,4 GHz-Umgebungen, zusätzlich belegt etwa durch Funkmäuse und -telefone. Dualbandgeräte ermöglichen hier jederzeit den Wechsel auf den 5 GHz-Frequenzbereich sowie dessen alleinige Verwendung. Er wird im Gegensatz zu 2,4 GHz noch nicht im großen Stil genutzt und ist somit weitaus stabiler. Ferner steht für die Datenübertragung eine größere Zahl sich nicht überlappender Kanäle zur Verfügung.

Uneinheitliche Marktsituation

Während Dualband Geräte im 54 MBit/s-Bereich (Standard 802.11g) lediglich eine untergeordnete Rolle spielten, scheint das parallele Funken auf den Frequenzbändern 2,4 und 5 GHz beim Standard 802.11n mehr und mehr in den Mittelpunkt zu rücken. Denn oftmals ist das Ausweichen auf den höheren Frequenzbereich die einzige Möglichkeit oder zumindest ein gangbarer Weg, um hohe Datentransferraten und Kompatibilität zu gewährleisten. Parallel-Band-Systeme, basierend auf der Wireless N-Technologie, sind im Handel seit Ende 2008 erhältlich.

Derzeit existieren erhebliche Unterschiede zwischen den verfügbaren Produkten. Tatsächliche 2,4/5 GHz Parallel-Band-Systeme zeichnen sich durch das gleichzeitige Arbeiten mit der vollen 802.11n-Leistung in beiden Frequenzbändern aus: So kann ein dual funkender Access Point im 2,4 GHz-Band zum einen die vorhandenen 54 MBit/s- (Standard 802.11g) und 300 MBit/s-Clients (Standard 802.11n) parallel anbinden. Zum anderen bedient er simultan auf der 5 GHz-Frequenz Geräte nach den Standards 802.11a und 802.11n. Die maximale Leistungsfähigkeit von Wireless N wird dabei immer komplett ausgeschöpft.

Andere Systeme – ebenfalls als Dualband bezeichnet – decken zwar zwei Frequenzbereiche ab, funken jedoch lediglich wahlweise im 2,4- oder im 5-GHz-Band. Des Weiteren existieren Geräte, die zwar parallel mit beiden Frequenzbändern arbeiten, aber nur auf einer Frequenz in der Lage sind, die maximale Geschwindigkeit von 300 MBit/s (brutto) zu nutzen.

Dualband Wireless N im Unternehmenseinsatz

Mit der drahtlosen Funktechnologie 802.11n lassen sich nicht nur höhere Datendurchsätze erreichen, sondern auch die Reichweite sowohl im Unternehmensgebäude als auch im Freien um den Faktor zwei bis drei steigern. Dadurch ergibt sich die Abdeckung einer größeren Fläche und es werden weniger Access Points zur Funkversorgung des gleichen Gebietes benötigt. Der Einsatz von Dualband Wireless N im Unternehmen bietet sich daher beispielsweise an, wenn eine große Anzahl von Nutzern über einen Access Point auf ein Netzwerk zugreift, da sich dann die zur Verfügung stehende Bandbreite auf die angebundenen Nutzer aufteilt.

Kanaltabelle 2,4 GHz-Band	
Kanal	Mittenfrequenz
1	2412 MHz
2	2417 MHz
3	2422 MHz
4	2427 MHz
5	2432 MHz
6	2437 MHz
7	2442 MHz
8	2447 MHz
9	2452 MHz
10	2457 MHz
11	2462 MHz
12	2467 MHz
13	2472 MHz

Kanaltabelle bei 40 MHz Bandbreite		
Kanal	Bündelung	Mittenfrequenz
1	1+5	2422 MHz
2	2+6	2427 MHz
3	3+7	2432 MHz
4	4+8	2437 MHz
5	5+1	2422 MHz
6	6+2	2427 MHz
7	7+3	2432 MHz
8	8+4	2437 MHz
9	9+5	2442 MHz
10	10+6	2447 MHz
11	11+7	2452 MHz
12	12+8	2457 MHz
13	13+9	2462 MHz

Weiterhin profitiert jeder einzelne Nutzer dank der insgesamt höheren Bandbreite, nämlich 300 MBit/s im Vergleich zu 54 MBit/s, von einer besseren Datentransferrate. Auf diese Weise lassen sich anspruchsvolle Unternehmensapplikationen erheblich schneller übertragen. Auch trägt die Dualband-Technologie zu einem stabileren Signal und folglich einer besseren Ausleuchtung der WLAN-Umgebung bei.

MIMO-Technologie für mehr Datendurchsatz

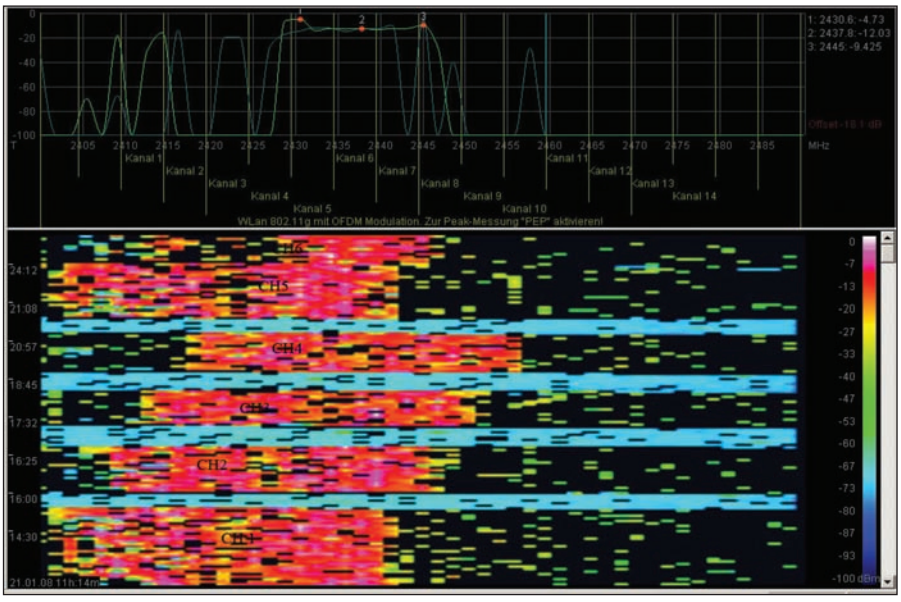
Einer der größten Vorteil der Wireless N-Technologie beruht auf dem Einsatz von MIMO (Multiple Input Multiple Output)-Mehrantennensystemen. Diese verwenden mindestens zwei Sende- und ebenso viele Empfangsantennen. Wireless N-Produkte werden stets mit der Eigenschaft von N x M Antennen beschrieben, wobei N die Anzahl der Sendeantennen und M die Anzahl der Empfangsantennen beschreibt. Das Prinzip der Antennen-Diversity ist zwar bereits von einigen 802.11g-Geräten bekannt, jedoch trifft es bei 802.11n mit einer weiteren neuen Eigenschaft zusammen – dem "Spatial Multiplexing". Hierbei wird zum einen entschieden, an welcher Antenne das qualitativ bessere Signal auf der Empfangsseite anliegt. Zum anderen schickt der Sender den Bitstrom verteilt auf seine Sendeantennen.

Das heißt, bei 4x4 MIMO kann sich der Bitstrom in vier separate Übertragungen aufteilen, die parallel übertragen werden. Auf der Empfängerseite erhält jede der vier Antennen ein Summensignal der Sendeantennen, das anschließend decodiert werden muss. Rein theoretisch können diese Geräte damit in der gleichen Zeit die vierfache Datenmenge übertragen, ohne zusätzliche Frequenzbandbreite zu benötigen. Voraussetzung dafür ist jedoch die mögliche Dekodierung der Empfangssignale an den einzelnen Empfangsantennen. Dies ist der Fall, wenn genügend Reflexionen durch eine Mehrwegeausbreitung der Sendesignale auftreten. Da dieses automatisierte Verfahren dynamisch arbeitet, ist eine Anpassung auch auf geänderte Umgebungsvariablen möglich.

Kanalbündelung im 2,4 GHz-Band

Der Frequenzbereich von WLAN im 2,4 GHz-Band reicht in Europa von 2.400 MHz bis 2.485 MHz. Für die Wireless Standards 802.11b/g und auch 802.11n stehen insgesamt 13 verschiedene Kanäle zur Auswahl. Die Bandbreite eines Kanals beträgt dabei circa 20 MHz. Anhand der Kanaltabelle 2,4 GHz-Band wird deutlich, dass sich einige Funkkanäle überschneiden, da der Kanalabstand nur 5 MHz zwischen zwei benachbarten Kanälen beträgt. Um die erforderliche Dämpfung von -20 dB zu erreichen, muss jedoch ein Abstand von mindestens 22 MHz eingehalten werden. Wird zum Beispiel Kanal 1 verwendet, ist der nächste freie Kanal die Nummer 6. Eine sinnvolle Kanalzuordnung wäre somit 1, 6, 11 oder 1, 7, 13 oder aber 1, 6, 13 et cetera. Der 802.11n-Standard sieht zur Erhöhung der Datendurchsätze eine Kanalbündelung vor, das heißt, es werden jeweils zwei bisherige 20 MHz-Kanäle zu einem 40 MHz-Kanal zusammengefasst. Gleichzeitig wird ebenfalls die Mittenfrequenz verschoben.

Demnach werden bis zu Kanal 4 höhere Kanäle gebündelt, ab Kanal 5 werden niedrigere Kanäle zusammengefasst. Dieser Effekt der Kanalbündelung kann am besten anhand einer Spektrumsanalyse veranschaulicht werden. In solch einer Spektraldarstellung wird grafisch dargestellt, dass ab Kanal 5 die Bündelung abwärts mit Kanal 1 erfolgt.



Spektrumsanalyse der gebündelten Kanäle 1 bis 6, mit Rot für starke Signale

Durchsatzraten und Stolpersteine in heterogenen Umgebungen

Überlappen sich nun 802.11n- und 802.11g-Produkte in einem Gebiet, so senden bei Verwendung der 40 MHz-Kanäle zwar die Wireless N-Geräte untereinander mit hohen Datendurchsatzraten, blockieren aber gleichzeitig freie Kanäle für die 802.11g-Clients. In der Folge leidet der Gesamtdatendurchsatz im WLAN. Um diese Koexistenz von 802.11b/g/n zu berücksichtigen, bieten Wireless N-Produkte die Konfigurationsmöglichkeit eines reinen 20 MHz- sowie eines 20/40 MHz Auto-Modus. Bei der Einstellung von 20 MHz müssen sich alle Stationen fest mit dieser Bandbreite verbinden. Der 20/40 MHz Auto-Modus erlaubt, dass sich Clients sowohl mit 20 MHz als auch mit 40 MHz verbinden können. Sind zu viele Störungen im Frequenzband vorhanden, schaltet der Access Point außerdem automatisch auf 20 MHz Kanäle zurück.

Im Hinblick auf die Durchsatzraten von Wireless N-Produkten ist darauf hinzuweisen, dass selbst geringere Werte zwischen 802.11n-Komponenten untereinander immer noch deutlich höher sind als jene, die zwischen 802.11b/g- oder 802.11a-Produkten realisiert werden können. So liegen die Wireless N-Netto-Datenraten üblicherweise bei circa 30 bis 40 MBit/s, während sie beim Standard 802.11g in der Regel Werte zwischen 13 und 16 MBit/s erreichen. In typischen Büroumgebungen, in denen die Signale reflektiert werden, betragen die Datendurchsätze bei Entfernungen bis zu 15 Metern zwischen 50 bis 70 MBit/s. In Umgebungen mit einem geringen Anteil anderer, auf der gleichen Frequenz funkender Geräte ermöglicht die 802.11n-Technologie auch Durchsätze von über 100 MBit/s (netto). Aktuelle Testergebnisse weisen für Dualband-Produkte sogar einen Netto-Datendurchsatz bis zu 189 MBit/s pro Router aus, unter der Voraussetzung, dass im 2,4- und 5 GHz-Frequenzband gleichzeitig gesendet wird.

Neuer Aufbau von WLAN-Netzwerken

Bei der Einbindung von Wireless N Dualband-Geräten in die IT-Infrastruktur von Unternehmen gilt es vor allem, die Kompatibilität beziehungsweise die Upgrade-Fähigkeit der zum Einsatz kommenden Komponenten zu prüfen. Außerdem müssen die MIMO-Mechanismen unter Nutzung der Reflexionen beachtet werden. Dies gilt insbesondere für Richtfunkstrecken und reflexionsarme Umgebungen. Beim Design heterogener WLAN-Netze mit vorhandenen 802.11-b/g-Geräten sollte der 20 MHz-Modus verwendet werden. Denn die Verwendung von 40 MHz-Kanälen birgt erhebliche Risiken für den Gesamtdatendurchsatz in dem bereits stark belegten 2,4 GHz-Frequenzband.

Hinzu kommt, dass die Steigerung der Netto-Datendurchsätze bei 40 MHz-Kanälen gegenüber 20 MHz-Kanälen nicht zu der angenommenen, theoretischen Verdoppelung der Datendurchsätze führt. Die Kanal-Verdopplung ist bei einigen Geräten standardmäßig deaktiviert, wodurch einer größeren Anzahl an WLAN-Clients freie Kanäle zur Verfügung gestellt werden. Ferner geht mit der deaktivierten 40 MHz-Kanalbündelung die Möglichkeit einher, im 2,4 GHz-Band Brutto-Datenraten von maximal 288,89 MBit/s zu erreichen; auf die Netto-Datendurchsätze wirken sich die Neuerungen allerdings eher marginal aus. Natürlich lässt sich auf Wunsch jederzeit die 40 MHz-Kanalbündelung aktivieren.

Fazit und Ausblick

Die Ratifizierung der Wireless-LAN-Spezifikation IEEE 802.11n beschleunigt die Ablösung des Wireless G-Standards und ebnet den Weg, Wireless N zur dominierenden drahtlosen Technologie der nächsten Jahre zu machen. Es ist zu erwarten, dass Firmen und Behörden die schnelle WLAN-Technik in stärkerem Maße als bislang implementieren werden und neben höheren Datendurchsätzen gleichzeitig die Reichweite sowohl im Innen- als auch im Außenbereich um den Faktor zwei bis drei steigern. In diesem Zusammenhang wird auch der Bedarf an Wireless N Parallel Band-Geräten steigen. Vor allem im industriellen Umfeld, in dem mittlerweile eine Vielzahl von Technologien basierend auf der 2,4 GHz-Frequenz funkt, ist für die Zukunft eine Anbindung von flexiblen Dualband Produkten nicht wegzudenken. *(ln)*

Dominik Fritzsche ist Produktmanager bei D-Link Deutschland.

IT-Service Management in der Praxis mit ITIL 3

Auch kleine und mittelständische Firmen können von den stark strukturierten ITIL-Prozessen profitieren. Ob dabei eine Zertifizierung erfolgt, spielt gar nicht die entscheidende Rolle. Alleine die Beschäftigung mit den Abläufen im Unternehmen, die ITIL automatisch mit sich bringt, deckt oft Engpässe und Sand im Getriebe auf. Wer noch Respekt vor dem Konzept ITIL hat, kann sich langsam mit "IT-Service Management in der Praxis mit ITIL 3" an das Thema herantasten. Martin Beims geht die Materie zwar gründlich an, bleibt mit 300 Seiten jedoch in einem Bereich, der nicht von Anfang an abschreckend wirkt. Trotzdem geht es methodisch zur Sache: ITIL wird kurz grundsätzlich beschrieben, dann stellt der Autor den Bezug zu typischen IT-Umgebungen und deren Anforderungen her. So bleibt es auch für den Rest des Buches. Es handelt sich zwar nicht um eine Anwendergeschichte, doch der Praxisbezug wird durchgehend aufrechterhalten. Wichtig ist das vor allem in den gut 100 Seiten, in denen die Theorie der Prozesse erläutert wird. Dabei helfen die zahlreichen Diagramme und Schaubilder, auch wenn sie manchmal für die Fülle der dargestellten Elemente etwas arg klein geraten sind.

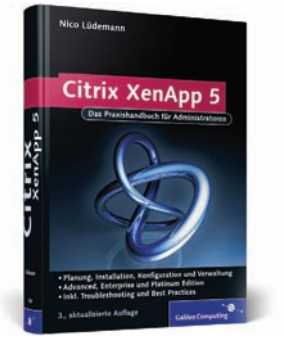
Nach der Prozessbeschreibung geht der Autor auf ISO 20000 und Prozessmanagement ein. Hier dürften nur noch Leser mitkommen, die bereits ITIL-Projekte gestartet haben. Beims handelt die Themen etwas knapp ab, Einsteiger müssen sich hier wohl Zusatzinformationen besorgen. Dafür ist das Beispielprojekt am Ende des Buchs sehr hilfreich für eigene Gehversuche mit ITIL. Die Vorgehensweise mit Tipps und Anleitungen kann in vielen Firmen direkt übernommen werden oder die Projektverantwortlichen zumindest in die richtige Richtung leiten. Man merkt, dass Beims aus der Praxis kommt und schon in einigen Firmen ITIL implementiert hat. Enthalten sind auch Checklisten und Musterdokumente, die dabei helfen, typische Anfängerfehler zu vermeiden.

Fazit: Mit dem Buch können IT-Verantwortliche mit vertretbarem Aufwand viel über ITIL lernen. Durch die Checklisten und das Praxisbeispiel eignet sich "IT-Service Management in der Praxis mit ITIL 3" auch, um die ersten Schritte zur Zertifizierung im eigenen Unternehmen anzustoßen.

Elmar Török

Autor:	Martin Beims
Verlag:	Hanser
Preis:	49,90 Euro
ISBN:	978-3-446-41320-7
Bewertung:	★★★★☆

Citrix XenApp 5



Früher wurde der Titel "Citrix XenApp 5" von Nico Lüdemann noch als "Citrix Presentation Server" herausgegeben. In der dritten Auflage hat sich neben dem Titel eine ganze Menge am Inhalt geändert. Der Einführungsbereich ist noch einmal dicker geworden und führt kurzweilig durch die Geschichte von Citrix und seiner Produkte. Ganz neu ist der Abschnitt über die Terminal Services von Windows Server 2008. Lüdemann geht auf die Unterschiede zur Vorgängerversion ein und zählt auf, was mit den Out-of-the-Box-Features machbar ist und was nicht. Wichtig dürfte für Citrix-Neulinge die Erläuterung des "großen Ganzen" sein. Der Autor zerlegt die Strategie von Citrix in verständliche Happen und beschreibt, wie die Bausteine aufeinander aufbauen.

Erhalten geblieben ist das ausführliche Kapitel über die Planung und Dimensionierung der XenApp-Umgebung. Dazu gehört auch eine kurze Übersicht der Lizenzmodelle – unverzichtbar bei den aktuellen Auswahlmöglichkeiten. Die eigentliche Installation beschreibt Lüdemann sehr ausführlich und mit zahlreichen Screenshots. Auch für die folgende Konfiguration nimmt sich der Autor viel Platz und simuliert diese anhand einer Musterfirma auf über 70 Seiten. Weil viele Unternehmen mittlerweile ihre Umgebung über die Terminalservices hinaus erweitern, geht der Autor im nächsten Abschnitt auf weitere Komponenten von XenApp ein. Anwendungsstreaming wird sehr ausführlich behandelt, EdgeSight, Network Manager, Access-Gateway und Webinterfaces werden ebenfalls beschrieben. Das "Best-Practice"-Kapitel ist das Highlight des Buchs. Lüdemann gibt darin Tipps für den Upgrade einer älteren XenApp-Version und zeigt, wie Anwendungen migriert werden können. Leider fiel ein Teil der Tipps für eine optimale Dokumentation den neuen Best-Practices zum Opfer. Und auch die Troubleshooting-Anleitung hätte gern über das Auflisten von Kommandozeilen-Tools hinausgehen können.

Fazit: Citrix XenApp 5 kann getrost als Standardwerk zum Thema bezeichnet werden. Es hat seine ganz besonderen Stärken bei der Konzeption und der optimalen Einrichtung eines Citrix-Systems.

Elmar Török

Autoren:	Nico Lüdemann
Verlag:	Galileo Computing
Preis:	47,95 Euro
ISBN:	978-3-8362-1390-5
Bewertung:	★★★★☆

www.archive.org

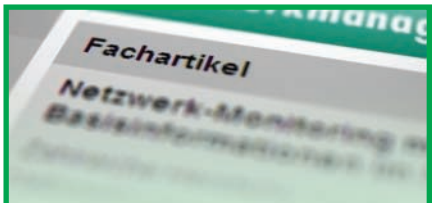
Zurück in die Vergangenheit

Ende Oktober 2009 war es soweit: das Internet wurde 40. Der Informatikprofessor Leonard Kleinrock und ein Student verbanden im Oktober 1969 einen Computer in Los Angeles mit einem Rechner in Stanford, immerhin 500 Kilometer entfernt. Gut 20 Jahre später, 1989, erfand dann Tim Berners-Lee das World Wide Web und machte das weltweite Datennetz so für die Masse an Nutzern interessant. Zahllose Webseiten tummeln sich heute in den Weiten des Internets und laufend kommen neue hinzu. Dabei gehen jedoch auch stets Inhalte verloren oder finden sich nur verstreut in den Caches von Suchmaschinen wieder.

Diesen Umstand hat das Projekt "Internet Archive" erkannt und archiviert seit 1996 die Webinhalte. Mit der "Wayback Machine" können Nutzer dabei das Vergangene zurückholen und längst gelöschte oder geänderte Webseiten betrachten. Die erste Homepage, die ehemalige Chatgemeinde oder die aus dem Netz verschwundene Infoseite sind so höchstwahrscheinlich in diesem digitalen Archiv hinterlegt und wieder auffindbar. Zwei Milliarden Webseiten hat das Internet-Archiv dabei nach eigenen Angaben bereits abgelegt, fein säuberlich nach Datum und URL sortiert. Mit dem "Archive-It"-Service finden Besucher auch digitale Kopien von Websites öffentlicher Einrichtungen. Darüber hinaus sind umfangreiche Materialsammlungen zu Ereignissen wie dem 11. September oder dem Hurrikan Katrina angelegt. Darin finden sich Links zu Webseiten, die sich mit den jeweiligen Themen befasst haben. Neuere Ereignisse fehlen bislang jedoch in der Sammlung.

Doch nicht nur Online-Inhalte archiviert das Projekt – auch Bücher finden ihren Weg in die digitale Lagerstätte. Über 1,5 Millionen Werke stehen so für die Besucher zum Online-Lesen etwa in PDF-Form zur Verfügung. Zahlreiche hauptsächlich amerikanische Bibliotheken unterstützen das Projekt und stellen Buchinhalte zur Verfügung. Suchen können die Nutzer die Bücher dann alphabetisch nach Titel oder Autoren sortiert. Und auch für Musikliebhaber hat das Internet-Archiv etwas zu bieten. Knapp 70.000 Musikstücke aus Live-Konzerten finden sich alphabetisch sortiert und lassen sich anhören. Daneben stehen zahlreiche weitere Audiodateien wie etwa Hörbücher und auch Filme bereit. In einem Forum schließlich können sich die Nutzer über ihre Lieblingsfundstücke austauschen. *(dr)*

Im Internet-Archiv finden sich alte und längst vergessene Webseiten-Inhalte wieder – hier am Beispiel der SuSE-Site



Unser Internetauftritt versorgt Sie jede Woche mit einem neuen interessanten Fachartikel. Dieser erklärt aktuelle Netzwerktechniken oder zeigt anhand eines Anwenderberichts ganz praktisch auf, mit welchen Lösungen Sie alltäglich anfallende Aufgaben leichter und effizienter erledigen können. Als Abonnent des IT-Administrator können Sie schon jetzt auf die Fachbeiträge zugreifen, noch bevor diese der Öffentlichkeit zur Verfügung stehen. **Diesen Monat erfahren Sie auf unserer Webseite mehr zu folgenden Themen:**

Hochverfügbarkeit für virtuelle Server

Virtualisierung liegt voll im Trend. Allerdings übersehen viele Unternehmen, dass durch das Zusammenlegen von Rechnern ein höheres Risiko entsteht, weil der Ausfall eines einzigen Servers nun eine ganze Produktivumgebung lahmlegen kann. Virtualisierte Server müssen daher besonders abgesichert werden. Wir stellen in unserem Online-Fachartikel verschiedene Wege zur Hochverfügbarkeit vor und beschreiben, wie Sie das Ausfallrisiko mit einer entsprechenden Software und nur wenig Aufwand minimieren.
www.it-administrator.de/themen/virtualisierung/fachartikel/69190.html

Automatisierte Softwarepaketierung

Fehlerhafte Installationen, die geschäftskritische Anwendungen zum Absturz bringen oder die Produktivität beeinträchtigen, resultieren oft daraus, dass die Verteilung von Software nicht sorgfältig genug vorbereitet wurde. Durch die Softwarepaketierung in das stabile MSI-Format lässt sich ein Setup erstellen, das unabhängig von der eingesetzten Software-Management-Lösung verteilt werden kann. Unser Online-Artikel gibt einen Überblick über den Status in der Softwarepaketierung, beschreibt den komplexen Prozess und geht dabei auf Windows Installer ein.
www.it-administrator.de/themen/server_client/fachartikel/69191.html

Überwachung virtualisierter Datenbanken

Virtualisierung stellt neue Anforderungen an das Monitoring immer komplexer werdender IT-Landschaften, vor allem, wenn auch Datenbanken in der virtuellen Umgebung betrieben werden sollen. Obwohl etwa Oracle den Betrieb von Datenbanken nur unter Verwendung der eigenen Virtualisierungs-Umgebung zertifiziert hat, werden die meisten virtuellen Datenbanken in der Praxis auf dem ESX-Server von VMware betrieben. Im Online-Fachbeitrag gehen wir darauf ein, wie Sie virtuelle Datenbanken im Auge behalten und Probleme wie die Überallokation von Arbeitsspeicher vermeiden.
www.it-administrator.de/themen/virtualisierung/fachartikel/69192.html

Besser informiert: Mehr Fachartikel auf der Website des IT-Administrator

»Virtualisierung ist ein wichtiger Faktor für Green IT«

Maria Siegert ist als IT-Administratorin für die über mehrere Standorte verteilte IT-Landschaft von Bioland verantwortlich. Rund 5.000 Biobauern sowie mehr als 800 Lebensmittel-Hersteller, darunter Bäckereien und Metzgereien sowie Molkereien, Brauereien oder Safthersteller, arbeiten nach den Richtlinien des Anbauverbands.

Welche Ausbildung haben Sie gemacht?

Ich bin Betriebswirtin und Quereinsteigerin in der IT. Im Laufe meines Berufslebens habe ich überwiegend bei kleineren Unternehmen gearbeitet und war dabei auch mit für die IT verantwortlich. Bei Bioland wechselte ich im Zuge einer Umstrukturierung dann vollends von der Finanz- in die IT-Abteilung.

Welche IT-Umgebung betreuen Sie?

Bei Bioland bin ich Leiterin der IT und zusammen mit zwei weiteren Mitarbeitern auch verantwortlich für die IT-Administration. Unsere Infrastruktur basiert auf rund 20 Servern, die deutschlandweit verteilt an zehn Standorten installiert sind. Bei den Betriebssystemen arbeiten wir sowohl mit Windows als auch mit Linux. Insgesamt betreuen wir etwa 410 interne und externe Arbeitsplätze.

Spielen Home Office-Arbeitsplätze bei Ihnen eine Rolle?

Ja, eine sehr große sogar. Wir haben eine ganze Reihe von Home Office-Arbeitsplätzen in unsere Strukturen integriert. Hinzu kommen mobile Arbeitsplätze. Insgesamt macht das etwa ein Drittel aller Clients aus.

Was sind im Hinblick auf die IT-Administration die größten Herausforderungen Ihres Arbeitsalltags?

Die sehr unterschiedliche Struktur der Anwender mit ihren verschiedenen Anforderungen und Anwendungen bereiten uns schon gelegentlich Kopfschmerzen. Erschwerend ist auch die Tatsache, dass wir bei einigen Lösungen noch mit unterschiedlichen Release-Ständen arbeiten sowie mobile Rechner oder die Installationen in den Home Offices zu betreuen haben.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Das nächste Hauptprojekt ist, unser Lotus Notes auf einen einheitlichen Versionsstand zu bringen. Das wird uns insgesamt dann auch den Support erleichtern.

Geburtstag: März 1963
Familienstand: verheiratet
Hobbys: Lesen, Segeln, Reisen

Maria Siegert, IT-Administrator

Was macht Ihnen an Ihrem Job am meisten Spaß?

Mir gefällt es, die Strukturen der IT permanent weiterzuentwickeln. Ich mache auch gerne Schulungen, da mir der unmittelbare Kontakt zu den Kollegen und Kolleginnen wichtig ist.

Was mögen Sie nicht so sehr, muss aber gemacht werden?

Die Feuerwehrfunktion, die wir Administratoren erfüllen müssen, kostet manchmal ganz schön Nerven. Ich mag auch die kleinen, nervigen Zeiträuber nicht – dazu gehören für mich Updates, Patches oder auch unplanbare Dinge, die meinen Zeitplan durcheinander bringen.

Was tun Sie für Ihre Fort- und Weiterbildung?

Sehr gute Erfahrungen habe ich mit der Donau Uni in Krems gemacht, die sich ganz auf die Weiterbildung von Berufstätigen spezialisiert hat. Hinzu kommen Messebesuche sowie das Lesen von Fachzeitschriften.

Was war der größte persönliche Flop oder Fehler, den Sie gemacht haben?

Ich bin inzwischen mehrmals mit Partnern aufgelaufen, die ich ausgesucht hatte. So schlitterte eine Firma, die sich um eine zusätzliche Programmierung für unser Lotus Notes kümmern sollte, ebenso in die Insolvenz wie ein Telekom-Anbieter, den ich ausgewählt hatte.

Was war Ihr größter Erfolg als IT-Administrator?

Eine große Herausforderung war die gute Anbindung unserer unterschiedlichen Standorte. Das war nicht immer ganz einfach, weil einige davon in extrem strukturschwachen Gebieten liegen.

Was war der dümmste Anwender oder Anwenderfehler, der Ihnen untergekommen ist?

Kürzlich hatte ein Kollege sein Notebook mit dem Auto überfahren. Der Rechner war in seinem Rucksack, den er beim Beladen seines Autos vergessen hatte. Glücklicherweise war die Festplatte nicht beschädigt und wir konnten die Daten retten. Das übrige Gerät war Schrott.

Was sehen Sie als die größte Herausforderung der IT in den nächsten drei Jahren?

Es muss immer im Blick bleiben, dass die IT dazu da ist, die Geschäftsprozesse zu unterstützen, sie aber auch ein Faktor im Wettbewerb ist. Ein wichtiges Thema sind sicher auch die zunehmenden Web-Anwendungen und auch die Virtualisierung wird sich weiter etablieren. Sie trägt dazu bei, Hardware zu reduzieren und Strom einzusparen.

Das Interview führte Petra Adamik.

Möchten Sie auch einmal das letzte Wort im IT-Administrator haben? Dann melden Sie sich einfach unter redaktion@it-administrator.de (Betreff: "Das letzte Wort"). Wir freuen uns auf Sie!

Was haben Sie zu sagen?

Die Ausgabe 1/10 erscheint am 8. Januar 2010

Schwerpunktthema:

Monitoring und Inventarisierung

Das lesen Sie in den nächsten Ausgaben des IT-Administrator:

Unsere Ausgabe im **Februar** steht unter dem Schwerpunkt **Sicherheit von Webservern und Applikationen**. In unserer Test-Rubrik nehmen wir die Application-Firewall Airlock von phion unter die Lupe. In einem unserer Workshops lesen Sie außerdem, wie Sie Ihren Apache-Webserver absichern.

Als Schwerpunkt im **März** folgt dann das Thema **Rechenzentrumsausstattung**.

Im Vergleichstest: Client Lifecycle Management-Suiten

Workshop: Service Pack 2 für Exchange Server 2007

Workshop: Storage-Management mit OpenFiler

Workshop: DNS-Fehler erkennen und beseitigen

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

IMPRESSUM

Redaktion
John Pardey (jp), *Chefredakteur*
verantwortlich für den redaktionellen Inhalt
john.pardey@it-administrator.de

Daniel Richey (dr), *Redakteur*
daniel.richey@it-administrator.de

Lars Nitsch (ln), *Redakteur*
lars.nitsch@it-administrator.de

Markus Heinemann, *Schlussredakteur*
markus.heinemann@email.de

Autoren dieser Ausgabe
Petra Adamik, Thomas Bär, Dominik Fritzsche, Sascha Giebelhausen, Christian Knermann, Robert Lindermeier, Sandro Lucifora, Thorsten Scherf, Dirk Srocke, Elmar Török, Hagen Will

Anzeigen
Anne Kathrin Heinemann, *Anzeigenleitung*
verantwortlich für den Anzeigenteil
kathrin@it-administrator.de
Tel.: 089/4445408-20

Es gilt die Anzeigenpreisliste Nr. 6 vom 01.01.2009

LAC/2008

Produktion / Anzeigendisposition
Lightrays: Lorenz Mueller, Andreas Skrzypnik
dispo@it-administrator.de
Tel.: 089/452196-90
Fax: 089/452196-89

Druck
Ceská Unigrafie, a.s.
U Stavoservisu 1
CZ - 100 40 Prag 10

Vertrieb
Anne Kathrin Heinemann
Vertriebsleitung
kathrin@it-administrator.de
Tel.: 089/4445408-20

Abo- und Leserservice:
Vertriebsunion Meynen GmbH & Co. KG
Stephan Orgel
Große Hub 10
65344 Eltville
leserservice@it-administrator.de
Tel.: 06123/9238-251
Fax: 06123/9238-252

Erscheinungsweise
monatlich

Bezugspreise
Einzelheftpreis: € 12,60
Jahresabonnement Inland: € 135,-
Studentenabonnement Inland: € 67,50
Jahresabonnement Ausland: € 150,-
Studentenabonnement Ausland: € 75,-
Jahresabonnement Inland mit Jahres-CD: € 144,84
Studentenabonnement Inland mit Jahres-CD: € 77,34
Jahresabonnement Ausland mit Jahres-CD: € 159,84
Studentenabonnement Ausland mit Jahres-CD: € 84,84
E-Paper-Einzelheftpreis: € 9,45
E-Paper-Jahresabonnement: € 99,-
E-Paper-Studentenabonnement: € 49,50
Jahresabonnement-Kombi mit E-Paper: € 168,-

(Studentenabonnements nur gegen Vorlage einer gültigen Immatrikulationsbescheinigung)

Alle Preise verstehen sich inklusive der gesetzlichen Mehrwertsteuer sowie inklusive Versandkosten.

Internet
www.it-administrator.de

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
80802 München

Tel.: 089/4445408-0
Fax: 089/4445408-99

(zugleich Anschrift aller Verantwortlichen)

Web: www.heinemann-verlag.de
E-Mail: info@heinemann-verlag.de

Eingetragen im Handelsregister des Amtsgerichts München unter HRB 151585.

Geschäftsführung / Anteilsverhältnisse
Geschäftsführende Gesellschafter zu gleichen Teilen sind Anne Kathrin und Matthias Heinemann.

ISSN
1614-2888

So erreichen Sie den Leserservice
Leserservice IT-Administrator
Stephan Orgel
65341 Eltville
Tel.: 06123/9238-251
Fax: 06123/9238-252
E-Mail: leserservice@it-administrator.de

Bankverbindung für Abonnenten
Konto 174 966 462 bei der
Postbank Dortmund, BLZ 440 100 46
Kontoinhaber: Vertriebsunion Meynen

So erreichen Sie die Redaktion
Redaktion IT-Administrator
Heinemann Verlag GmbH
Leopoldstr. 85
80802 München
Tel.: 089/4445408-10
Fax: 089/4445408-99
E-Mail: redaktion@it-administrator.de

So erreichen Sie die Anzeigenabteilung
Anzeigenverkauf IT-Administrator
Anne Kathrin Heinemann
Heinemann Verlag GmbH
Leopoldstr. 85
80802 München

Tel.: 089/4445408-20
Fax: 089/4445408-99
E-Mail: kathrin@it-administrator.de

INSERENTENVERZEICHNIS

Die Ausgabe enthält einen Beihefter der Firma IAIT zwischen Seite 34 und 35 sowie einen Beihefter der Firma REALTECH (Schirmherr 2009 der IT-Administrator User Group ITANet) zwischen Seite 50 und 51.

Das IT-Administrator Komplettprogramm!!!

Sichern Sie sich jetzt das **IT-Administrator Jahresabo All-Inclusive** mit allen Monatsausgaben, Sonderheften und der Jahres-CD.

Statt Euro 29,90 zahlen Sie dabei für jedes Sonderheft nur Euro 19,90 – und müssen keine zusätzliche Bestellung mehr tätigen.

Automatisch bekommen Sie im März und Oktober jeden Jahres das jeweilige IT-Administrator Sonderheft und mit Ihrer Dezemberausgabe die jeweilige Jahres-CD mit allen Monatsausgaben des Jahres im PDF-Format zugestellt.

Als bestehender Jahresabonnent können Sie hier upgraden:

www.it-administrator.de/abonnements/aboupgrade/

Oder Sie sind Neukunde? Hier können Sie bestellen:

www.it-administrator.de/abonnements/jahresabo/

www.it-administrator.de

Heinemann Verlag
Im Dialog mit Spezialisten.

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
D-80802 München
Tel: 0049-89-4445408-0
Fax: 0049-89-4445408-99
info@heinemann-verlag.de

Vertrieb, Abo- und Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville
Tel: 06123/9238-251
Fax: 06123/9238-252
leserservice@it-administrator.de

1&1 WEBHOSTING

HOMEPAGE

MIT BESTEN AUSSICHTEN FÜR 2010!

WEBHOSTING

Komplett-Lösungen für den perfekten Internet-Auftritt

z. B. 1&1 Homepage Business:
- 3 Inklusiv-Domains
- 5 GB Webspace
- UNLIMITED Traffic

3 Monate für 0,– €*

~~14,99 €/Monat*~~

Nach 3 Monaten zahlen Sie günstige 14,99 €/Monat.*

0,– €/Monat in den ersten 3 Monaten*

SERVER

Hochleistungs-Server für gehobene Ansprüche

z. B. 1&1 Dedicated Server Dual-Core XL:
- AMD Opteron™ 1218
- 2 x 2,6 GHz
- UNLIMITED Traffic

3 Monate für 0,– €*

~~99,99 €/Monat*~~

Nach 3 Monaten zahlen Sie günstige 99,99 €/Monat.*

0,– €/Monat in den ersten 3 Monaten*

ANGEBOTE NUR NOCH BIS 31.12.2009!

.de-Domain ein ganzes Jahr lang für 0,– €/Monat!*

Viele weitere attraktive Angebote im Internet!

*Einmalige Einrichtungsgebühr 9,60 € (bei 1&1 Homepage Business 14,90 € und bei 1&1 Dedicated Server 99 €). 12 Monate Mindestvertragslaufzeit. Preise inkl. MwSt.

MEMBER OF united internet

0180 5 / 001 535 14 ct/Min. dt. Festnetz, Mobilfunkpreise ggf. abweichend.

0800 / 100 668 Anrufe aus dem österr. Festnetz und Mobilfunknetz kostenfrei.

www.1und1.info

1&1