IT-ADMINISTRATOR.DE

02/2010

€ 12,60 ISSN 1614-2888

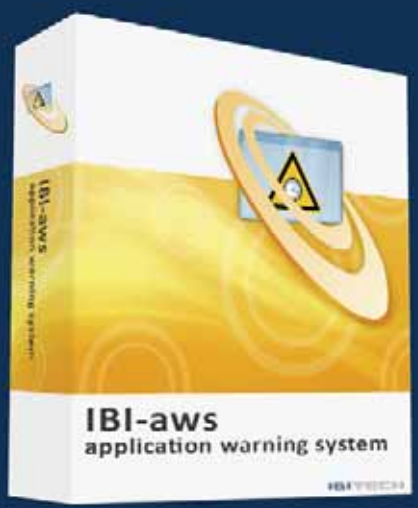
iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

Sicherheit von Webservern und -Applikationen

Und wie informieren Sie Ihre Anwender?

IBI-aws – die überlegene Informationslösung zwischen IT und Anwendern.



Informiert über Applikationsstörungen, IT-Probleme und Wartungsfenster.

- Zielgenaue Information
- Eingrenzung der Zielgruppe nach Applikation, IP-Bereich, AD-Gruppe
- Zeitliche Begrenzung der Meldung
- Verbindungslose Kommunikation
- Kein Setup benötigt
- Keine offenen Ports
- Keine Admin-Rechte notwendig
- Weniger Ressourcen, mehr Qualität
- Zufriedene Anwender und Supporter

mehr Info und Demo unter www.ibi-aws.de

EDITORIAL

Web-Anwendungen im Fadenkreuz

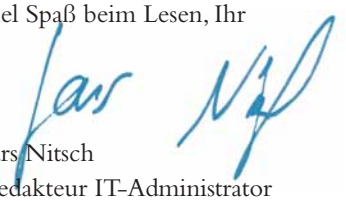
Liebe Leser,

Apple ist es zu verdanken, dass mobile Anwendungen – neudeutsch als "Apps" bezeichnet – derzeit in aller Munde sind. Neben den Schneehöhenständen der beliebtesten Skigebiete oder den Abfahrtszeiten der nächsten U-Bahn finden sich auch kuriose Tools: So erfreut sich ein Programm zur ballistischen Berechnung der Flugbahn einer Gewehrkugel großer Beliebtheit unter Scharfschützen in Afghanistan. Das Smartphone bezieht in seine Kalkulation unter anderem die Erdrotation und die vom Server geladene Wetterlage ein, um den Weg eines Geschosses zum Ziel möglichst genau vorherzusagen. Die passende Halterung für die Präzisionswaffe gibt es auf Wunsch gleich mit dazu.

Scharf geschossen wird jedoch nicht nur von, sondern vor allem auf Anwendungen. War vor Jahren der Betrieb eines Webservers aufgrund vorwiegend statischer Webseiten noch eine relativ ungefährliche Angelegenheit, öffnet sich heute wegen des dynamischen Charakters des Internets eine Vielzahl von Einfallstoren für wenig wohlmeinende Zeitgenossen. Cross-Site-Scripting, SQL-Injektionen oder Path-Traversal-Angriffe sind nur einige der Möglichkeiten, um über einen Webserver Schadcode ins Netzwerk einzuschleusen oder um sensible Informationen aus einer Datenbank auszulesen. Hinzu kommt, dass so beliebte Skriptsprachen wie PHP per se schon Sicherheitsrisiken in sich tragen, die letztendlich Sie als Administrator ausbügeln müssen. Aus diesem Grund haben wir in unserem Workshop ab Seite 42 unser Augenmerk darauf gelegt, wie Sie einen Webserver wirkungsvoll gegen unsichere PHP-Anwendungen härten.

Auch sonst steht diese Ausgabe im Zeichen der Web-Sicherheit: Ab Seite 12 lesen Sie in unserem Test, wie sich phions airlock als Schleuse für ausschließlich gutartige Dateneingaben schlägt. Wem die kommerzielle Version einer solchen Web Application Firewall nicht zusagt, der findet mit Hilfe unseres Workshops zur freien Linux-Distribution IPCop ab Seite 28 vielleicht eine Alternative. Auch für Ihre tägliche Arbeit erwarten Sie mit Beiträgen zur automatischen Verteilung von Windows 7 und zu den dabei entstehenden Upgrade-Kosten wieder eine Menge interessanter Themen. Immer mit dem Ziel, nicht nur Ihren Webserver vor Beschuss zu bewahren.

Viel Spaß beim Lesen, Ihr



Lars Nitsch
Redakteur IT-Administrator

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

INHALT

IT-Administrator – Ausgabe Februar 2010

Sicherheit von Webservern und -Applikationen

Im Test: GFI WebMonitor 2009

Der GFI WebMonitor 2009 ermöglicht IT-Verantwortlichen, alle firmeninternen Webseitenaufrufe und Downloads in Echtzeit zu überwachen und darüber hinaus zu steuern. Gemäß verschiedener Studien verwenden bis zu 40 Prozent der Mitarbeiter in Unternehmen ihren Firmenzugang auch für private Zwecke. Im Angesicht der möglichen Gefahren von Trojanern, nicht zulässigen Downloads oder Spionage-Tools ist dies ein in den seltensten Fällen zulässiges Risiko. Dieses Unheil im Zaum zu halten und ein sicheres Surfen im Internet zu ermöglichen, das verspricht die neueste Version des WebMonitors aus dem Hause GFI. IT-Administrator hat im Test untersucht, ob das Werkzeug dieses Versprechen einhält.

Seite 24

Web-Applikationen absichern

Seitdem sich PHP von der einfachen Skriptsprache für die Entwicklung dynamischer Webseiten zur objektorientierten Allzweckwaffe für Millionen von Web-Anwendungen entwickelt hat, steht PHP im Zentrum der Sicherheitsdebatte. Denn PHP-basierte Web-Applikationen bilden anno 2010 entweder als Web 2.0-Anwendungen oder in Form eines der zahlreichen PHP-basierten CMS-Systeme das Gros des modernen Web-Angebotes und stehen damit im Fokus der meisten Angriffs-Szenarien. In diesem Workshop zeigen wir Ihnen die wichtigsten Maßnahmen, um Ihre PHP-Umgebung gegen Angriffe zu härten.

Seite 42

Themenübersicht

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

Betriebssystem auf Reisen

Iomega bietet mit **v.Clone** eine Software an, mit der Nutzer ihr **Windows-Betriebssystem** als **Klon** auf eine externe Festplatte kopieren können, um es anschließend an einem anderen Rechner zu starten. Das Verfahren nutzt dabei eine VMware-basierte virtuelle Maschine und erstellt neben dem virtuellen Klon des Betriebssystems auch ein Abbild der Applikationen und Einstellungen. Diese sichert es auf einem externen Iomega-Laufwerk über eine USB-Verbindung. Schließt der Nutzer nun die externe Festplatte mit der v.Clone-Software an einen anderen PC an, kann er wie mit seinem Ursprungsrechner weiterarbeiten. Nach Beendigung der Arbeit bleiben mit Ausnahme der v.Clone-Applikation selbst keine Daten auf dem Zweitrechner zurück. Darüber hinaus synchronisiert die Lösung die Daten mit dem Datenbestand auf den Hauptrechner, sobald dieser wieder genutzt wird. Um sensible Daten und Nutzerinformationen, die auf dem v.Clone-Image gespeichert sind, zu schützen, stehen zwei Sicherheitsfeatures zur Verfügung. Die erste Sicherheitsstufe ist ein eingebauter Passwortschutz in der v.Clone-Anwendung. Nutzer, die kein passendes Passwort eingeben, haben keinen Zugang zur virtuellen Umgebung des Hauptrechners. Daneben kann v.Clone auch mit einer Iomega eGo Encrypt- oder Encrypt Plus-Festplatte genutzt werden, die eine Datenverschlüsselung vornehmen.

v.Clone steht für Käufer von externen Iomega-Festplatten ab sofort zum Download zur Verfügung. Noch im ersten Quartal will der Hersteller auch die portablen Iomega-Festplatten wie eGo, eGo Encrypt Plus, eGo BlackBelt und Prestige mit dem vorinstallierten Programm ausliefern. *(dr)*

Iomega: http://go.iomega.com/de/

"v.Clone" von iomega erlaubt, ein komplettes Betriebssystem auf eine externe Festplatte wie das Modell "Prestige" zu kopieren und auf jedem beliebigen Rechner zu starten

Firmen-Notebook für alle Ecken

Aus dem Hause **Lenovo** kommt eine neue Notebook-Serie mit der Bezeichnung **ThinkPad Edge**. Der Hersteller hat die 13-, 14- und 15-Zoll-Modelle laut eigenen Angaben speziell für **kleine und mittelständische Unternehmen** entwickelt. Der 13-Zoll-Rechner ist der erste ThinkPad mit AMD Dual-Core-Prozessor und AMD VISION Pro-Technologie, die bei der Ausführung von Collaboration-Anwendungen und visuellen Geschäftsapplikationen für eine erhöhte Performance sorgen soll. Je nach Variante und Ausstattung verspricht Lenovo dabei eine Batterielaufzeit von über acht Stunden. Die Geräte erfüllen die Energiespar-Richtlinie "Energy Star 5.0" und werden auf Wunsch mit zusätzlichen Service-Angeboten vertrieben. So etwa sorgt das Programm "Hard Disk Drive Retention" dafür, dass defekte oder beschädigte Festplatten beim Kunden bleiben, um die Sicherheit sensibler Daten zu gewähren. Gefeilt hat der Hersteller auch am Design – unter anderem kam es bei Funktionstasten und Touchpad zu einer Überarbeitung. Die 13-Zoll-Variante ist ab sofort zu einem Preis ab 570 Euro verfügbar, während die größeren Modelle erst im zweiten Quartal des Jahres in den Verkauf kommen. *(ln)*

Lenovo: www.lenovo.com/de/

Die neue Notebook Serie "Lenovo ThinkPad Edge" gibt es in den Formaten 13, 14 und 15 Zoll

Das ganze Netzwerk unter einer Haube

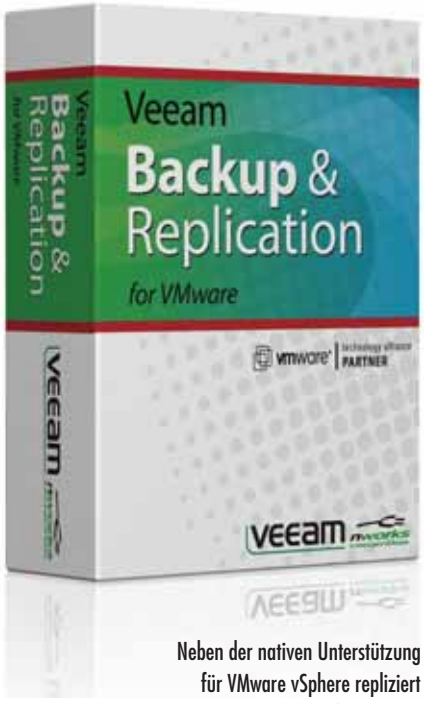
Aruba Networks präsentiert mit **AirWave7** die aktuellste Version seiner **Hersteller-übergreifenden Software zum Netzwerkmanagement**, welche die Verwaltung von drahtlosen Netzwerken, verkabelter Infrastruktur und mobilen Clients unter einer gemeinsamen Benutzerschnittstelle vereint. Der Anbieter hat das Werkzeug mit diversen neuen Funktionen ausgestattet. Dazu zählt unter anderem der "AirWave Mobile Device Manager", der Endgeräte vom Handheld bis zum drahtlosen Drucker steuert. Die "AirWave Management Platform" kommt jetzt auch mit Edge-Switches von Cisco und HP zurecht und will so das Management von verkabelter und drahtloser Infrastruktur zusammenführen. Zusätzlich verfügt die Software über eine offene XML API-Architektur, welche die Kooperation zwischen AirWave7 und übriger IT-Infrastruktur-Managementsoftware verbessern soll. Nicht zuletzt sorgen anpassbare Benutzerschnittstellen und individuelle Dashboards dafür, dass Nutzer für jede Rolle eine spezifische Sicht auf die Daten erstellen können. Zusätzlich lassen sich eigene Reporte definieren und speichern. Das Produkt ist als reine Softwarelösung, installiert auf einer Appliance oder als Software-as-a-Service, ab März erhältlich. Der Preis richtet sich nach der Anzahl der verwalteten Geräte, eine Lizenz für 50 Devices kostet knapp 3.000 US-Dollar. *(ln)*

Aruba Networks: www.arubanetworks.com/company.de.php

Mehr Replikationswege in virtualisierten Umgebungen

Veeam bringt Version 4.1 von **Backup & Replication** für VMware auf den Markt. Zu den Neuerungen der **Disaster Recovery-Software für virtualisierte Umgebungen** zählt die vollständige Unterstützung für die Replikation auf ESXi-Hosts in der Kaufbeziehungsweise lizenzierten Version von ESXi. Nutzer des Programms sollen so über die Möglichkeit verfügen, einen Failover sowohl zum letzten als auch zu vorherigen Points-in-Time bei der Replikation auf ESXi durchzuführen. Durch die Nutzung von vStorage API und VMware Consolidated Backup lassen sich Backup und Replikation anstoßen, ohne den laufenden Betrieb der virtuellen Maschinen zu beeinflussen. Außerdem versendet die Software nun SNMP-Benachrichtigungen, etwa wenn ein einzelner Backup-Job oder die Replikation einer virtuellen Maschine abgeschlossen ist. Zudem bietet sich die Gelegenheit, beim Tape-Backup ein Standalone-Utility mit auf Band zu spielen, das ein Hersteller-unabhängiges Recovery der Daten auch ohne die Veeam-Software möglich macht. Das Werkzeug ist ab sofort erhältlich und kostet bei einer Lizenzierung pro Prozessor 510 Euro. *(ln)*

Veeam: www.veeam.com/de/product.html#1



Neben der nativen Unterstützung für VMware vSphere repliziert "Veeam Backup & Replication" nun auch auf ESXi-Hosts

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

Der **IT-Administrator** ist nun auch auf der Networking-Plattform **Xing** als Gruppe präsent. Damit will die Redaktion den Lesern und Admins in Xing einen **interaktiven Austausch** untereinander sowie mit den Autoren des Magazins ermöglichen. Welche Themen bewegen Sie zurzeit? Was wollten Sie schon immer mal fragen? Und wie sehen Sie den IT-Administrator? Mitglied werden kann jeder Administrator, der sich gerne mit den Kollegen und Heftmachern austauschen möchte. Wir freuen uns auf Ihre Teilnahme. *(dr)*

www.xing.com/net/itanet

Netgear stellt mit den Modellen **DGN2200M** und **MBRN3000** zwei neue Router vor, die den Internetzugang über **3G-, 4G- und WiMAX-Mobilfunknetze** ermöglichen. Der 3G- und 4G-Mobile Broadband Wireless-N Router MBRN3000 kombiniert 802.11n-WLAN mit Unterstützung des Zugangs zu Hochgeschwindigkeits-Mobilfunknetzen über ein externes Funkmodem. Der Wireless-N 300 Router mit DSL Modem in der Mobile Broadband Edition DGN2200M bietet zudem ein ADSL2+-Modem. Damit ermöglicht das Gerät eine DSL-Verbindung bei paralleler Ausfallsicherheit über Breitband-Mobilfunk. Ab dem zweiten Quartal 2010 sollen die Router auf dem Markt verfügbar sein. Die Preise standen zu Redaktionsschluss noch nicht fest. *(dr)*

www.netgear.de

IGEL Technology stattet die Linux- und Windows Embedded Standard-basierten Thin Clients der Reihe **Universal Desktop** mit dem neuen VDI-Client **VMware View 4** aus. Der Softwareclient beinhaltet das neue Displayprotokoll PC-over-IP (PCoIP), das VMware speziell für den Zugriff auf virtuelle Desktops entwickelt hat. Dabei handelt es sich um ein leistungsfähiges Anzeigeprotokoll speziell für die Bereitstellung virtueller Desktops über WAN- oder LAN-Verbindungen. Die neue Firmware steht zum kostenfreien Download auf der Herstellerseite bereit. *(dr)*

www.myigel.com

Clavister erweitert die UTM-Appliances der Serie **Security Gateway 4300** um **zusätzliche Hardware-Komponenten**. So sind die Geräte ab sofort optional mit einer redundanten Stromversorgung sowie einem austauschbaren Lüfter-Modul ausgestattet. Das integrierte VPN-Modul liefert laut Hersteller bis zu 10.000 simultane VPN-Tunnel mit einem Datendurchsatz von 2,5 GBit/s und erlaubt auch Hosted-VPN-Services. Zudem unterstützen die Torwächter das neue zentralisierte Managementsystem "InControl". Der Preis für die Clavister 4300 SG-Serie beginnt bei rund 9.000 Euro. *(ln)*

www.clavister.com

Ein-Prozessor-Server für schmale Geldbörsen

Fujitsu stellt mit den Modellreihen **TX150 S7** und **RX100 S6** eine neue Generation seiner **Primergy Ein-Prozessor-Server** vor. Bei der T-Variante handelt es sich um einen Computer im Tower-Format, der in Versionen mit zwei oder vier Rechenkernen erhältlich ist. Konzipiert wurde der Server für KMUs oder den Einsatz in dezentralen Infrastrukturen. Zudem ist er laut Hersteller der einzige Ein-Prozessor-Server, der optional eine Hot-Plug-Stromversorgung bietet. Dies soll die Verfügbarkeit des Geräts verbessern und den Rechner attraktiver für den Einsatz als Virtualisierungs-Host machen. Die zweite Modellreihe ist für den Einbau im Rack gedacht, wo sie als Terminal- und Infrastruktur-Server oder in Webserver-Farmen zum Einsatz kommen kann. Das modular aufgebaute Festplattenkonzept unterstützt entweder zwei 3,5-Zoll- oder vier 2,5-Zoll-Laufwerke. Die verschiedenen RAID-Konfigurationen kommen mit SATA-, SAS- und SSD-Speichern zurecht. Beide Modelle sind mit PCIe-Slots gemäß dem Standard Gen2 ausgestattet und verfügen über SAS 2.0-Schnittstellen. Nutzer können die Rechner auf maximal 32 GByte Arbeitsspeicher erweitern. Das Tower-Modell schlägt in einer Ausstattung mit einem Intel X3430-Prozessor, 4 GByte RAM, einem DVD-RW-Laufwerk und zwei Festplatten zu je 160 GByte mit knapp 1.200 Euro zu Buche. *(ln)*

Fujitsu: http://de.ts.fujitsu.com/products/standard_servers/

Rundum-Erfassung

Mit **Version 5.0** erweitert **itelio** den Funktionsumfang der **Netzwerkdokumentationslösung Docusnap**. Mit der Software lässt sich das **Netzwerk inventarisieren und dokumentieren**. Im Release 5 erfasst und verarbeitet die Software nun rund 40 Prozent mehr Daten als in der Vorgängerversion. Die gespeicherten Daten werden in mehr als 50 neuen Berichten visualisiert. Die Erfassung und Dokumentation von Netzwerkumgebungen ist nun nicht mehr auf physikalische Rechner und IT-Umgebungen begrenzt. Mit dem neuen Modul "VMware" werden auch die Daten von virtuellen Rechnern und Netzwerken auf Basis von VMware/ESX Server und VirtualCenter ausgelesen und dargestellt. Das Modul "Lizenzverwaltung" hat der Anbieter zudem um einige wesentliche Funktionen erweitert, die den Abgleich von installierten und gekauften Lizenzen komfortabler gestalten sollen. Verschiedene Lizenzkategorien und Lizenztypen können nun angelegt werden, wahlweise ist dabei die Zuweisung von Lizenzen auf User, Geräte oder Prozessoren möglich. Im Modul "Exchange Server" ist mit Version 5.0 nun auch die Erfassung von Exchange Server 2007-Umgebungen möglich. Neben der reinen Inventarisierung lässt sich auch eine Dokumentation von öffentlichen Ordnern erstellen. Für Linux-Nutzer erfasst die Software im Bereich der Serverkonfiguration bei Apache und Samba außerdem mehr Daten als bisher. Mit Docusnap 5.0 können Nutzer zudem ohne manuellen Eingriff den automatischen Start einer Inventarisierung und Dokumentation zu definierten Zeitpunkten einleiten. Ist ein mobiles Gerät zum Zeitpunkt des Scans nicht im Netzwerk angemeldet, wird die Inventarisierung skriptbasiert automatisch nachgeholt. Für eine Active Directory-Umgebung mit 25 Computerkonten kostet die Basislizenz lediglich 200 Euro. Wird zusätzlich das Modul-Bundle Exchange-SQL-DHCP/DNS-VMware-Lizenzverwaltung-Rechteanalyse gewünscht, beträgt der Preis 380 Euro. *(dr)*

itelio: www.docusnap.de

Kompakter Windows-Speicherserver

Buffalo Technology stellt die **TeraStation Windows Server WS-QL** für den Einsatz in SoHo- und KMU-Umgebungen vor. Das Speichergerät basiert auf dem **Windows Storage Server 2003 R2** in der Express Edition. Dank der Remote-Administration über die Windows Storage Server-Oberfläche auf Basis der Microsoft Management Console (MMC) soll die nahtlose Einbindung in bestehende Windows-Umgebungen möglich sein. Die Protokollunterstützung für SMB/CIFS und NFS/SMB sowie die Integration in das Active Directory sorgen zusätzlich für eine schnelle Einrichtung. Zugriffsrechte können dabei ohne Einschränkungen vergeben und vorhandene Lese- und Schreibberechtigungen in Ordnern und Dateien 1-zu-1 übernommen werden. Die Datensicherheit des Windows Server wird durch den redundanten Verbund der vier SATA-II-Festplatten mit bis zu 4 TByte Gesamtkapazität in den RAID-Modi 0, 1 oder 5 und ergänzende Authentifizierungs- und Verschlüsselungs-Features gewährleistet. Dank der Deduplizierungsfunktion "Single Instance Storage" (SIS) spart die Storage-Lösung zudem Speicherplatz, indem sie mehrfach vorhandene identische Dateien nur einmal speichert. Für die Anbindung an das Netzwerk steht ein GBit-Ethernet-Port zur Verfügung. Für rund 1.200 Euro ist der Speicher-Server erhältlich. *(dr)*

Buffalo: www.buffalo-technology.de

Die TeraStation WS-QL von Buffalo basiert auf Windows Storage Server 2003

Die neue Server-Klasse!

Die neuen Enterprise Server von webtropia.com, leistungsstarke Hardware, kompromissloser Service

Hardware

- **Dual Quad-Core Xeon CPUs** mit gesamt 16 Ghz
- **Intel-Server** Hardware mit Remote Management
- Bis zu **16 GB DDR3-RAM**
- **1000 Mbit** Anbindung an **120 Gbit** Backbone
- **SLA mit 99,9 %** garantierter Verfügbarkeit
- Bereitstellung innerhalb von **24 Stunden**

Features

- Monatliche Laufzeit, monatliche Zahlung, Festpreis
- **24/7 kostenloser Support**
- **Plesk 9** oder **Confixx 3** als Admin-Tool
- Freie Betriebssystem-Auswahl:
  Debian 5.0, openSUSE 11.2, centOS 5.3,
  Windows 2008 (19,99€/Monat)

	Enterprise Server X-8	Enterprise Server X-12	Enterprise Server X-16
Prozessor	2 x Xeon - E5504	2 x Xeon - E5504	2 x Xeon - E5504
Leistung	2 x 4 x 2,0 Ghz	2 x 4 x 2,0 Ghz	2 x 4 x 2,0 Ghz
Arbeitsspeicher	8 GB DDR3-RAM	12 GB DDR3-RAM	16 GB DDR3-RAM
Festplatte	2 x 1000 GB SATAII	2 x 1500 GB SATAII	4 x 1000 GB SATAII
Hardware Raid	Ja	Ja	Ja
Traffic	4000 GB	5000 GB	6000 GB
Extras	Reboot-, Rescue-, Monitoring- und Domain-Registrierungs-System		
Vertragslaufzeit	1 Monat	1 Monat	1 Monat
Monatsgrundgebühr	**€ 119,99**	**€ 139,99**	**€ 159,99**

webtropia.com

Microsoft CERTIFIED SPLA MEMBER

Parallels PLATINUM PARTNER

Tel.: 0800 - 9328767
www.webtropia.com

IT-Administrator-Workshop "VoIP im Unternehmensnetz" am 25. Februar 2010 in München

ITANet Workshop-Partner:

Netcordia™
Simply a better way to manage

Bestmögliche Verbindung

von Mathias Hein und John Pardey

Quelle: mipan - Fotolia.com

Neben Messungen im Netzwerk, die vor der Einführung von Voice over IP erfolgen sollten, zeigt unser Februar-Workshop, wie Quality of Service im täglichen Betrieb gewährleistet wird. Dabei erfahren die Teilnehmer, welche Parameter die Sprachqualität beeinflussen und wie diese zu messen sind. Dozent Mathias Hein zeigt dabei im Rahmen einer Live-Demo, wie typische Fehler zu identifizieren und zu beheben sind. So stellen Verzögerungen, Jitter und Paketverluste keine VoIP-Installation mehr vor unüberwindbare Probleme.

Der Oberbegriff Quality of Service (QoS) beschreibt eine Serie von Parametern, die für eine fehlerfreie Übermittlung von Sprache und Video notwendig sind. Erst die Einhaltung dieser Parameter auf der gesamten Strecke sorgt für die notwendige Übertragungsqualität und Serviceverfügbarkeit. Die ultimative Messgröße zur Beurteilung der Übertragungsqualität ist der Anwender. Bei der Sprachübermittlung hängt die Beurteilung der Güte von subjektiven Kriterien ab. Auf die wichtigsten Parameter geht unser Workshop ein.

Sprachqualität messen

Die Sprachqualität beschreibt, wie gut die Verständlichkeit einer menschlichen Stimme bei Aufzeichnung und Wiedergabe durch die technischen Einrichtungen (Endgeräte, Netzwerkkomponenten, Gateways) ist. Die Bewertungskriterien der Sprachqualität sind unter anderem durch die ITU-Bewertungsmethoden im Standard P.800 spezifiziert.

Das bekannteste Sprachbewertungsverfahren ist der so genannte "Mean Opinion Score" (MOS). Mit Hilfe des MOS werden die Übertragungsqualitäten unterschiedlicher Sprachströme und Codierungen miteinander verglichen. Der MOS-Wert wird subjektiv ermittelt, indem Sprechproben den Probanden vorgespielt, die einzelnen Bewertungen gewichtet und daraus die statistischen Ergebnisse ermittelt werden. Beim MOS handelt es sich um einen Wert zwischen eins und fünf, der für die Sprachqualität steht; wobei der Wert "1" eine mangelhafte Sprachqualität repräsentiert, bei der keine Verständigung möglich ist, der Wert "5" hingegen für eine exzellente Übertragungsqualität steht, die nicht vom Original zu unterscheiden ist.

Der PESQ-Algorithmus spezifiziert in der ITU-Vorschrift P.862 ein weiteres aktives Berechnungsmodell zur Bestimmung der Sprachqualtiät und basiert auf den realen Bedingungen einer Ende-zu-Ende-Sprachkommunikation. Das Verfahren berücksichtigt unter anderem Paketverluste, Rauschen und den verwendeten Sprachcodec. Bei der PESQ-Analyse wird ein Referenzsignal und das durch die Übermittlung über das Netzwerk geminderte Sprachsignal in das System eingegeben. Dabei werden alle Fehler sichtbar, auch diese, die außerhalb des IP-Netzwerks liegen.

Faktoren einer verringerten Sprachqualität identifizieren

Die Verzögerung beschreibt die Latenzzeit zwischen dem Auftreten eines Ereignisses und dem Auftreten eines erwarteten Folgeereignisses, um das ein Ereignis verzögert wird. In Netzwerken wird die Verzögerung oft mit dem Begriff Round Trip Time (RTT) beschrieben. Der Round Trip Delay beschreibt die Gesamtverzögerung (beide Wege) zwischen zwei IP-Endpunkten. Bei Voice over IP-Anwendungen und Videokonferenzen ist das so genannte One Way Delay (die Verzögerung in einer Richtung von Startpunkt zu Endpunkt) von Bedeutung.

Netzwerkverzögerungen werden durch die physische Verzögerung der Übertragungsleitungen, der Queuing- und Pufferungsmechanismen in den Koppelkomponenten (Router, Switches, Gateways) verursacht

und variieren in ihrem Ausmaß. Die so genannte Durchlaufzeit setzt sich aus einer konstanten oder nur leicht variierenden Netzverzögerung und schnellen Schwankungen der Verzögerung, gemeinhin als Jitter bekannt, zusammen.

Wie Sie in unserem Workshop sehen werden, stellt Jitter ein Taktzittern bei der Übertragung von Digitalsignalen beziehungsweise eine leichte Genauigkeitsschwankung im Übertragungstakt dar. In der Netzwerktechnik wird mit Jitter außerdem die Varianz der Laufzeit von Datenpaketen bezeichnet. Dieser Effekt ist insbesondere bei interaktiven Multimedia-Anwendungen störend, da dadurch Pakete zu spät eintreffen können, um noch zeitgerecht mit ausgegeben werden zu können. Dies wirkt sich wie eine erhöhte Paketverlustrate aus. Treffen die Pakete regelmäßig beim Empfänger ein, können diese direkt in Audio/Videosignale umgesetzt werden. Da die Verzögerungen bei der Übertragung nicht konstant sind, entstehen Lücken im abgespielten Signal. Die Differenz zwischen den Verzögerungen einzelner Pakete wird als Jitter (Verzögerungsschwankung) bezeichnet. Zur Vermeidung von Lücken im Signal müssen die empfangenen Daten in einem Zwischenspeicher abgelegt werden. Dieser Zwischenspeicher hat die Aufgabe, die Lücken zwischen verspäteten Paketen zu kompensieren. Die Größe dieses Zwischenspeichers (Synchronisationspuffer oder Jitter-Buffer) kann ein oder mehrere Frames umfassen. Durch die Pufferung mehrerer Sprachpakete/Video-Frames kann ein größerer Jitter ausgeglichen werden. Durch den Einsatz von einem größeren Jitterbuffer wird jedoch die Gesamtverzögerung negativ beeinflusst. Hier liegt die Kunst darin, die optimale Abstimmung der Puffergröße zu finden.

Die Paketverlustrate ist ein Maß für die Übertragungsqualität einer Datenverbindung. Die Paketverlustrate definiert, wie viele Pakete eines Datenstroms zwischen einem Sender und einem oder mehreren Empfängern während der Übertragung verloren gegangen sind. Die Paketverlustrate berechnet sich aus dem Verhältnis der Anzahl verloren gegangener zur Anzahl gesendeter Datenpakete. Um eine gute Verbindung zu haben, sollte dieser Fehlerwert so klein wie möglich sein. Optimal ausgelegte und gut administrierte IP-Backbones weisen heute in der Regel eine Paketverlustrate von weniger als 0,5 Prozent auf. Für die Übermittlung von VoIP-Datenströmen gilt gemäß der ITU G.114-Spezifikation eine Paketverlustrate bis zu 5 Prozent als noch akzeptable Qualität.

Diesen und vielen weiteren Themen (siehe Kasten "Agenda") wendet sich Mathias Hein in unserem Workshop am 25. Februar zu. IT-Verantwortliche, die den Einstieg in VoIP vor Augen haben oder aktuell Probleme mit der Sprachübermittlung in ihrem Unternehmensnetzwerk beobachten, sollten diesen Workshop nicht verpassen. Die Anmeldeinformationen finden Sie im Kasten auf dieser Seite. Der für alle Abonnenten kostenlose Workshop steht ab sofort zur Registrierung offen und wir würden uns freuen Sie in München begrüßen zu dürfen.

Agenda des Workshops "VoIP im Netz" am 25. Februar

iTANet
Die System und Netzwerk User Group

Die Agenda des Workshops

13.00 Uhr: Begrüßung

13.15 Uhr: Voice over IP - Teil 1

- Status des Marktes/Marktentwicklungen
- Problembereiche bei VoIP
  - Verzögerung
  - Packet Loss
  - Jitter
  - Gateways/NATs
  - SIP Trunks
- Ohne QoS geht die Sprache im Netz verloren

Dozent: Mathias Hein

14.30 Uhr: Kaffeepause

14.45 Uhr: Avoiding 8 out of the 10 Network Failures

Dozent: Simon Horrocks, EMEA Regional Sales Manager Netcordia
(Vortrag in englischer Sprache)

15.30 Uhr: Voice over IP - Teil 2

- Messszenarien mit Live-Demo zur Fehlersuche für den Praktiker:
  - Vormessungen
  - E-Model vs. PESQ
  - Sprachanalyse
  - Langzeitmonitoring
- Ausblick in die Zukunft

Dozent: Mathias Hein

17.30 Uhr: Ende des Workshops

Ort: ExperTeach Training Center, Wredestraße 11, 80335 München

Teilnahmegebühren:
Für IT-Administrator Abonnenten kostenlos.

Anmeldung bis zum 20. Februar unter
www.it-administrator.de/workshops

Mathias Hein verfügt über 25 Jahre Berufserfahrung und arbeitet als freier IT-Berater und Fachautor. Daneben ist er an der FH Reutlingen und der Berufsakademie Mannheim als freier Dozent tätig. An der ComConsult Akademie ist er Referent für die Themenbereiche Switching, TCP/IP und Netzmanagement. Als freier Autor im Fachbuchbereich und in den einschlägigen Fachzeitschriften trägt Mathias Hein regelmäßig zur Wissensvermittlung bei.

Mathias Hein erhielt zum Beginn seiner Karriere als einer der ersten Netzwerker in Deutschland die Aufgabe eines Produktspezialisten bei dem Distributor Wetronic (München). In seinen anschließenden Tätigkeiten als technischer Leiter bei Fuba Communication (Hilden) und Rockwell Communications (London) erwarb er sich den Ruf als pragmatischer Troubleshooter im Bereich der Netzwerke. Von 1990 bis 1994 arbeitete Hein als freier Unternehmensberater (Netzanalyse, Planung, Projektierung und Implementierung) sowie als TCP/IP-Trainer für diverse Schulungsunternehmen. Anschließend arbeitete er fünf Jahre als Marketingmanager für Bay Networks (Deutschland, Österreich und Schweiz). Seit 1999 ist er als freier Unternehmensberater, Autor und Trainer tätig.

Der Dozent

Im Test: phion airlock 4.2

Die Luftschleuse zum Internet

von Sandro Lucifora

Alle Web-Applikationen haben gemeinsam, dass sie Hackerangriffen fast schutzlos ausgesetzt sind. Mit der Version 4.2 der Web-Application-Firewall airlock bietet phion eine Lösung an, die maximale Sicherheit bei minimalem Aufwand verspricht. Sie arbeitet wie eine Luftscheuse zwischen dem Internet und den Servern und filtert schädliche Anfragen auf Anwendungsebene heraus. IT-Administrator hat getestet, ob die Software-basierte Firewall hält, was der Hersteller verspricht.

Früher waren Internetseiten statische, allenfalls zum Teil dynamische Informationsquellen für die Besucher. Zwischenzeitlich bieten viele Seiten ein interaktives Datenmanagement von persönlichen und Unternehmensdaten an. Im Ergebnis wird aus dem einfachen Webserver ein relevanter Applikationsserver, der direkten Zugriff auf sensible Daten hat. Der derzeit beste Schutz für eine Web-Applikation ist es, den Server vom Internet zu trennen. Da dies jedoch dem Sinn und Zweck widerspricht, muss ein möglichst sicherer Übergang zwischen Server und Internet die dahinter liegenden Anwendungen schützen. Diese Aufgabe übernimmt eine Web-Application-Firewall – kurz: WAF. Die WAF ist das Bindeglied zwischen dem Inter- und Intranet. Der Applikationsserver erhält eine interne IP-Adresse und ist von außen nicht mehr direkt erreichbar. Die erste Anlaufstelle für eine Anfrage aus dem Internet ist somit die WAF. Sie prüft die Anfragen auf schädliche Inhalte und leitet nur unbedenkliche Daten an den Server weiter.

Der Aufbau von airlock

phion airlock ist als reine Softwarelösung auf kompatiblen Hardware-Plattformen einsetzbar. Die Installation ist auch in einer virtuellen Maschine unter VMware möglich. Berücksichtigt werden muss in jedem Fall, dass die Auswahl der Hardware für die spätere Leistungsfähigkeit der Web-Application-Firewall (WAF) maßgeblich ist. Wer VMware einsetzt, muss dazu noch die VMware-Tools auf Betriebssystemebene nachinstallieren. Die Installation ist auch unter Microsoft Hyper-V möglich, wird jedoch vom Hersteller nicht offiziell unterstützt. Als Grundlage verwendet airlock Sun Solaris 10. In unserem Test hatten wir die Firewall sowohl unter VMware Server als auch als eigenständige Software-Appliance im Einsatz. Die Installation ist recht einfach – CD rein, System starten, einige Parameter angeben, fertig.

Grundsätzlich kann airlock direkt ins aktive Netzwerk eingebunden werden. Da phion seine WAF jedoch als Enterprise-Lösung entwickelt hat, bieten sich redundante sowie Testinstallationen an. Diese unterstützt der Hersteller sehr deutlich mit seiner Lizenzpolitik. So kostet die zweite Lizenz im Cluster als Failover nur 40 Prozent, eine Lizenz für ein Testsystem sogar nur zehn Prozent des regulären Preises. Vorwegnehmen können wir, dass airlock 4.2 einen Abgleich der Konfigurationen auf Knopfdruck vom Produktiv- zum Failover-System oder vom Test- zum Produktivsystem nicht unterstützt. Dies kann nur mittels Ex- und Import auf den jeweiligen Systemen erfolgen – hier sollte der Hersteller in jedem Fall nachbessern.

Konfiguration und Funktionen

Je nachdem, wie die WAF in die Infrastruktur eingebunden wird, fällt die erste Konfiguration aus. Wir haben im Test eine WAF im Netzwerk betrieben und so eingerichtet, dass die Verbindung zum Applikationsserver über die Schnittstelle "alta0" und das Management über ein separates Subnetz auf "alta2" erfolgt (sie-

- Sichere Reverse Proxy Terminierung von TCP/IP, SSL, HTTP/S und SOAP/XML
- Multi-Level Filtering
- Dynamisches White-Listing
- URL-Verschlüsselung
- Smart Form Protection
- Cookie Store
- Load Balancing
- ICAP Content Filtering
- Content Rewriter (Raw, HTML)
- Access Control und Single-Sign-On
- SOAP/XML Filter

Sicherheitsfunktionen von airlock

Bild 1: Die Netzwerkanbindung ist dank übersichtlichem GUI schnell eingerichtet

he Bild 2). Von großem Vorteil ist, dass phion die Konfiguration in airlock nicht sofort scharf schaltet. Somit können Administratoren unabhängig vom Betrieb Einstellungen verändern und diese erste bei Bedarf aktivieren oder exportieren.

Die Version 4.2 hat eine komplette Überarbeitung der Oberfläche erfahren. Die neue Reverse-Proxy-Seite ist die zentrale Schaltstelle des airlock und verwaltet die Regeln für das Mapping. Sie verbindet die Übersichten der virtuellen Hosts, Mappings und Backend Hosts. Die grafische Darstellung dieser Verbindungen erleichtert die Navigation sehr und bietet einen schnellen Überblick über den Datenaustausch. Dabei ist es möglich, Verbindungen interaktiv zu editieren. Das Hinzufügen oder Entfernen bestehender Verbindungen lässt sich mit einem einzigen Mausklick realisieren. Der Reverse-Proxy verbindet über Regeln den virtuellen Host – die eingehende Verbindung – durch ein Mapping mit dem Back-End-Host – dem Applikationsserver. Sind der virtuelle und der Back-End-Host eingerichtet, muss das Mapping konfiguriert werden. Hierzu steht eine Grundauswahl an fertigen Templates zur Verfügung.

Hilfreiche Mapping-Vorlagen

Neben einem authentifizierten Service liefert phion auch ein Template für Outlook Web Access (OWA) und Active Sync auf Exchange 2007 mit. Wer im Unternehmen noch mit Exchange 2003 arbeitet, muss sich sein Mapping mühevoller einrichten. Zwar stellt der Hersteller hierzu online einige Anleitungen zur Verfügung, doch ein Template kann dem Administrator viel Mühe ersparen. Im Test haben wir unter anderem auch mit den Templates OWA auf einem Exchange Server 2007 eingerichtet. Mit wenigen Mausklicks waren alle Basics und Filter konfiguriert. Im mehrwöchigen Test hatte sich keine Notwendigkeit ergeben, die Einstellungen zu verändern – hier hat phion gute Vorarbeit geleistet.

Als etwas schwieriger erwies sich die Konfiguration des Mappings auf eine Web-Applikation für das Intranet. Ohne die Unterstützung des Herstellers hätten wir diese Anwendung über die WAF nicht mehr erreicht. Das zeigt, dass trotz der übersichtlichen und einfachen Konfiguration die Tücke im Detail liegt und lässt verstehen, warum der Hersteller airlock nur über autorisierte Partner [1] vertreibt. Die von uns eingesetzte Applikation hat die Eigenschaft, dass der Login und das Session-Handling teilweise über den Client – also dem Rechner des Benutzers – generiert werden. Ohne manuelle Anpassung der Regeln hat airlock die aus der Sicht der WAF modifizierten

Gefährliche Lücken im IT-Sicherheitskonzept

Viele Administratoren sind der Meinung, dass eine Firewall zum Schutz einer Web-Applikation ausreicht. Doch das ist ein Trugschluss. Netzwerk-Firewalls prüfen lediglich den Datenverkehr zum Web-Server, eventuell noch die Signaturen und Protokolle der Nutzeranfragen. Im besten Fall erkennt die Firewall einfache Angriffe mittels vordefinierter Signaturen. Doch das ist Vergangenheit. Um heute getarnte Hackerangriffe zu identifizieren, müsste die Firewall auch auf den verschlüsselten Datenverkehr zugreifen können, was meist nicht der Fall ist.

Eine Lösung für den wirksamen Schutz, der über die reine Filterung von URL-Signaturen hinausgeht, sind applikatorische Themen wie zum Beispiel die vorgelagerte Authentisierung, die Cookie-Protection und der Schutz von URLs und HTML-Formularen. Ein beliebter Weg, Web-Applikationen zu hacken, ist der über manipulierte URLs – dies muss verhindert werden. Und auch vor noch unbekannten Angriffsmöglichkeiten benötigt die Applikation einen proaktiven Schutz. Eine Web-Applikation zu schützen, ist also vielschichtiger als das, was eine reguläre Firewall leisten kann.

Auch die Verschlüsselung via SSL/TLS bietet vor Angriffen keinen Schutz. Das SSL-Protokoll stellt zwar den sicheren Datenverkehr zwischen dem Web-Browser und dem Server her, trägt aber nicht zur Absicherung des Servers selbst bei. Hacker machen sich dies zu eigen und so gelangen die Angriffe über diesen Weg auch "sicher" und verschlüsselt bis zum Applikationsserver. Um Angriffe zu erkennen, müssen also auch SSL-verschlüsselte Verbindungen an den Unternehmensgrenzen enden. Als Prüfinstanz zwischen dem Client und der Applikation stoppt phion airlock den eingehenden Datenverkehr, prüft und filtert ihn und leitet ihn erst dann an das Ziel weiter, wenn keine Manipulation erkannt wurde. So erreichen nur autorisierte und geprüfte Anfragen den Applikationsserver.

Rückmeldungen verworfen – ein Login war nicht mehr möglich. Nach der Analyse der Kommunikation und der Anpassung des Cookie-Handlings mit regulären Ausdrücken gelang uns die Anmeldung wieder.

Im Test haben wir dann noch sowohl für OWA als auch beim Zugang zum Intranet die Anfragen manipuliert. Jede der geänderten Anfragen – auch, wenn es nur eine Zahl war – wurde durch airlock erkannt und der Zugriff zu den Applikationen verweigert.

Schutz für Cookies

Sehr viele Applikationen arbeiten mit Cookies, die sie auf dem Client speichern. Auch wenn die Art und Weise, wie der Inhalt von Cookies gespeichert wird, von der Applikation abhängt, lassen sich die Informationen einfach manipulieren. Um dem Einhalt zu gebieten, behandelt airlock Cookies je nach Notwendigkeit auf drei verschiedene Arten:

- Werden Cookies durch den Browser auf dem Client verändert, ist Pass-trough die Methode der Wahl. Durch diese werden Cookies so durchgeschleust, als wäre keine WAF im Einsatz.
- Werden Cookies nur durch die Applikation bearbeitet, ist die Funktion "Encrypt" beziehungsweise "Sign" hilfreich. Passiert ein Cookie auf dem Weg zum Client die WAF, wird dieser abgefangen, verschlüsselt und so an den Client weitergereicht. Greift die Applikation über den Browser auf den Cookie zu, werden die Daten zurückgeschickt, durch die WAF gefiltert, entschlüsselt und sicher vor Veränderungen an die Applikation geschickt.
- Falls im Rahmen der Anwendung möglich, bietet die Funktion "Cookie-Store" die sicherste Weise vor der Cookie-Manipulation. Ist diese eingeschaltet, werden die Cookies nicht an den Client geschickt, sondern in der User-Session auf der WAF gespeichert. Dies funktioniert jedoch nur, wenn der Client den Cookie nicht benötigt. Fragt die Applikation den Cookie auf dem Client ab, so wird diese Anfrage in der WAF gestoppt und die WAF liefert den Cookie aus dem internen Speicher zurück. Der Back-end-Host merkt von all diesem Vorgehen nichts.

Bild 2: Über Templates lassen sich immer wiederkehrende Grundeinstellungen und Mappings leicht einrichten

URL-Verschlüsselung

Ein weiterer Manipulationsweg für Hacker besteht darin, Parameter in der URL zu verändern, um sich so nicht autorisierten Zugriff zu verschaffen. Dies lässt sich zwar bedingt Programm-seitig eingrenzen, doch nie ganz ausschließen, da über *POST* und *GET* behandelte Parameter immer im Klartext übermittelt werden oder auch Verzeichnispfade in der Adresszeile auszulesen sind. Je nachdem, wie die URL aufgebaut ist, können versierte Angreifer auch schnell ermitteln, welche Applikationen im Back-End eingesetzt werden. Ein Weg, diese ungeschützte Außendarstellung zu verhindern, ist es, die URL auf dem Client umzuschreiben – sprich: zu verschlüsseln. Mit der "URL Encryption" bietet airlock genau diese Funktion an. Dabei fängt die WAF die von der Applikation an den Client geschickte URL ab, verschlüsselt sie und sendet die geänderte URL weiter. Auf dem Client ist damit nur die verschlüsselte URL ohne auswertbare und damit manipulierbare Bestandteile sichtbar. So ist weder ein Rückschluss auf die eingesetzte Technologie und Applikation noch auf die verwendeten Parameter möglich. Auf dem Rückweg entschlüsselt airlock die Angaben und sendet sie im Klartext an die Applikation. Dadurch erhält das Unternehmen 100-prozentigen Schutz vor URL-Manipulationen.

Die Firewall bleibt

phion airlock ist trotz ihrer umfangreichen Schutzmechanismen kein Ersatz für eine Stateful-Packet-Inspection-Firewall. Die WAF überwacht und filtert den Datenverkehr an eine oder mehrere IP-Adressen auf den Ports 80 und 443. Alle anderen Ports – wie zum Beispiel für eine RPC- oder Datenbank-Verbindung – sollten weiterhin über eine eigenständige Firewall geprüft werden. Daher ist es ratsam, ein zweistufiges Firewall-Konzept zu etablieren und airlock zwischen beiden Firewalls einzubinden. Die Firwall vor airlock ist zum Beispiel wegen möglicher SynFlood-Attacken auf die WAF notwendig. Solche Attacken auf Netzebene fängt airlock nicht ab. Die zweite Firewall hinter airlock wird so konfiguriert, dass sie den Datenverkehr an den Application-Server über die Ports 80 und 443 nur von der IP-Adresse der WAF zulässt.

Smart Form Protection

Vor allem für Webshops und andere E-Commerce-Applikationen bietet die "Smart Form Protection" einen Schutz vor Manipulationen von Formulareingaben. Es ist ein Leichtes, zum Beispiel in Drop-Down-Listen vorgegebene Werte im Browser zu verändern und diese zurückzuschicken. Damit diese Änderungen nicht den Server erreichen, stellt die Smart Form Protection sicher, dass die HTML-Vorgaben für Formularfelder (Größe, Art, vorgegebene Werte) nicht verändert werden können. Dazu speichert die WAF die von der Applikation vorgegebenen Angaben in einem Hidden-Field verschlüsselt ab und fügt sie dem HTML-Code hinzu. Bei der Rückmeldung des Formulars prüft airlock anhand der Werte im Hidden-Field, ob die Formulareingaben valide sind, entfernt das Hidden-Field und schleust die Angaben nach erfolgreicher Kontrolle durch.

Bild 3: Die verschlüsselte URL gibt keinen Aufschluss mehr auf Pfade und Parameter – Manipulation ausgeschlossen

HTML-Sicherheit dank ADAPS

Viele Webserver lassen sich manipulieren, indem über Textfelder von Formularen Programmcode an den Server geschickt wird, der ungewollte Aktionen ausführt. Das ist nur möglich, weil HTML vorab keine Möglichkeit der Validierung von Eingaben in Textfeldern bietet. Diese erfolgt immer erst serverseitig – und dann kann es schon zu spät sein. Mit ADAPS behebt airlock diese Schwachstelle und erlaubt es, dynamisch und on the fly die Eingaben in Formularen auf Validität zu prüfen. Dazu stellt die WAF zusätzliche HTML-Tags zur Verfügung, die aktiv im Quellcode für Formularfelder in der Applikation eingebunden werden. Diese führen dazu, dass die Firewall anhand von regulären Ausdrücken die Gültigkeit der Inhalte von Texteingabefeldern prüfen kann.

Damit Hacker auf dem Client nicht erkennen, welche regulären Ausdrücke hinterlegt sind, filtert die WAF die zusätzlichen Tags aus dem HTML-Code heraus und speichert diese ebenfalls verschlüsselt in einem Hidden-Field. Kommt das Formular ausgefüllt zurück, werden – wie auch bei allen anderen Filtern – die Angaben entschlüsselt, geprüft und der entsprechend korrigierte HTML-Code wieder an die Applikation geschickt. Sollten nicht erlaubte Eingaben oder Zeichen an den Server übertragen werden, blockiert die WAF diese Daten und schützt so das System.

Fazit

Ohne eine WAF sollte eine Applikation mit sensiblen Daten nicht mehr aus dem Internet erreichbar sein. airlock 4.2 zeigt, dass sich umfangreiche Schutzmechanismen effektiv umsetzen lassen. Doch die Vielfältigkeit der Konfigurationen macht es notwendig, die erste Einrichtung in jedem Fall einem erfahrenen Fachmann zu überlassen. Ideal ist es, wenn die Einbindung der WAF zusammen mit dem Hersteller oder Programmierer der Applikation erfolgt. Ansonsten kommt der Administrator um die aufwändige und zeitraubende Analyse des Datenverkehrs nicht herum. Ist die WAF einmal eingerichtet, können Feinheiten auch nachträglich und ohne große Auswirkung auf den Live-Betrieb angepasst und getestet werden.

Insgesamt konnte phion airlock 4.2 durch die gut integrierten und intelligenten Funktionen überzeugen. Gekauft werden kann airlock wegen der notwendigen Anpassungen übrigens nicht aus dem Regal. Es ist vielmehr wichtig, einen fachkundigen Partner bei der Einrichtung und Konfiguration – vor allem in der Kommunikation zwischen airlock und der Web-Applikation – zur Seite zu haben. *(dr)*

Produkt
Software-basierte Web-Application-Firewall.

Hersteller
phion AG
www.phion.de

Preis
phion airlock 4.2 ist ab 13.000 Euro erhältlich (erste produktive Instanz). Eine zweite Lizenz im Cluster für Failover kostet 40 Prozent, ein weiteres Testsystem ist für 10 Prozent des Preises zu haben.

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

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

Installation und Konfiguration	8
Filter-Funktionen	10
Schutz der Applikation	10
Einbindung in die IT-Infrastruktur	9
Hardware-Flexibilität	6

Dieses Produkt eignet sich

gut für Unternehmen, die Web-Anwendungen im Internet bereitstellen und diese sowie die dahinter liegenden Daten vor Angriffen auf Applikationsebene schützen möchten.

bedingt für Unternehmen, die auf spezielle Applikationen setzen, bei denen sich der Datenverkehr nur schwer analysieren und nachvollziehen lässt.

nicht als Ersatz für übliche Stateful-Packet-Inspection-Firewalls sowie für Unternehmen, die nur statische Webseiten betreiben.

phion airlock 4.2

Links

[1] phion airlock-Partner
www.phion.com/INT/channelpartner/airlock

Im Test: Trilead VM Explorer

Virtuelle Maschinen günstig verwalten

von Jürgen Heyer

Als erfreulich funktionell und gleichzeitig preisgünstig präsentiert sich der "VM Explorer" von Trilead. Das Tool spielt seine Stärken besonders dann aus, wenn kleinere Unternehmen auf Basis von VMware ESX oder vSphere virtualisieren möchten und ein Werkzeug für Management sowie Backup benötigen, aber den Aufwand und die Kosten einer Virtual Infrastructure scheuen. Im Test überzeugte der VM Explorer mit seiner Vielseitigkeit, auch wenn Kinderkrankheiten noch für die eine oder andere Hürde sorgten.

Der VM Explorer von Trilead lässt sich prinzipiell in jeglichen Virtualisierungsumgebungen auf Basis VMware ESX 3.x und vSphere 4 als Management- und Backup-Tool einsetzen, seine Stärke kommt aber vor allem in kleineren Landschaften ohne Virtual Infrastructure sowie in Kombination mit den kostenlosen ESXi-Varianten zur Geltung. Hier ergänzt er genau die Funktionen, die ein Administrator noch vermissen dürfte. So erlaubt der VM Explorer im Gegensatz zum vSphere-Client ohne vCenter-Einsatz den gleichzeitigen Zugriff auf mehrere ESX(i)-Hosts, ermöglicht ein Cloning, stellt eine SSH-Shell für den direkten Hostzugriff zur Verfügung und steuert Backup sowie Restore.

Kostenloser Einstieg

Der VM Explorer kann auf der Webseite von Trilead einfach heruntergeladen werden und überzeugt bereits in einer etwas eingeschränkten Freeware-Variante durch eine beeindruckende Funktionalität. Mit dem kostenpflichtigen Erwerb eines Freischaltschlüssels können dann alle Funktionen genutzt werden, wobei sich mit einer 490 Euro teuren Lizenz beliebig viele ESX-Hosts von einer Konsole aus administrieren lassen. Letzten Endes bestimmt allein die Anzahl der Konsolen den Preis, denn hier wird für jede eine eigene Lizenz benötigt.

Die Installation aus der 3,3 MByte großen Setupdatei bereitete in unserem Test keinerlei Probleme, wobei als Konsole grundsätzlich ein System unter Windows XP, Vista, 7 oder 2003/2008-Server benötigt wird. Bei den VM-Hosts werden alle Varianten ab VMware ESX 3.02 inklusive der kostenlosen i-Versionen unterstützt. Um nun den Zugang zu einem oder mehreren Hosts zu erhalten, werden diese mit IP-Adresse oder DNS-Namen erfasst und das Root-Passwort angegeben. Der VM Explorer testet dann den Zugang und listet in der Konsole

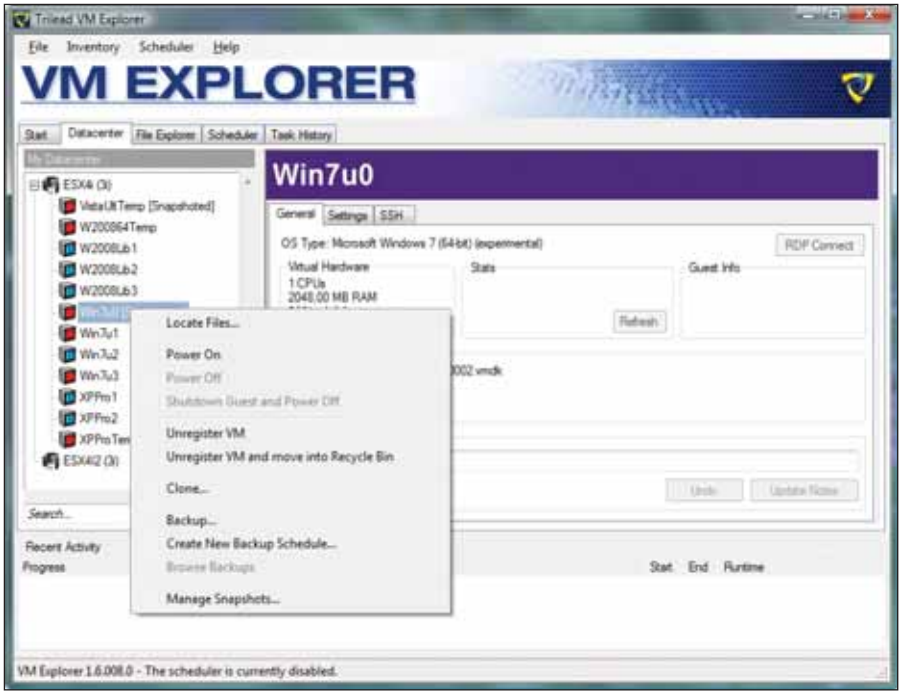


Bild 1: Der VM Explorer bietet ähnliche Optionen wie der vSphere-Client zum Steuern der virtuellen Maschinen

die installierten virtuellen Maschinen untereinander auf. Vorteilhaft ist, dass er gleichzeitig die Verbindung zu mehreren Hosts hält und so als zentrales Werkzeug genutzt werden kann.

Standardmäßig konfiguriert erfolgt der Zugriff des VM Explorers auf einen Host über die normale ESX-API und ist unter anderem bei der Anmeldung vergleichsweise langsam. Vorteilhaft ist deshalb, dass beim Aufruf der Konsole keine automatische Anmeldung an allen Hosts erfolgt, sondern nur sukzessive, so wie der Administrator den Zugriff anfordert. Ganz neu ist eine alternative Zugriffsmöglichkeit über einen VMX-Agenten, der bis auf wenige Ausnahmen wie beispielsweise das Klonen alle Funktionen unterstützt. Um den VMX-Agenten zu nutzen, ist es beim ESXi-Server erforderlich, den SSH-Zugang über den etwas versteckten "Tech Support Mode" zu aktivieren. Dies muss der Administrator für jeden Host getrennt durchführen, die dazu erforderlichen Schritte sind innerhalb des VM Explorers genau beschrieben und mit Linux-Grundkenntnissen zur Bedienung des vi-Editors mit wenigen Arbeitsschritten problemlos zu bewältigen. Anschließend sind innerhalb der VM-Konsole für jeden Host getrennt einige Einstellungen zu ändern. Dabei müssen beim Einsatz von Firewalls die TCP-Ports 62000-65000 freigeschaltet sein. Tatsächlich geschieht die Anmeldung in diesem Modus merklich zügiger und auch alle Kopieroperationen erfolgen deutlich schneller, was unsere Messungen im Test klar belegen – dazu später mehr.

Vom Hersteller erfuhren wir, dass der Nachfolger der getesteten Version eine Unterstützung von vCenter und DRS mitbringen wird. Kurz vor Testende konnten wir noch einen Blick auf die Beta-Version werfen. Darin existiert ein neues Objekt namens "vCenter" zur Anmeldung, um direkt den vCenter-Server zu adressieren. Das erspart das Eintragen der einzelnen Hosts.

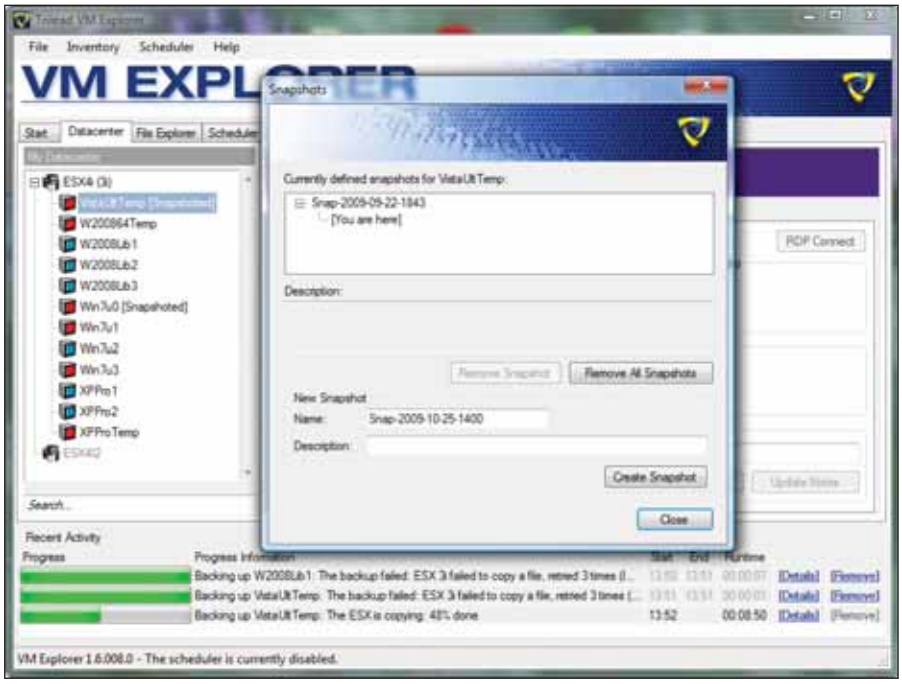


Bild 2: Die Snapshot-Funktion schlägt automatisch einen Namen vor, der Datum und Uhrzeit des Schnappschusses enthält

Bequeme VM-Verwaltung

Sind die Grundeinstellungen des VM Explorers erledigt und die gewünschten Hostzugriffe eingetragen, ermöglicht die so genannte Datacenter-Ansicht eine komfortable Verwaltung der virtuellen Maschinen, die von hier aus über das Kontextmenü gestartet und gestoppt werden können. Weiterhin erfolgt auf diesem Weg der Einstieg zum Klonen, zum Backup und zur Snapshot-Verwaltung. Auch konnten wir von hier direkt in das Filesystem eines ESX-Hosts springen, um uns alle zu einer VM gehörenden Dateien anzeigen zu lassen. Der Betriebsstatus einer VM wird über ein Symbol signalisiert – markiert der Administrator eine VM, werden in einem weiteren Konsolenfenster deren Eckdaten (Betriebssystem, Arbeitsspeicher, CPU, Platten und Netzwerkkarten) sowie der Speicherort der Platten im Dateisystem des ESX-Hosts angezeigt. Bei einer laufenden VM gibt die Konsole auch Auskunft über die Speicher- und CPU-Nutzung sowie den vollen DNS-Namen und die IP-Adresse. Der VM Explorer ist allerdings nicht dazu gedacht, Änderungen an einer VM durchzuführen oder gar eine neue VM zu erzeugen, hierzu sind die VMware-eigenen Tools erforderlich. Gut ist aber, dass aus dem VM Explorer heraus direkt eine RDP- sowie eine SSH-Sitzung zu einer laufenden VM aufgebaut werden kann. Im Gegensatz zum vSphere-Client ist es aber nicht möglich, eine integrierte Konsolenansicht zu einer VM zu öffnen.

Markiert der Administrator in der Datacenter-Ansicht statt einer VM einen ESX-Host, zeigt der VM Explorer die Speicherbereiche (Datastores) und deren Füllgrad sowie die geplanten Backup-Aufträge an. Im unteren Bereich der Konsole wird übrigens der Arbeitsfortschritt für alle anstehenden Aufträge ähnlich wie im vSphere-

Client für VM Explorer
Windows XP, Vista, 2003/2008-Server in 32 oder 64 Bit

Host-Unterstützung
VMware ESX ab 3.0.x und ESXi, Redhat Enterprise 5.x, FreeBSD ab 6.x, Feodora Core 3-9, CentOS 5.x, Ubuntu Server 6 und 8, Debian 4

Kompatible Hypervisoren
Ab ESX 3.0.2 sowie ESXi

Systemvoraussetzungen

1&1 Dynamic Cloud Server

FLEXIBLER

Nach Bedarf konfigurieren. Einfach online –

1&1 DYNAMIC CLOUD SERVER

Hochleistungsserver mit eigener dedizierter Serverumgebung und vollem Root-Zugriff. CPU-Anzahl, Festplattenspeicher und Arbeitsspeicher können jederzeit nach Bedarf konfiguriert werden – der Preis passt sich automatisch an.

Konfigurieren Sie Ihren Server individuell. Starten Sie mit dem 1&1 Dynamic Cloud Server Basis-Paket:

- **1 AMD Opteron™ 2352 Core (bis auf 4 Cores erweiterbar)**
- **1 GB RAM (bis auf 15 GB RAM erweiterbar)**
- **100 GB Webspace (bis auf 800 GB Webspace erweiterbar)**
- **Linux (Windows optional)**
- **Unlimited Traffic**
- **Voller Root-Zugriff**
- **Parallels Plesk Panel 9**
- **24/7 Hotline und Support**

Große Einführungs-Aktion:

3 Monate gratis!*

Basis-Paket

~~39,99 €/Monat*~~

3 Monate für 0,– €/Monat, danach 39,99 €/Monat.*

0,– €/Monat*

AKTION NUR NOCH BIS 28.02.2010!

*Große Einführungs-Aktion: Das 1&1 Dynamic Cloud Server Basis-Paket gibt es 3 Monate für 0,– €, danach 39,99 €/Monat. Einmalige Einrichtungsgebühr 39,– €. 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.

1&1 Innovation!

SERVER

jederzeit.

Als einer der ersten Server-Hoster weltweit präsentiert 1&1 seinen neuen Dynamic Cloud Server – die individuelle Server-Lösung, mit der Sie Leistung und Performance jederzeit ganz flexibel an Ihre aktuellen Bedürfnisse anpassen können.

Weitere attraktive Server-Angebote im Internet!

1&1

www.1und1.info

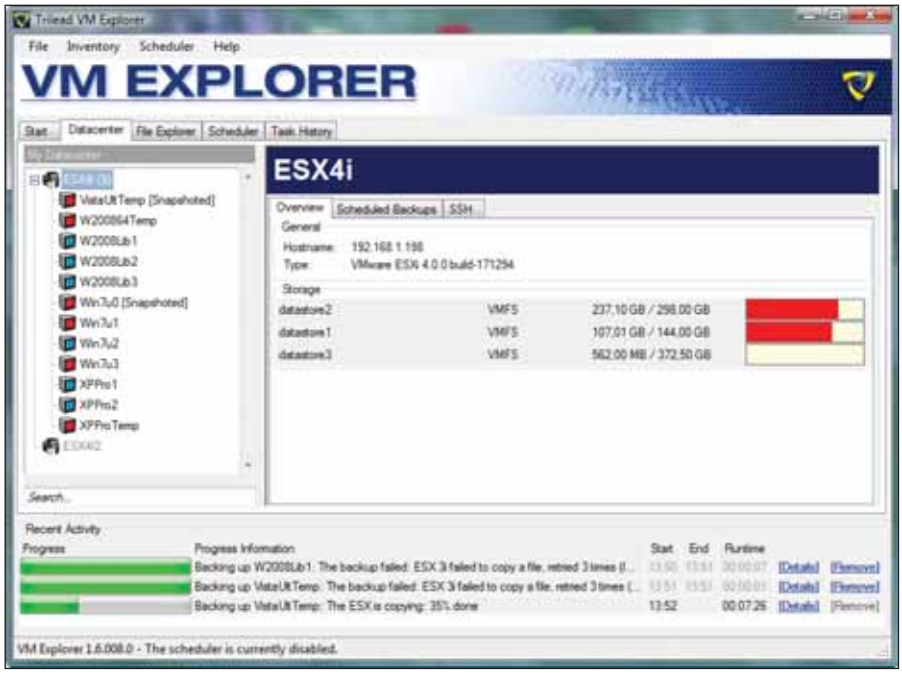


Bild 3: Der VM Explorer zeigt die Belegung der Datastores des ausgewählten Hosts übersichtlich an

Client eingeblendet. Das Tool ermöglicht zudem das Erstellen von Snapshots und arbeitet dabei auf der einen Seite noch etwas komfortabler als der vSphere-Client, denn er schlägt gleich einen Standardnamen für den Snapshot vor, der das Erstellungsdatum samt Uhrzeit enthält. Auf der anderen Seite ist es nicht möglich, den Arbeitsspeicher des Systems mit in den Snapshot zu nehmen oder das Gastbetriebssystem über die VMware-Tools vorher stillzulegen. Es ist auch nicht vorgesehen, über den VM Explorer eine virtuelle Maschine auf einen erstellten Snapshot zurückzusetzen, hierzu muss der Bediener auf den VMware vSphere-Client zurückgreifen, was das Ganze wieder etwas unhandlich macht. In der Regel werden häufig Snapshots erzeugt, aber nur selten wieder genutzt. Das Auflösen einzelner oder aller Snapshots ist aus dem VM Explorer heraus möglich.

Abgesehen von den beschriebenen funktionalen Unterschieden ist der Snapshot-Manager des VM Explorers ähnlich aufgebaut wie beim vSphere-Client, so dass praktisch keine Umgewöhnung erforderlich ist. Laut Trilead gab es anfangs Gedanken, mit dem VM Explorer den vSphere-Client ersetzen zu wollen. Dies wurde aber mittlerweile verworfen, da sich sowieso nicht alles über die API realisieren lässt. Insofern ist der VM Explorer in Kombination mit dem vSphere-Client als Ergänzung gedacht.

Cloning für ESX3i/4i

Ein sehr wertvolles Add-On ist die Möglichkeit, mit dem VM Explorer virtuelle Maschinen auch auf ESX3i- und ESX-4i-Hosts zu klonen, ohne weitere VMware-Lizenzen beschaffen zu müssen. Im Test funktionierte dies mit der zu diesem Zeitpunkt vorliegenden Version 1.6.008.0 allerdings noch nicht im schnellen Zugriffsmodus. Wenig elegant fanden wir es auch, dass das Kloning in diesem Modus trotzdem angeboten wurde, also die Funktion nicht ausgegraut war, und dass das Programm sogar den Prozess startete und laut Arbeitsfortschritt eine temporäre VMX-Datei anlegte, hier aber nie fertig wurde. Es war dann nicht möglich, den Cloning-Job über den vorhandenen Abort-Button abzubrechen, sondern die gesamte Konsole musste geschlossen werden. Hier wäre es sinnvoll, wenn der Hersteller (noch) nicht unterstützte Funktionen ausgrauen oder zumindest mit einem Hinweis abfangen würde. Im Test haben wir uns übrigens damit beholfen, dass wir den VM Explorer auf zwei Systemen einmal mit Standard- und einmal mit schnellem Zugriff installierten, um sowohl den schnelleren Zugriff als auch die volle Funktionalität nutzen zu können. Dies würde jedoch laut der Lizenzbedingungen von Trilead korrekterweise den Kauf zweier Lizenzen erfordern.

Bild 4: Beim Klonen zeigt der VM Explorer den Arbeitsfortschritt sowie den aktuellen Datendurchsatz an

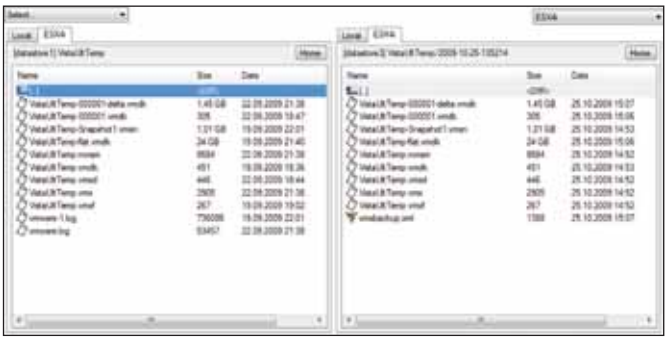


Bild 5: Neben den gesicherten Dateien legt der VM Explorer die Datei *vmxbackup.xml* an, über welche die Wiederherstellung gestartet wird

Für das Erstellen eines Klons legt der VM Explorer einen Snapshot an, den er dann kopiert. Interessanterweise gibt es hier die Möglichkeit, auch den Arbeitsspeicher mit zu klonen und die Maschine auf Wunsch vorher stillzulegen – zwei Features, die wir bei der reinen Snapshot-Funktion vermissen. Für unseren Test erzeugten wir einige Klone und analysierten diese, wobei uns doch gewisse Unterschiede gegenüber der Vorgehensweise von VMware auffielen. So dauert das Klonen relativ lange, was daher rührt, dass sich der VM Explorer offensichtlich nicht des VMware-eigenen Werkzeugs "vmkfstools" bedient. Vielmehr realisiert er das Klonen als reinen Kopiervorgang, wobei die gesamte Datenmenge über das System, auf dem der VM Explorer läuft, transferiert wird. Zwar komprimiert das Tool dabei – für das Klonen einer 34 GByte großen VM wurden im Test aber dennoch rund 8 GByte übertragen, was etwa 23 Minuten dauerte. Mit Hilfe eines zum Vergleich installierten vCenter-Servers dauerte das Klonen der gleichen Maschine mit den VMware-eigenen Mitteln nur gut 16 Minuten, wobei das Netz praktisch nicht belastet wurde, da nur innerhalb des ESX-Servers kopiert wurde.

Auch bei der Detailanalyse der beiden Klone zeigten sich einige Unterschiede. So benennt der VM Explorer das Verzeichnis entsprechend dem Namen der Ziel-VM, alle Dateien aber behalten den ursprünglichen Namen, also die Bezeichnung des Klon-Vaters. Bei der mit VMware geklonten Maschine dagegen werden auch alle Dateien des Klons entsprechend umbenannt und der Inhalt der Konfigurationsdateien angepasst. Hier erinnert nichts mehr an den Klon-Vater. Prinzipiell funktioniert zwar die einfachere Vorgehensweise des VM Explorers, es zeigt sich aber, dass der eigentlich von VMware vorgesehene Prozess nicht exakt nachvollzogen wird.

Komfortabler Dateibrowser

Zentraler Bestandteil des VM Explorers ist ein recht komfortabler Dateibrowser, der in Verbindung mit ESX-Servern, aber auch sonstigen Linux- und FreeBSD-Servern eingesetzt werden kann. Für den Zugriff sind für derartige Server genauso wie für die ESX-Hosts die entsprechenden Anmel-

Bild 6: Der komfortable Datei-Browser erlaubt den Zugriff auf alle erfassten ESX-Hosts sowie Linux-/FreeBSD-Server und das lokale System

deparameter einmalig anzugeben. Die Browseransicht besteht aus zwei nebeneinander liegenden Fenstern, wobei der Administrator für jedes auswählen kann, von welchem Server das Filesystem angezeigt werden soll. Darüber hinaus lassen sich auch die lokalen Laufwerke auswählen und anschließend komfortabel per Drag-and-Drop Dateien kopieren. Allerdings ist es nur möglich, eine oder mehrere Dateien zu markieren und zu kopieren, nicht ganze Verzeichnisse. Ärgerlich ist, dass beim Versuch, ganze Verzeichnisse zu kopieren, keinerlei Hinweis erscheint, sondern das System einfach nicht reagiert. Der Durchsatz ist entscheidend abhängig von der Netzwerkbandbreite, da ebenso wie beim Klonen alle Daten über das System mit der VM-Konsole fließen müssen. Gut ist, dass durch die Linux- und FreeBSD-Unterstützung auch preiswerte Storageserver mit einem dieser Betriebssysteme zur Dateiablage genutzt werden können.

Übersichtliche Backup-Aufträge

Im Gegensatz zu den Funktionen Cloning und Snapshot ist das Backup ein zusätzliches Feature des VM Explorers, das VMware weder in den vSphere-Client noch in das vCenter gepackt hat und das daher grundsätzlich eines Zusatzproduktes bedarf. Der Administrator kann, je nach Bedarf, ein einmaliges Backup einer VM veranlassen oder einen integrierten Scheduler konfigurieren. Die Sicherung ist auf einen ESX-Server, aber auch auf einen Linux- oder FreeBSD-Storage Server sowie lokal auf das System mit der VM-Konsole möglich. Standardmäßig erzeugt der VM Explorer auf einem vorgegebenen Zielpfad ein Verzeichnis mit dem Namen der VM und darunter ein Verzeichnis mit Datums- und Zeitangabe, in das er die gesicherten Dateien ablegt. Sollte das Verzeichnis schon existieren, was aufgrund der besagten Datums- und Zeit-Verknüpfung eher unwahrscheinlich ist, gibt es diverse Vorgaben, wie das Tool reagiert. Weiterhin kann der Administrator vorgeben, welche virtuellen Platten gesichert werden sollen und ob der Arbeitsspeicher sowie Snapshots mit ins Backup integriert werden sollen.

Um Platz zu sparen, komprimiert der VM Explorer auf Wunsch die Plattendateien. So dauerte ein Backup einer 34 GByte großen VM mit Komprimierung 22 Minuten und der Platzbedarf schrumpfte auf 4,8 GByte. Ohne Komprimierung dauerte die Sicherung rund 18 Minuten, sie belegte aber wie die Quell-VM 34 GByte. Abgesehen von der Komprimierung bietet der VM Explorer keine Möglichkeit, Platz einzusparen. Er unterstützt weder eine inkrementelle Sicherung noch beherrscht er eine Versionspflege, indem er beispielsweise nur eine bestimmte Anzahl an Sicherungen hält und ältere automatisch löscht. Bezüglich der Performance ist es bei Backup- und Restore-Aufträgen wichtig, den VMX-Agenten zu nutzen, da diese sonst etwa die doppelte Zeit benötigen.

Um regelmäßige Sicherungen zu automatisieren, ist in den VM Explorer ein flexibler Scheduler integriert. Sicherungen können täglich, wöchentlich, monatlich oder auch einmalig zu einer bestimmten Zeit erfolgen. Sehr von Vorteil ist, dass nicht für jede VM ein eigener Auftrag einzurichten ist. Vielmehr kann der Administrator alternativ für zusammenhängende Aufträge einen Job anlegen, durch den alle gewünschten VMs nacheinander gesichert werden. Letztendlich hat er es in der Hand, den Ablauf hinsichtlich Zeitbedarf und Belastung gezielt zu steuern. So werden die einzelnen Punkte eines Jobs nacheinander abgearbeitet, richtet er aber mehrere Aufträge zeitlich parallel oder überlappend ein, so werden diese auch zeitgleich erledigt. Sprengen zu viele Jobs auf einer Konsole das verfügbare Zeitfenster, können diese auch auf mehrere verteilt werden. Dann sind nur entsprechend viele Programmlizenzen zu beschaffen.

Von Vorteil ist zudem, dass sich in einen Job nicht nur Sicherungsaufträge aufnehmen lassen, sondern auch das Versenden eines Reports per SMTP-Mail. So lässt sich der Abschluss einfach mit einer automatischen Benachrichtigung verknüpfen. Im Test klappte die Sicherung mehrerer VMs mit abschließender E-Mail ohne Probleme. Für eine Rücksicherung legt der VM Explorer in jedem Siche-

rungsverzeichnis eine XML-Datei namens *vmxbackup.xml* an, die über den Dateibrowser auszuwählen ist. Über das Kontextmenü der rechten Maustaste kann der Administrator nun einen Restore anstoßen. Hierbei öffnet sich ein Fenster, in dem er den Zielpfad anlegt und anwählen kann, ob die VM auf dem ESX-Host registriert werden soll. Außerdem kann er vorgeben, ob nur bestimmte virtuelle Disks wiederhergestellt werden sollen.

Diverse Wiederherstellungen im Testlabor zeigten wiederum, dass es hier umso wichtiger ist, den VMX-Agenten zu nutzen. Damit erzielten wir ähnlich kurze Restorezeiten wie für das oben genannte Backup. Eine Wiederherstellung ohne VMX-Agent dauerte dagegen mehr als viermal so lange. Störend fiel nur auf, dass die automatische Registrierung am ESX-Host nicht funktionierte, diese musste über den vSphere-Client nachgeholt werden. Zu erwähnen ist auch, dass der VM Explorer und damit auch der Scheduler nicht als Dienst arbeiten. Zwar lässt sich das Programm in die Taskleiste verbannen, es muss für die Ausführung aber immer ein Benutzer angemeldet sein, so dass der Administrator den PC allenfalls sperren kann.

Fazit

Insgesamt erweist sich der VM Explorer vor allem für kleinere VMware-Umgebungen als sehr hilfreich, wobei der Administrator die wenigen Einschränkungen genau kennen sollte, um das Tool in Kombination mit dem VMware-eigenen Bordmittel vSphere-Client optimal zu nutzen. Ein echter Mehrwert ergibt sich durch das Backup und den Restore virtueller Maschinen sowie im ESXi-Umfeld durch die Möglichkeit zum Klonen. Auch die SSH-Konsole sowie die Browser-Funktion für den Zugriff auf das Filesystem eines ESX-Servers sind sehr sinnvolle und hilfreiche Beigaben. Bezüglich des Klonens ist allerdings zu berücksichtigen, dass dieses mit dem VM Explorer deutlich zeitaufwändiger ist und das Netzwerk stärker belastet.

Den insgesamt positiven Eindruck trübten noch einige Kinderkrankheiten, die aber hoffentlich nach und nach verschwinden dürften, da der VM Explorer aktuell ständig weiterentwickelt wird. So stehen in Verbindung mit einem schnelleren Zugriff nicht alle Funktionen wie beispielsweise das Klonen zur Verfügung, wobei auch nicht auf die Einschränkungen hingewiesen wird. Auch sollte der integrierte Scheduler als Dienst arbeiten können, ohne dass am System mit der VM Konsole ein Benutzer angemeldet sein muss.

Wer den VM Explorer einmal länger ausprobieren möchte, dem sei die kostenlose Free Edition empfohlen, darüber hinaus gibt es eine zeitlich begrenzte Trialversion mit vollem Funktionsumfang. *(dr)*

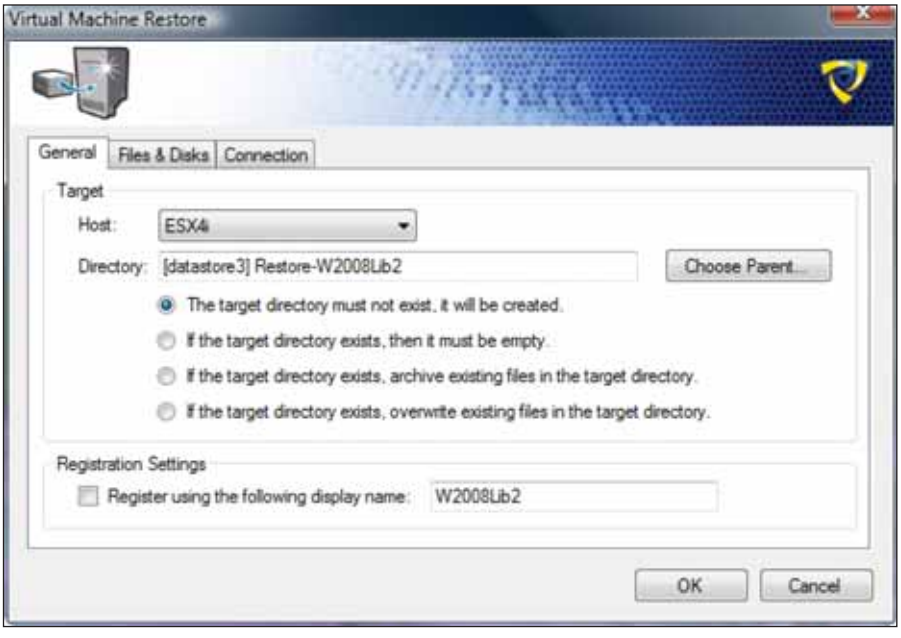


Bild 7: Beim Start einer Wiederherstellung über die Datei *vmxbackup.xml* erscheint ein Fenster mit mehreren Reitern und Optionen, um unter anderem den Zielort der VM festzulegen

Produkt

Backup- und Managementtool für VMware ESX/vSphere-Umgebungen.

Hersteller

Trilead
www.trilead.com

Preis

Die VM Explorer Pro Edition kostet pro Installation mit einem Jahr kostenlose Updates und Wartung 490 Euro, es können beliebig viele ESX-Hosts administriert werden, eine funktional eingeschränkte Free Edition ist kostenlos erhältlich.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

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

Installation und Bedienung	8
Snapshot-Funktion	6
Backup und Restore	8
Klonen	6
Dokumentation	5

Dieses Produkt eignet sich

optimal für kleinere Virtualisierungsumgebungen unter VMware ohne Virtual Infrastructure. Hier bringt der VM Explorer den größten funktionalen Gewinn.

nur bedingt für größere VMware-Umgebungen. Dieses Manko dürfte aber die nächste Version durch eine vCenter-Unterstützung beheben.

nicht für Umgebungen, die nicht auf VMware ESX/vSphere als Hypervisor setzen.

Trilead VM Explorer

Im Test: GFI WebMonitor 2009

Geprüfte Verbindung ins Internet

von Thomas Bär

Der GFI WebMonitor 2009 ermöglicht IT-Verantwortlichen, alle firmeninternen Webseitenaufrufe und Downloads in Echtzeit zu überwachen und darüber hinaus zu steuern. Gemäß verschiedener Studien verwenden bis zu 40 Prozent der Mitarbeiter in Unternehmen ihren Firmenzugang auch für private Zwecke. Im Angesicht der möglichen Gefahren von Trojanern, nicht zulässigen Downloads oder Spionage-Tools ist dies ein in den seltensten Fällen zulässiges Risiko. Dieses Unheil im Zaum zu halten und ein sicheres Surfen im Internet zu ermöglichen, das verspricht die neueste Version des WebMonitors aus dem Hause GFI. IT-Administrator hat im Test untersucht, ob das Werkzeug dieses Versprechen einhält.

GFI bietet die Software in zwei grundsätzlich unterschiedlichen Editionen an: den GFI WebMonitor 2009 for ISA Server und den GFI WebMonitor 2009. Erstere Version arbeitet dabei als dediziertes Plug-In ausschließlich für den Microsoft ISA-Server und bildet im Zusammenspiel mit der Microsoft-Software eine Internet-Überwachung, eine Webseiten-Kategorisierung und Filterung an. Die Variante ohne ISA-Server wird wiederum in drei unterschiedlichen Editionen angeboten: "WebFilter Edition" mit URL-Filterung und Website-Kategorisierung, "WebSecurity Edition" mit Viren- und Phishing-Schutz und Suchfunktionalität für Spyware und die alle Funktionen in sich vereinende "Unified-Protection Edition".

Geht es nur darum, die Bewegungen von Benutzern im Internet zu protokollieren und einen Überblick über das erzeugte Datenvolumen zu bekommen, so ist die kostenfreie Freeware-Variante des "GFI WebMonitors" möglicherweise bereits ausreichend. Alle Versionen bietet der Hersteller gegen Eingabe einiger persönlicher Daten im Internet auch als 30-Tage Testversion an.

Hervorragend dokumentierte Installation

Die Qualität der beiden dem Softwarepaket beigefügten PDF-Dokumente (in englischer Sprache) zur Einrichtung und Konfiguration ist herausragend gut – der Installationsvorgang wird beispielsweise für jede Variation der Einbindung in das Netzwerk separat beschrieben. Entscheidet sich der Administrator für eine ausschließliche Überwachung des HTTP/HTTPS-Transfers, so beschränkt sich der Installationsweg auch auf die benötigten Parameter. Ein Modell, das gern Schule machen darf – insbe-

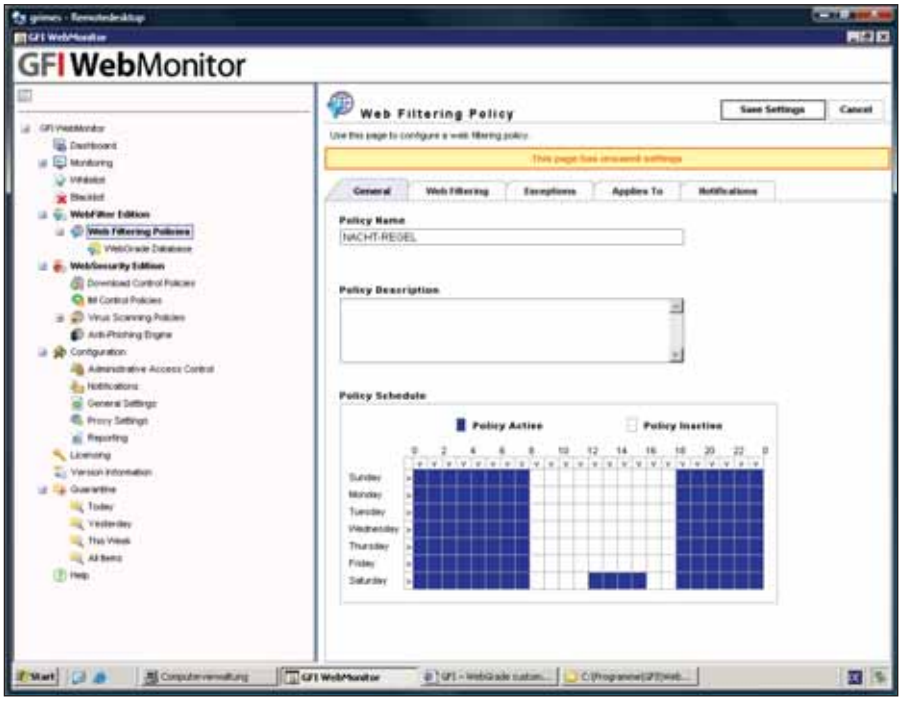


Bild 1: Regelwerke lassen sich auf Basis der verschiedensten Objekte aufsetzen: Zeit, Kategorien, IP-Adresse, Benutzername, Benutzergruppe oder URL. Eine Verschachtelung der Regeln ist auch möglich.

Bild 2: Erst nach verschiedenen Sicherheitsbewertungen von bis zu drei Antivirenprogrammen wird bei Verwendung des GFI WebMonitors 2009 ein Download für den Benutzer tatsächlich freigegeben

sondere Administratoren, die noch keine Erfahrung mit dem Aufsetzen von Proxy-Servern haben, kommen so viel schneller und einfacher zum Ziel.

Der Installations-Assistent unterstützt in ebenfalls sehr hoher Qualität die Einrichtung und zeigt mit einfachen Schaubildern, welche Netzwerkstruktur für welches Szenario am sinnvollsten ist. Einziger Kritikpunkt bei der Einrichtung ist die Konfiguration der E-Mail-Benachrichtigung. Zwar gibt es einen Test-Button für den Versand von E-Mails, jedoch meldet diese Funktion beim Aufruf lediglich, ob die Versandanfrage erfolgreich oder erfolglos war – nicht aber warum. Bei einem Mailserver, der Log-in-Informationen benötigt, beispielsweise ein Microsoft Exchange Server 2007 in der Standardkonfiguration, ist ein Versand so nicht möglich, da das Konfigurationsfenster keine Möglichkeit zur Eingabe von Log-in-Daten bietet. Folgerichtig ist irgendwo im Netzwerk ein ungeschützter SMTP-Server zu betreiben, über den administrative E-Mails versendet werden. Mit diesem Makel ist der GFI WebMonitor 2009 jedoch nicht allein – verschiedenste Programme, die zu Tests eingereicht wurden, bieten keine Eingabemöglichkeit für AuthSMTP oder andere Benutzerkennungen.

Eine kleine Besonderheit findet sich am Ende des Einrichtungsvorgangs. Für eine Auswahl von in den USA gebräuchlichen Internet-Routern ist jeweils eine spezielle Anleitung zur Umsetzung der benötigten Konfiguration im "Simple Proxy Mode" vorhanden. Bei diesem Modus wird das alleinige Internetzugriffsrecht auf den Computer mit der GFI-Installation gelenkt, alle anderen PCs und Server müssen ihren Internet-Netzwerkverkehr über den GFI-Proxy lenken.

In der von uns getesteten Variante ohne Microsoft ISA-Server fungierte der GFI WebMonitor 2009 als einziger Proxy-Server für eine Active Directory-Domäne. Die Installation führten wir auf einem VMware Virtual Server 2.0 unter Microsoft Windows Server 2003 Standard durch. GFI weist stets darauf hin, dass die Produkte die gängigsten Virtualisierungstechnologien wie VMware, Microsoft Virtual Server und Microsoft Hyper-V unterstützen. Die Ressourcen-Zuordnung belief sich auf eine virtuelle CPU, 768 MByte Arbeitsspeicher und einer virtuellen Festplatte mit 40 GByte Kapazität. In dieser Konfiguration ist die Oberfläche für die tägliche Administration ausreichend zügig in der Reaktion.

Clientseitig ist für den Administrator nicht viel zu tun. Entweder werden die benötigten Einstellungen für den Zugriff über den neuen Proxy-Server per Gruppenrichtlinie verteilt oder das so genannte "Web Proxy Autodiscovery" (WPAD) sorgt für eine automatische Verwendung. WPAD wird von vielen Browsern als Standard-Einstellung verwendet, sofern diese keine direkte Verbindung über den Standard-Gateway mit dem Internet aufbauen können.

URL-Katalog als Basis der Filterung

Der GFI WebMonitor besteht aus einer einzigen, sehr übersichtlichen Oberfläche, in deren Baumstruktur alle Einstellungsmöglichkeiten und Auswertungen zu finden sind. Zur Zuordnung von Richtlini-

Bild 3: Durch ein Optionshäkchen in der Konfiguration wird der Zugriff über den GFI WebMonitor 2009-Proxy auf bestimmte Active Directory-Gruppen beschränkt

en arbeitet die Software über drei verschiedene Gruppen: den einzelnen Benutzer oder eine Benutzergruppe aus dem Active Directory oder eine IP-Adresse. Die Verwendung von Computernamen oder IP-Bereichen bietet die Software leider nicht an.

Die Hauptwaffe bei der Steuerung des Internetzugriffs ist eine Kategorie-Datenbank, die so genannte "WebGrade Database". Für sehr viele URLs haben die GFI-Experten Kategorien gebildet, darunter Erotikseiten, Online-Spiele, Freemail-Anbieter, P2P-Tauschplattformen, Flugbörsen oder Social-Networking-Plattformen. Laut Datenblatt des Herstellers verfügt die Kategorisierungs- und Filterdatenbank für den GFI WebMonitor 2009 über die Informationen von über 205 Millionen URLs. Dass eine komplette Katalogisierung des Internets von Haus aus ein nicht umsetzbares Unterfangen darstellt, leuchtet wohl allen Administratoren ein. Warum jedoch selbst sehr typische Webseiten aus dem deutschsprachigen Bereich von GFI nicht erfasst wurden, verwundert ein wenig. Im Zweifelsfall sortiert der GFI WebMonitor 2009 die Seiten in die Rubrik "Unkategorisiert" – für die es aber ein definierbares Regelwerk geben kann. Quasi als Nebeneffekt der URL-Datenbank ist GFI in der Lage, einen laufend aktualisierten Anti-Phishing-Filter anzubieten. Wird eine manipulierte Site erkannt, erfolgt deren umgehende Sperrung samt Warnung an den Anwender.

Black- und Whitelisting mit leichten Hindernissen

Ein "alter Klassiker" bei der Zugriffskontrolle auf das Internet darf auch beim GFI WebMonitor 2009 nicht fehlen: Die Black- und Whitelist. Während in der Whitelist die Seiten geführt werden, auf die das System grundsätzlich einen Zugriff gewährt, so ist die Blacklist das exakte Gegenteil. Unabhängig davon, welche sonstigen Regelwerke der Administrator definiert, verhindert ein Eintrag in der schwarzen Liste jeglichen Zugriff. Soll beispielsweise das Online-Auktionshaus ebay unerreichbar bleiben, so lässt sich dies durch den Eintrag "www.ebay.de" in der Blacklist sehr schnell umsetzen.

Ehe der Eintrag aktiv wird, muss der Administrator die Änderungen durch einen Mausklick auf "Save Settings" bestätigen. Ein gelb-orangenes Kästchen macht auf die ausstehende Speicherung deutlich aufmerksam. Wird das Fenster durch einen Mausklick auf einen anderen Befehl verlassen, ohne die Änderungen gespeichert zu haben, so erfolgt jedoch keine erneute Nachfrage, ob die Änderungen wirklich verworfen werden sollen. Da dieses Verhalten eher ungewöhnlich ist, darf mit einigen Gewöhnungsschwierigkeiten gerechnet werden. Die Hilfestellung, wie ein Eintrag vorzunehmen ist, erscheint erst, sobald der Mauszeiger auf dem Eingabebereich ruht. Insgesamt unpraktisch, da dieser Hilfetext verschwindet, sobald eine Eingabe erfolgt. Zwar erlaubt der GFI WebMonitor die Verwendung von Wildcards (*), jedoch nicht bei den Top-Level-Domain-Names. Das hat den Nachteil, dass eine Sperrung von Webseiten internationaler Unternehmen per Blacklist recht zeitaufwändig ist, sofern diese nicht über die Kategorisierung der Datenbank gelistet sind.

Auch ohne die optional zu installierenden Reports liefert der GFI WebMonitor eine Menge an aktuellen Informationen über die Zusammensetzung des Internetverkehrs. Welcher Benutzer greift auf welche Daten zu, wie viel Volumen bindet diese oder jene Webseite – beispielsweise wird der Microsoft Update Service Dienst als wahrlich kommunikationsfreudig enttarnt, sofern kein WSUS-Dienst im Unternehmen aktiv ist. Mit Blick auf die Usability ist es etwas schade, dass eine Top-Seite aus einer Auswertung nicht per Rechtsklick in eine Black- oder Whitelist übertragen werden kann. Das würde viel Tipparbeit sparen und zudem das Risiko des Vertippens minimieren.

Gewünschte Updates von unerlaubten Downloads trennen

Einige Programme erstellen per HTTP-Tunneling automatisch und ohne Benutzergenehmigung eine Verbindung zur Website des Herstellers, um nach Updates zu suchen. Als Erleichterung für die Produktwartung gedacht, stellt diese Unterstützung jedoch mitunter auch ein Sicherheitsrisiko

dar: Unbekannte Anwendungen und Trojaner können mit der gleichen Methode unbemerkt schädliche Dateien auf PCs übertragen. Der GFI WebMonitor 2009 erlaubt es dem Administrator, mit wenigen Mausklicks festzulegen, dass Updates nur von vertrauenswürdigen Websites bezogen werden dürfen.

Produkt

Software zur Überwachung und Regulierung firmeninterner Website-Aufrufe und Downloads in Echtzeit.

Hersteller

GFI Software
www.gfisoftware.de

Preis

Der WebMonitor 2009 kostet für zehn bis 49 Arbeitsplätze im Jahresabonnement 34,51 Euro in der Unified-Protection Edition pro Platz. Eine Verlängerung kostet in dieser kleinsten Ausprägung 32,78 Euro pro Jahr und Platz. Je nach Anzahl benötigter Plätze sinkt der Preis gemäß der Staffelung auf 16,66 Euro bei Abnahme von mehr als 1.000 Plätzen.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

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

Installation	8
Virenschutz	8
Seiten-Klassifizierung	6
Individuelle Regelwerke	8
Dokumentation	9

Dieses Produkt eignet sich

optimal für Einsatzgebiete, in denen eine exakte Steuerung des Internet-Verkehrs vorgenommen werden soll.

gut für Administratoren, die bisher wenig Kontakt mit dieser Materie hatten, da leichte Installation und Administration einen schnellen Einstieg ermöglichen.

nicht für Unternehmen, die ein System gemäß dem Motto "einschalten und vergessen" suchen.

GFI WebMonitor 2009

In Abhängigkeit von der Black- und Whitelist und der Kategorisierung von Webseiten bietet das Programm die Möglichkeit, über Benutzer-, Gruppen- und IP-spezifische Richtlinien mit einer Download-Kontrolle das Herunterladen einzelner Dateitypen wie JavaScript, MP3, MPEG oder EXE differenziert zu unterbinden. Sicherheitsgefährdende Programme, wie beispielsweise Trojaner-Downloader, versuchen oftmals als harmlose Dateien getarnt in ein System einzudringen. Mit Hilfe des Dateisignatur-Scanners im GFI WebMonitor lässt sich der tatsächliche Dateityp von heruntergeladenen HTTP-/FTP-Dateien ermitteln.

Antivirus durch Kombination verschiedener Engines

Je nach Konfiguration der Software muss jeder Download zunächst von bis zu drei Virenscannern durchleuchtet werden, ehe die Datei für den Client-Computer freigegeben wird. In vielen Unternehmen wird die endgültige Prüfung eines Downloads ausschließlich dem Client-Computer aufgebürdet. Das Vorschalten des Proxy-Download-Scans von GFI steigert die Sicherheit zusätzlich und hebt die alleinige Abhängigkeit vom Client-Scan auf.

Die Verwendung verschiedener Antiviren-Engines verkürzt rechnerisch die durchschnittliche Wartezeit bis zum Erhalt einer aktualisierten Signatur und bietet einen schnelleren Schutz vor neuesten Gefahren. Zudem wendet jede AV-Lösung ihre eigene Heuristik an und besitzt individuelle Erkennungs- und Abwehrmethoden. Einige Scanner erkennen bestimmte Virenarten samt Untergruppen besser als andere, die wiederum ihre eigenen, speziellen Stärken haben. Der GFI WebMonitor wird gemeinsam mit den Programmen Norman Virus Control und BitDefender ausgeliefert. Die Virendefinitionen für Norman Virus Control und BitDefender werden automatisch auf den neuesten Stand gebracht, die Kosten für beide Produkte sind im Preis des GFI WebMonitors inbegriffen.

Sollten diese beiden Programme für den Sicherheitsanspruch im Unternehmen nicht ausreichen, so bietet GFI die optionale Integration der SuperSecure-Datenbank von Kaspersky als optionale und kostenpflichtige Ergänzung an. Die Lösung aus dem russischen Softwarehaus Kaspersky erkennt laut Herstellerangaben weitere schädliche Programme zur unerwünschten Remote-Verwaltung, Tastatur-Logger, Passwort-Späher und Adware-Downloader. Die Updates der Viren- und Malware-Definitionsdateien für Kaspersky übernimmt ebenfalls der GFI WebMonitor.

Fazit

Der WebMonitor 2009 von GFI ist eine insgesamt überzeugende Lösung, um den Internetzugriff im Unternehmen zu steuern und zu reglementieren. Dank der verschiedenen Möglichkeiten wie Black- und Whitelists, den zeitlich und von Anwendergruppen abhängigen Regelwerken mit der WebGrade-Datenbank und der automatischen Integration ins Active Directory ist eine Einbindung in die eigene Umgebung sehr schnell und leicht möglich. Im Vergleich zu verschiedenen kostenlosen Proxy-Servern hat die GFI-Lösung mehr Features im Portfolio, wie beispielsweise die Instant-Messaging-Richtlinie, die eine Überwachung oder Blockade des Windows Live Messengers (MSN) erlaubt.

Mit den Regelwerken ist es immer so eine Sache – wird sehr genau parametriert und einige Stunden an Arbeitszeit investiert, so ist eine sehr genaue Steuerung möglich. Einfach nur Einschalten ist auch beim GFI WebMonitor 2009 nicht wirklich hilfreich, da die WebGrade-Datenbank ihre US-amerikanische Herkunft nicht verschleiern kann. Viele halbwegs bekannte, deutschsprachige Webseiten werden nicht durch die Datenbank erkannt und müssen über die Black- und Whitelist gesteuert werden. Zwar bietet GFI die Möglichkeit, eigene Webseiten zur Kategorisierung vorzuschlagen, doch bis diese Einträge erfolgen, vergehen einige Tage. *(jp)*

Das Netzwerk mit IPCop schützen

Ehrenamtlicher Netzwerk-Sheriff

von Dr. Holger Reibold

IT-Verantwortliche, die ihr Netzwerk vor Attacken schützen möchten, setzen zumeist auf Firewall-Lösungen. Entsprechende Umgebungen und Software gibt es zuhauf. Doch nur wenige sind so einfach zu handhaben und funktional flexibel wie IPCop. In diesem Workshop zeigen wir Ihnen, wie Sie die Linux-basierte Firewall effektiv einsetzen.

Bei IPCop [1] handelt es sich um eine freie Linux-Distribution, deren Hauptaufgabe das Bereitstellen von Firewall- und Router-Funktionen ist. Da in dem Linux-System ohnehin gängige Server enthalten sind, kann die Distribution auch ausgewählte Server-Dienste anbieten. Das Schöne an IPCop: Die Sicherheitslösung lässt sich einfach installieren und konfigurieren. Außerdem bietet sie bereits nach der Erstinstallation ein hohes Maß an Schutz. Nach der Installation stellt IPCop neben einer funktionierenden Firewall einen Proxy-Server (Squid), einen DHCP-Server, einen Caching-Nameserver (dnsmasq) und das Intrusion-Detection-System Snort bereit. Außerdem stellt Ihnen IPCop interessante Zusatzfunktionen wie Traffic-Shaping, VPN und Dynamic DNS zur Verfügung.

Die Inbetriebnahme der Umgebung ist einfach: Laden Sie sich das aktuelle ISO-Image 1.4.20 von der Projekt-Website herunter und folgenden Sie den wenigen Anweisungen. Neuerdings wird IPCop bei SourceForge [2] gehostet. Die Steuerung der Umgebung erfolgt über das Web-Interface, das unter *https://{Hostname_bzw_IP-Adresse}:445* verfügbar ist. Beachten Sie, dass der übliche HTTP-Port nicht länger unterstützt wird. Sollten Sie den HTTPS-Port ändern wollen, weil Windows diesen beispielsweise für Verzeichnisdienste verwendet (SMB über TCP/IP) oder dieser aus Sicherheitsgründen gesperrt ist, so greifen Sie einfach zu dem Kommandozeilentool *setreservedports*. Die Port-Änderung erfolgt mit diesem Kommando:

```
$ /usr/local/bin/setreservedports
  {neuer Port}
```

Sie können jeden Port zwischen 445 und 65535 verwenden.

Administrative Benutzerkonten

IPCop kennt vier verschiedene Benutzerkonten für die Systemadministration: root, admin, backup und dial. Die Benutzer root und backup sind Systemkonten, während die Benutzer admin und dial für die Bedienung der Web-Oberfläche benötigt werden. Diese Konten sollten Sie kennen, weil sie zum einen bei der Installation angelegt werden und zum anderen für die effektive Nutzung der Umgebung wichtig sind. Hinter dem Benutzerkonto root steht der Systemverwalter. Für diesen Account wird das Kennwort während der Installation von IPCop festgelegt, wobei die Mindestlänge des Kennworts sechs Zeichen beträgt. Der Benutzer root kann sich entweder direkt an der Konsole oder, falls der Remote-Zugriff aktiviert ist, aus dem lokalen Netzwerk über SSH (Secure Shell) anmelden. Im Normalfall ist eine Anmeldung als Benutzer root jedoch nicht erforderlich. Beachten Sie Folgendes: Mit diesem Konto verfügen Sie über alle Berechtigungen auf dem System. Vergeben Sie deshalb ein sicheres Kennwort für diesen Benutzer. Sie sollten den SSH-Zugang außerdem nur aktivieren, falls dies auch erforderlich ist.

Mit dem admin-Konto führen Sie die meisten Arbeiten durch. Dessen Kennwort legen Sie ebenfalls während der Installation fest – auch hier beträgt die Mindestlänge sechs Zeichen. Dieser Benutzer hat vollen Zugriff auf die Konfiguration und die Protokolle der IPCop-Umge-

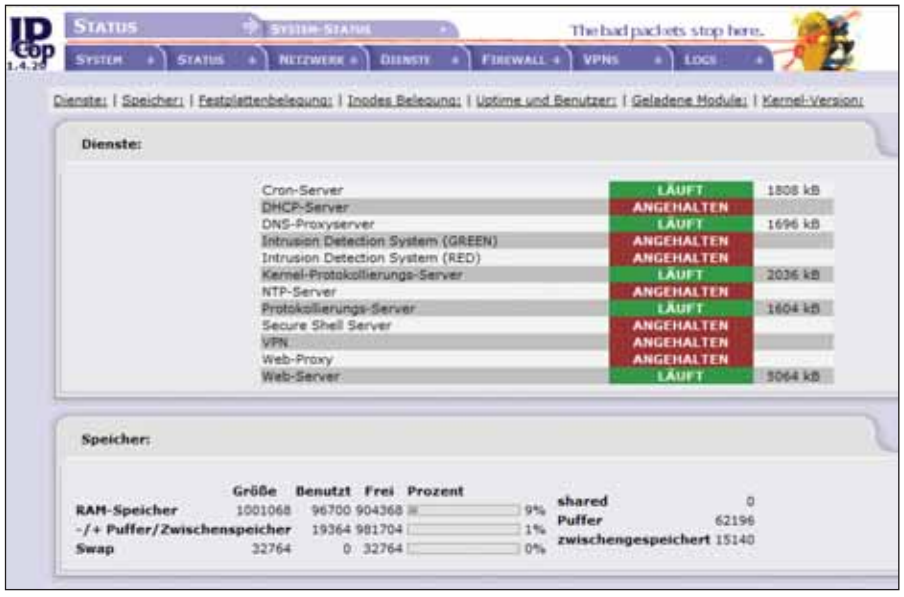


Bild 1: Ein erster Blick auf die webbasierte Administrationszentrale von IPCop mit der Dienste-Übersicht

bung. Die Anmeldung erfolgt beim Zugriff auf die geschützten Bereiche der Web-Oberfläche. Der admin-Benutzer kann sich nur an der Web-Oberfläche anmelden. Eine Anmeldung an der Konsole ist nicht möglich. Das Kennwort für den Benutzer admin können Sie jederzeit nach erfolgter Anmeldung über die Web-Oberfläche ändern. Haben Sie das Kennwort einmal vergessen, melden Sie sich einfach als root an der Konsole an und ändern das Kennwort des Benutzers admin mit dem Programm *setup*.

Beim Benutzer backup handelt es sich nicht um einen Benutzer im herkömmlichen Sinn, denn eine Anmeldung am System ist nicht möglich. Das während der Installation für diesen Benutzer vergebene Kennwort wird nur dann benötigt, wenn der Schlüssel für eine Wiederherstellung von Sicherungsdateien exportiert werden soll. Dieser Schlüssel ist erforderlich, wenn Sie IPCop neu installieren und bei der Installation eine vorhandene Sicherungsdatei zurückschreiben wollen. Abschließend kennt IPCop noch den Benutzer dial. Er ist standardmäßig deaktiviert und wird nur dann benötigt, wenn IPCop über eine manuelle Einwahlverbindung (auch DSL) mit dem Internet verbunden ist.

Einstieg in die IPCop-Konfiguration

Nachdem Sie IPCop in Betrieb genommen haben, gilt es im nächsten Schritt, die Umgebung an Ihre Anforderungen anzupassen. Nach dem ersten Einloggen beschwert sich IPCop über ein fehlerhaftes Profil. Der Grund: Das Tool ist noch nicht für die Einwahl ins Internet konfiguriert. Wenn Sie eine Verbindung ins Internet über DSL herstellen, müssen Sie zuerst ein Einwahlprofil erstellen. Dazu wählen Sie in der Web-Oberfläche unter "Netzwerk" den Punkt "Einwahl". Als Nächstes sollten Sie sich dem System-Menü widmen. Dort bieten sich Ihnen verschiedene Möglichkeiten zur Konfiguration und Administration des Systems. Sie können insbesondere unter "Passwörter" die Kennwörter für admin und dial anpassen. Unter "SSH-Zugriff" erfolgt die Konfiguration des SSH-Zugriffs auf den IPCop. Unter "Einstellungen" der Benutzeroberfläche passen Sie beispielsweise die Spracheinstellungen, Anzeige und Klang an. Daneben konfigurieren Sie über das "Dienste"-Menü die Dienste, die IPCop für sich selber nutzt oder anderen Computern im Netzwerk zur Verfügung stellt. Hier finden Sie die folgenden Einträge:

- Proxy: Web-Proxy zur Beschleunigung des Webzugriffs.
- DHCP-Server: DHCP-Server für die IP-Konfiguration von Clients.
- Dynamischer DNS: Dynamische DNS-Namen für wechselnde IP-Adressen.
- Hosts bearbeiten: Statische Einträge im DNS-Cache.
- Zeitserver: Automatische Aktualisierung von Datum und Uhrzeit.
- Traffic Shaping: Priorisieren von Netzwerkverkehr.
- Einbruchdetektierung: Erkennung von Angriffsversuchen.

In der Regel kommt in einem lokalen Netzwerk ohnehin ein DHCP-Server für die Client-Anbindungen zum Einsatz. Um die Administration Ihrer Infrastruktur zu vereinfachen, bietet es sich an, eine bestehende DHCP-Server-Konfiguration durch den in IPCop integrierten abzulösen. Der DHCP-Server lässt sich für die grüne und die blaue Schnittstelle getrennt konfigurieren. Beachten Sie, dass der Abschnitt für die blaue Schnittstelle nur dann verfügbar ist, wenn auch eine blaue Schnittstelle konfiguriert ist. Da der DHCP-Server standardmäßig nicht aktiviert ist, müssen Sie diesen über "Dienste / DHCP" zunächst aktivieren. Auf dem zugehörigen Formular erfolgt auch die Basiskonfiguration, die beispielsweise den zu vergebenden Adressbereich definiert.

Die Firewall-Konfiguration

Die Hauptaufgabe von IPCop ist das Bereitstellen der Firewall-Funktionen, die Sie über das gleichnamige Menü vornehmen. Hier erzeugen und verwalten Sie insbesondere die Firewall-Regeln Das Menü bietet drei Untermenüs: Das Untermenü "Port-Weiterleitung" dient dem Weiterleiten von Anfragen an interne Adressen, "Externer Zugang" konfiguriert den externen Zugriff von Rot auf IPCop und "DMZ-Schlupflöcher" dient dem Anlegen von Firewall-Regeln zwischen den einzelnen Zonen.

Die Port-Weiterleitung können Sie verwenden, um einen Port von der roten Schnittstelle auf einen beliebigen Port eines internen Computers weiterzuleiten. Damit können Sie Dienste im Internet anbieten, ohne den Server direkt mit dem

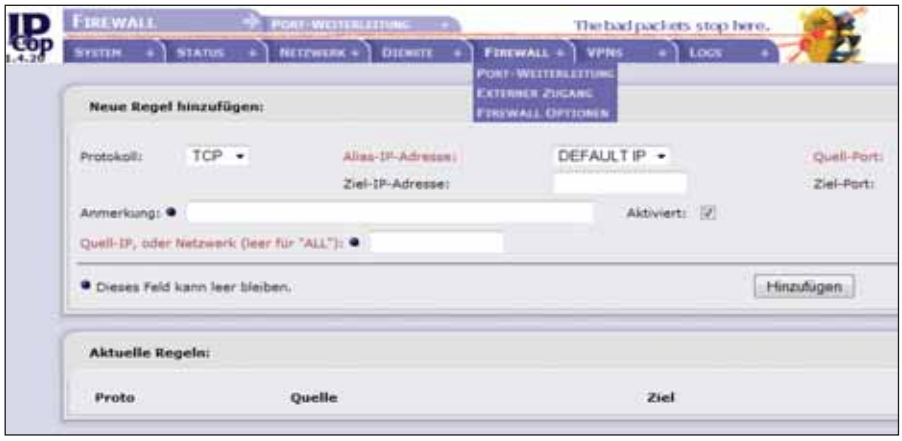


Bild 2: Das Anlegen einer Port-Weiterleitung ist mit wenigen Angaben erledigt

Internet verbinden zu müssen. Durch die Weiterleitung eines einzelnen Ports bleiben alle anderen Ports des Servers auch weiterhin durch die Firewall geschützt. Bei der Port-Weiterleitung sind die folgenden Regeln zu beachten:

- Quell- und Ziel-Port brauchen bei einzelnen Ports nicht identisch sein.
- Wenn Sie einen Ziel-Port-Bereich angeben, muss der Quell-Port-Bereich identisch sein.
- Ein Quell-Port kann nicht gleichzeitig auf verschiedene interne Ziele umgeleitet werden.
- Port-Bereiche dürfen sich nicht überlappen. Ports innerhalb eines Bereiches können nicht noch einmal einzeln weitergeleitet werden.
- Die vom IPCop reservierten Ports 67, 68, 81, 222 und 445 können nicht weitergeleitet werden.
- Erstellen Sie nach Möglichkeit nur Port-Weiterleitungen nach Orange.

Mit der Funktion "Externer Zugang" richten Sie einen Zugang von der roten Schnittstelle direkt zu IPCop ein. Der externe Zugang ist nicht ungefährlich, da Sie damit einen Zugang aus dem Internet auf Ihren IPCop schaffen. Die Port-Weiterleitung ist allerdings unabhängig vom externen Zugang. Sie müssen also Ports, die Sie für die Weiterleitung definiert haben, nicht auch noch zusätzlich als externen Zugang einrichten. Die Port-Weiterleitung geht am IPCop vorbei, der externe Zugang endet auf dem IPCop-System.

Von den Netzen Orange und Blau kann standardmäßig nicht auf das grüne Netz zugegriffen werden, da diese Richtung von der Firewall geblockt wird. In einigen Fällen ist es jedoch erforderlich, für die Kommunikation nach Grün ein kleines Loch in die Firewall zu bohren. Diese kleinen Löcher werden DMZ-Schlupflöcher (DMZ Pinholes) genannt, auch wenn Blau im weiteren Sinne nicht als DMZ zu bezeichnen ist.

Notwendige Systempflege

Ein weiterer sehr wichtiger Aspekt der IPCop-Administration ist die Systemwartung. Die verfügbaren Funktionen finden Sie über das Menü "System". Zur Wartung gehören insbesondere die Funktionen zweier Untermenüs: "Updates" dient der Update-Prüfung und Systemaktualisierung, "Datensicherung" der Sicherung und Wiederherstellung der Konfiguration. Über das Update-Menü können Sie nach Aktualisierungen für den IPCop suchen, diese auf das System hochladen und installieren oder sich eine Liste der bereits installierten Updates anzeigen lassen. IPCop prüft bei jedem Verbindungsaufbau ins Internet automatisch, ob neue Updates verfügbar sind. Stehen neue Updates zum Download bereit, so erscheint auf der Startseite im Fenster mit den Verbindungsinformationen ein entsprechender Hinweis. Die Updates für den IPCop sind nicht kumulativ. Sie müssen jedes Update daher nacheinander in der vorgegebenen Reihenfolge installieren und können nicht einfach nur das neueste Update installieren. Beachten Sie außerdem, dass sich die Update-Installation nicht mehr rückgängig machen lässt.

Um die Konfiguration im Fehlerfall oder bei einer Neuinstallation möglichst schnell wieder herstellen zu können, bietet der IPCop eine eingebaute Datensicherung

Die Sicherheitszonen von IPCop

IPCop nutzt ein spezielles Sicherheitsmodell, das zwischen vier verschiedenen Zonen unterscheidet, die jeweils mit einer eigenen Farbe dargestellt werden: Rot, Grün, Blau und Orange. Jede dieser Zonen stellt einen eigenen Netzwerkbereich mit einer unterschiedlich definierten Sicherheitsstufe dar. Die Zonen Rot und Grün sind grundsätzlich immer vorhanden, die Einrichtung der Zonen Blau und Orange ist optional. Die Sicherheitszonen und Ihre wichtigsten Merkmale im Überblick:

- **Rot – das Internet:** Diese Zone bezeichnet aus der Sicht der Firewall das externe Netz, das grundsätzlich als nicht vertrauenswürdig gilt. Computer in dieser Zone haben grundsätzlich keinen Zugriff auf die anderen Zonen.
- **Grün – das lokale Netzwerk:** Die Farbe Grün steht für das innere Netz, in dem sich Ihre zu schützenden Computer, Server und andere Netzwerksysteme befinden. Diese Zone hat den höchsten Schutzbedarf und ist deshalb für eingehende Zugriffe jeglicher Art standardmäßig gesperrt.
- **Orange – die DMZ:** Mit Orange wird das Perimeternetzwerk, die sogenannte demilitarisierte Zone (DMZ, Demilitarized Zone) gekennzeichnet. In dieser Zone befinden sich Computer, die aus dem Internet heraus erreichbar sein sollen, zum Beispiel eigene Mail- oder Webserver. Durch diese Zwischenzone können Sie eigene Dienste im Internet anbieten, ohne dass diese Server in Ihrem grünen Netzwerkbereich stehen müssen. Damit die Server von außen zu erreichen sind, müssen Sie bestimmte Bereiche für eingehenden Verkehr von Rot öffnen. Um diesem erhöhten Sicherheitsrisiko zu begegnen, werden alle öffentlichen Dienste in der orangenen Zone zusammengefasst. Orange kann von Grün und Blau heraus angesprochen werden, der einzige Weg aus Orange heraus ist über Rot. Diese Sicherheitszone ist optional.
- **Blau – das Drahtlosnetzwerk:** Üblicherweise wird die blaue Zone für Computer verwendet, die per WLAN verbunden sind. Hier sind zusätzliche Sicherheitsmaßnahmen erforderlich, damit nicht jeder beliebige WLAN-fähige Computer auf Ihr Netzwerk zugreifen kann. In der Grundkonfiguration ist Blau völlig isoliert und kann keine andere Zone erreichen. Die Kommunikation von Grün nach Blau ist jedoch standardmäßig möglich. Diese Sicherheitszone ist optional.

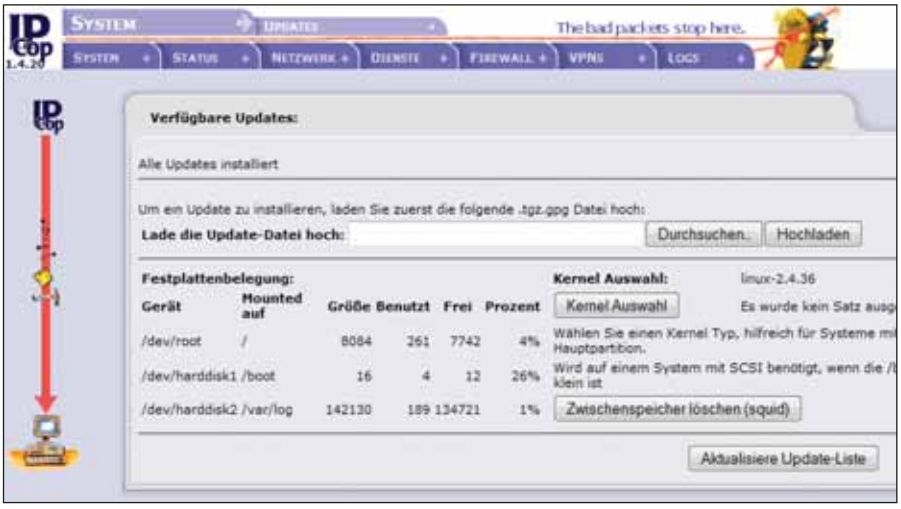


Bild 3: Dank des integrierten Update-Mechanismus ist es einfach, die IPCop-Installation auf dem neuesten Stand zu halten

an. Die Sicherung ist auf Disketten und beliebigen anderen externen Datenträgern möglich. Alle Datensicherungssätze, mit Ausnahme der Diskettensicherung, werden grundsätzlich verschlüsselt. Dazu wird ein Schlüssel verwendet, der während der Installation von IPCop erzeugt wird. Sie können den Schlüssel mit der Schaltfläche "Exportiere Backup Schlüssel auf Ihren lokalen Computer" exportieren. Damit Sie den Schlüssel überhaupt exportieren dürfen, müssen Sie beim Export das Kennwort des Benutzers backup eingeben. Sie exportieren dabei jedoch nicht den Original-Schlüssel, sondern eine mit dem Kennwort des Benutzers backup verschlüsselte Kopie.

Zum Erstellen eines neuen Datensicherungssatzes geben Sie im Feld "Beschreibung" einen Namen für den Datensicherungssatz an und klicken auf den Button "Einen neuen Sicherungssatz anlegen". Der Datensicherungssatz wird erstellt und in der Auflistung unter Datensicherungssätze angezeigt. Um einen vorher exportierten Datensicherungssatz von Ihrem lokalen Computer wieder auf den IPCop zu laden, wählen Sie den Datensicherungssatz über den Button "Durchsuchen" aus und klicken anschließend auf "Import". Der Datensicherungssatz wird nun auf den IPCop hochgeladen und in der Auflistung unter Datensicherungssätze angezeigt.

Im Status-Menü finden Sie außerdem alles, was Sie zur regelmäßigen Überwachung des IPCop-Systems benötigen. Neben der Anzeige der aktuellen Zustände können die wichtigsten System- und Netzwerkaktivitäten auch in Diagrammform dargestellt werden.

Tipps und Tricks

Sollte es einmal vorkommen, dass Sie das Kennwort für den Benutzer root vergessen haben, dann müssen Sie IPCop nicht neu installieren. Sie können auch bei einem bestehenden System das Kennwort zurücksetzen. Zunächst fahren Sie IPCop herunter und starten das System erneut. Bei der Anzeige des GRUB-Bootloaders drücken Sie innerhalb von fünf Sekunden die Taste "a", um die Befehlszeile für den Bootvorgang anzupassen. In dem darauf erscheinenden Bildschirm geben Sie das Wort "single" an das Ende der Zeile und bestätigen mit der Enter-Taste. IPCop startet bis zu einem Shell-Prompt durch. Sie sind nun automatisch als Benutzer root angemeldet, ohne dass Sie ein Kennwort eingeben müssen. Mit den Befehlen *passwd* und *reboot* vergeben Sie ein neues Kennwort für den Benutzer root und führen anschließend einen Neustart durch. Wenn der IPCop wieder hochgefahren ist, können Sie sich als Benutzer root mit dem neuen Kennwort an der Konsole anmelden.

IPCop und Active Directory

Betreiben Sie in Ihrem Netzwerk ein Active Directory, können Sie für die Windows-Clients nicht den DNS-Server von IPCop verwenden. Die Windows-Clients verwenden den DNS, um den Domänen-Controller im Netzwerk zu finden. Da IPCop aber keinen echten DNS-Serverdienst anbietet, sondern nur einen Caching-DNS für Anfragen an externe DNS-Server im Internet, kann er den für eine Active Directory-Umgebung benötigten SRV-Eintrag im internen Netz nicht bereitstellen. Aus diesem Grund müssen Sie Ihre Windows-Clients so konfigurieren, dass Sie über einen

Windows-Server den DNS-Server des Active Directory verwenden. Da dieser aber standardmäßig keine externen Namen aus dem Internet auflöst, müssen Sie den DNS-Server auf Ihrem Windows-Server so einstellen, dass er IPCop als DNS-Forwarder nutzt. Das bedeutet, dass alle DNS-Anfragen, die der Windows-Server nicht beantworten kann, automatisch an den DNS-Server auf IPCop weitergeleitet werden.

Möchten Sie IPCop nachträglich in ein bestehendes Active Directory implementieren, so müssen Sie den DNS-Dienst auf dem Windows-Server entsprechend anpassen. Das Ziel ist es, alle Anfragen für Namen außerhalb der eigenen DNS-Domäne an IPCop weiterzuleiten. Öffnen Sie dazu die DNS-Managementkonsole. Klicken Sie mit der rechten Maustaste auf das Server-Objekt und wählen Sie im Kontextmenü den Punkt "Eigenschaften" aus. Dann wechseln Sie auf den Reiter "Weiterleitungen" und fügen dort im Feld unter "Weiterleitungs-IP-Adressliste" der gewählten Domänen die IP-Adresse Ihres IPCop hinzu.

Add-ons für IPCop

Da IPCop eine Linux-basierte Umgebung ist, ist es sehr einfach, das System den eigenen Wünschen entsprechend zu erweitern und zu modifizieren. Einige Programmierer haben ihre Modifikationen und Erweiterungen zu einem Paket geschnürt und es der Allgemeinheit zur Verfügung gestellt. Diese Modifikationen für IPCop werden Add-ons oder auch kurz "Mods" genannt.

Einige Add-ons sind nur für eine ganz bestimmte IPCop-Version geschrieben worden. Das bedeutet, dass Sie vor dem Update Ihres IPCop auf eine neuere Version sicherstellen müssen, dass das von Ihnen verwendete Add-on auch auf der neuen IPCop-Version einwandfrei funktioniert. Ebenso müssen Sie beachten, dass die offiziellen IPCop-Updates für die Original-Distribution konzipiert sind und wenig Rücksicht auf vorhandene Modifikationen nehmen, sodass nach einem Update eventuell eine Neuinstallation des Add-ons erforderlich sein kann.

Es gibt mittlerweile eine fast unüberschaubare Anzahl an Erweiterungen für den IPCop. Auch dem fortgeschrittenen IPCop-Admin fällt es nicht immer leicht, sich einen Überblick über die verfügbaren Add-ons und deren Funktionalitäten zu verschaffen. Aus diesem Grund wurde das Projekt der IPCop Add-on Datenbank [3] ins Leben gerufen. In dieser Datenbank finden Sie sehr viele IPCop-Add-ons mit einer Kurzbeschreibung und nach Themengebieten sortiert. Die hier vorgestellten Add-ons stellen nur eine sehr kleine Auswahl aller verfügbaren Erweiterungen dar.

Advanced Proxy

Der "Advanced Proxy" erweitert den vorhandenen Web-Proxy um sehr viele Möglichkeiten. Neben zahlreichen Einstellungen zur Cache-Verwaltung bietet der Advanced Proxy auch eine Benutzerauthentifizierung für die verschiedensten Systemumgebungen. Zusätzlich zu der globalen Zugriffssteuerung über IP- und MAC-Adressen können Sie auch eigene Adresskreise definieren, die beliebig ein- und ausgeschaltet werden können, ohne dass administrative Berechtigungen für die Web-Oberfläche erforderlich sind. So haben beispielsweise Lehrkräfte die Möglichkeit, den Internetzugriff für Klassenräume zu steuern.

BlockOutTraffic (BOT)

Das Standardverhalten von IPCop, ausgehenden Verkehr grundsätzlich zuzulassen, ist nicht immer gewünscht. Das Add-on "BlockOutTraffic" (kurz BOT) bietet Ihnen die Möglichkeit, Regeln für den ausgehenden Verkehr sowie zwischen den einzelnen Schnittstellen komfortabel über die Web-Oberfläche zu erstellen. Dabei können Sie auch Dienste und Adressen gruppieren und Zeitregeln festlegen.

Extra Interfaces

Falls Sie bei IPCop mehr interne Schnittstellen als nur Grün und Blau benötigen, finden Sie die Lösung im Add-on "Extra Interfaces". Damit haben Sie die Möglichkeit, den IPCop um bis zu vier weitere interne Schnittstellen, Grau 1 bis Grau 4, auf insgesamt maximal acht Schnittstellen zu erweitern.

IPCop addon binary collection

Nicht nur ein einzelnes Add-on, sondern eine umfangreiche Sammlung von Add-ons ist die "IPCop addon binary collection". Dort finden Sie unter anderem eine ganze Reihe von nützlichen Werkzeugen zur Hardwarediagnose, Programme für die Netzwerkanalyse sowie Clients für die verschiedensten Netzwerkprotokolle wie ssh, rsync oder wget.

URL-Filter

Der "URL-Filter" ist ein Add-on, mit dem Sie steuern können, auf welche Webseiten Ihre Benutzer zugreifen dürfen. Der URL-Filter verwendet dazu eine Datenbank mit verschieden kategorisierten URLs, die bei Bedarf auch automatisch aktualisiert werden kann. Sie können neben den globalen Einstellungen auch Regeln für bestimmte IP-Adressen oder Benutzer erstellen, in denen Sie festlegen können, zu welcher Zeit welche Webseiten freigeschaltet oder gesperrt sind.

Fazit

Mit IPCop steht Ihnen die wohl benutzerfreundlichste Firewall-Lösung der Open Source-Gemeinde zur Verfügung. Keine andere Umgebung ist vergleichbar einfach zu administrieren und konfigurieren. Auch den Vergleich mit kommerziellen Lösungen muss IPCop nicht scheuen – im Gegenteil. Die Firewall ist ebenso sicher und flexibel, zudem vor allem kostenfrei. *(dr)*

Links

[1] IPCop
www.ipcop.org
[2] SourceForge
www.sourceforge.net
[3] IPCop Add-on-Datenbank
www.ipcopaddons.org

Webserver Apache härten

Zutritt verboten!

von Thomas Hümmler

Eine Firewall schützt Netzwerke gegen Angriffe. Allerdings lässt sich nicht alles abschotten, manche Tore müssen offen bleiben. So der Port 80, an dem der HTTP-Server wacht. Wichtig ist, dass dieser korrekt eingerichtet und konfiguriert ist, damit er nichts und niemand unerlaubt durchlässt. Wie das bei dem bekannten Web-Server Apache geht, zeigt dieser Workshop.

Der Feind hat viele Waffen: Beispielsweise greift er mit SQL-Injektionen oder Cross-Site-Scripting (XSS) an. Dem kann der Administrator mit mehreren Maßnahmen begegnen und vorbeugen. Eine in diesem Zusammenhang sinnvolle Maßnahme ist der Einsatz einer Web-Application-Firewall. Für Apache eignet sich dafür der Input-Filter ModSecurity, den wir Ihnen in einer früheren Ausgabe vorstellten [1].

Apache ins Gefängnis

Einen anderen Ansatz als ModSecurity verfolgt das ältere Makejail [2] von Alain Tésio. Es benötigt zusätzlich die Programmiersprache Python sowie die Programme strace und stat. Die in Python geschriebenen Skripts erzeugen für Programme wie bind, ssh, MySQL und Apache eigene Root-Umgebungen mit Hilfe des Unix-Befehls *chroot*. Wenn in einer solchen Umgebung etwas passiert, wird der Rest des Systems nicht infiziert.

Welche Dateien in der separaten Root-Umgebung eingesperrt werden, hängt von mehreren Faktoren ab. Es werden alle erforderlichen Pakete in das chroot-Gefängnis gesteckt, die der Server benötigt. Zusätzlich enthält ein Skript meist schon eine Vorauswahl bestimmter Dateien. Außerdem finden die Skripte durch wiederholtes Starten heraus, auf welche Dateien der Server noch zugreift. Diese werden ebenfalls in die chroot-Umgebung verschoben. Dort werden – falls erforderlich – Verzeichnisse rekursiv erstellt, die Ziele symbolischer Links hinzugefügt sowie die erforderlichen Bibliotheken; Dateirechte bleiben dabei erhalten. Sockets werden nicht kopiert. Sind Dateien aus der /proc-Verzeichnisstruktur betroffen, wird stattdessen das procfs-Dateisystem gemountet. Der Befehl

```
./makejail {Konfigurationsdatei}
```

erzeugt eine chroot-Umgebung für das jeweilige Programm. In Debian liegt Makejail als Paket vor. Die Konfigurationsdateien stehen dort im Verzeichnis "/usr/share/doc/makejail/examples". Um zum Beispiel eine chroot-Umgebung für den Webserver Apache zu erzeugen, lautet der Befehl

```
# makejail
  /usr/share/doc/makejail/examples/
  apache.py
```

Erfolgreich getestet – so steht es in der Konfigurationsdatei – wurde das Skript mit Apache 1.3.22, PHP 4, MySQL und einer Suchmaschine auf dem veralteten Debian Woody. Auf neueren Systemen sollten Sie dieses daher zunächst in einer Testumgebung überprüfen und eventuell die Konfigurationsdatei anpassen. Dabei bietet es sich an, mit einer Kopie zu arbeiten. So ist sichergestellt, dass auch nach einem Paket-Udpate die Datei nicht überschrieben wird. In der Konfigurationsdatei sind einige Direktiven bereits gesetzt, unter anderem:

- chroot-Pfad: /var/chroot/apache
- Startaufruf für den Daemon innerhalb der Umgebung: */usr/sbin/apachectl start*
- Prozessname nach dem des Daemon: apache

Wer Apache 2 einsetzt, sollte sowohl den Startaufruf in "/usr/sbin/apache2ctl start" als auch den Prozessnamen in "apache2" ändern. Wurde der Daemon erfolgreich in der chroot-Umgebung installiert, testet Makejail von außerhalb mit Hilfe der Programme wget und lynx, ob tatsächlich alles innerhalb der Umgebung bleibt.

Apache nur im eigenen Lager

Wenn Sie den Webserver nur intern nutzen, etwa für Testzwecke oder zum Zugriff auf einen zentralen Dokumenten-Pool, schalten Sie ihn am besten für den externen Zugriff ab. Das geschieht mit Hilfe der "Listen"-Anweisung zum Setzen der IP-Adressen und Portnummern. Hinweis: In früheren Versionen war das auch mit dem "BindAddress"-Befehl möglich. In der aktuellen Apache-Version wurde diese Anweisung entfernt.

Ohne die Direktive "Listen" startet Apache seit der Version 2.0 nicht mehr. Die vorgeschriebene Anweisung teilt dem HTTP-Server mit, an welchem Port oder

welcher IP-Adresse er lauschen soll. In Debian und Ubuntu steht diese Direktive in der Datei */etc/apache2/ports.conf*. Dort ist voreingestellt

```
NameVirtualHost *:80
Listen 80
```

Der Webserver gewährt damit uneingeschränkten Zugriff auf Port 80. Wird das geändert, müssen Sie Apache mit */etc/init.d/apache restart* neu starten. Die Zeile "Listen 127.0.0.1:80" in der Apache-Konfiguration sorgt dafür, dass der Server nur auf Anfragen des Localhosts reagiert. Je nach Distribution findet sich die Listen-Anweisung eventuell in einer anderen Konfigurationsdatei. Wo Konfigurationsdaten in anderen Distributionen und Betriebssystemen liegen, erfahren Sie im Apache-Wiki [3].

Soll hingegen der Zugriff im gesamten lokalen Netz erfolgen dürfen, nutzen Sie die Direktive "Allow from" aus dem Apache-Modul "mod_authz_host", das es seit der Version 2.1 gibt. "Allow from" lässt sich in den Bereichen "Directory", "Files" und "Location" verwenden. Für das lokale Netz oder verschiedene Subnetze beschränken Sie einfach den Zugriff auf das Webserver-Verzeichnis, etwa so:

```
<Directory /var/www/>
  Options Indexes FollowSymLinks
  MultiViews
  AllowOverride None
  Order allow,deny
  Allow from 172.20 192.168.2
  RedirectMatch ^/$ /apache2-
  default/
</Directory>
```

Das würde nur Rechner aus dem IP-Adressbereich 172.20.* und 192.168.2.* zulassen. Alternativ können Sie mit *Allow from test.net* auch den Domainnamen angeben.

Nutzung von htaccess-Dateien vermeiden

Eines der Dinge, das in der Apache-Konfiguration am meisten missverstanden wird, sind die htaccess-Dateien. Vielfach kursiert etwa noch die Behauptung, dass die Benutzer-Authentisierung mit Hilfe dieser Dateien geregelt werden müsse. "This is simply not the case" steht dazu in der Apache-Dokumentation [4]. Die Apache-Entwickler schreiben, dass htaccess-Dateien dann genutzt werden sollten, wenn der Herr der Maschinen die Server-Konfiguration nicht häufig ändern will und es daher einzelnen Nutzern erlauben möchte, Änderungen selbst vorzunehmen.

Generell empfehlen die Apache-Entwickler, .htaccess-Dateien zu vermeiden – sowohl die Geschwindigkeit als auch die Sicherheit leiden. Falls es mit der Direktive "AllowOverride" erlaubt ist, htaccess-Dateien zu nutzen, schaut Apache in jedem Verzeichnis nach diesen Dateien, selbst wenn dort keine zu finden sind. Außerdem wird jedes Mal, wenn ein Dokument angefordert wird, die htaccess-Datei geladen. Des Weiteren muss Apache in jedem darüber liegendem Verzeichnis nach diesen Dateien suchen, um keine darin stehende Direktive zu übersehen.

Das Sicherheitsproblem sehen die Entwickler darin, dass Nutzern erlaubt wird, die Server-Konfiguration zu ändern, sodass der Administrator darüber eventuell keine Kontrolle mehr hat. Die Empfehlung der Profis ist daher eindeutig: die "Allow Override"-Direktive auf "none" zu setzen. Außerdem – so das zweite Argument – ist ein Eintrag in einer htaccess-Datei identisch mit dem Eintrag innerhalb eines "Directory"-Bereichs.

CGI-Skripte und SSI

CGI-Skripte und sogenannte Server Side Includes können ebenfalls ein Sicherheitsrisiko sein. SSI sind Direktiven, die innerhalb einer HTML-Seite stehen und ausgeführt werden, wenn die Seite vom Server angefordert wird. Beliebt sind diese, weil sie erlauben, mit wenig Aufwand dynamische Seiten zu erzeugen. Per SSI wird beispielsweise mit *<!—#echo var="DATE_LOCAL" —>* das Datum abgefragt, es erfolgt die Ausgabe eines CGI-Seitenzugriffszählers mit

```
<!–#include virtual="/cgi-bin/
  counter.pl" –>
```

oder die Anzeige eines Verzeichnisses mit Hilfe eines Shell-Befehls:

```
<pre>
<!–#exec cmd="ls" –>
</pre>
```

Anstelle von *ls* nutzen Sie unter Windows den Befehl *dir*. Damit SSI funktioniert, muss es in der Webserver-Konfiguration mit *Options +Includes* eingeschaltet werden. Da die meisten Konfigurationen mehrere Options-Direktiven enthalten, die sich gegenseitig überschreiben können, sollten Sie die Option explizit auf das jeweils gewünschte Verzeichnis anwenden. Außerdem müssen Sie Apache mitteilen, welche Dateien verarbeitet werden.

Die elegante Methode ist die sogenannte XbitHack-Direktive, die Sie mit *XBitHack on* einschalten. Dann müssen Dateien nur mit "chmod +x DATEI.html" das ausführbare Bit erhalten. Unter Windows funktioniert das nicht. Hier hilft nur die Methode, bestimmte Dateien, etwa alle mit der Endung shtml, zu parsen:

```
AddType text/html .shtml
AddOutputFilter INCLUDES .shtml
```

Damit schlagen Sie gleich zwei Fliegen mit einer Klappe. Die Serverlast ist deutlich geringer, weil nicht jedes Mal alle htm- und html-Dateien nach SSIs geparst werden. Außerdem lässt sich so das Risikomanagement in der Konfiguration vereinfachen, weil nur ein bestimmter Dateityp betroffen sein kann.

Was für den Anwender eine feine Sache ist, erfordert vom Administrator entsprechende Vorkehrungen. Denn SSI und CGI-Skripte können mit Hilfe des "exec cmd" jeden Befehl ausführen mit den Benutzerrechten des Webservers. Um möglichen Schaden abzuwenden, hat der Admin verschiedene Möglichkeiten.

Zunächst kann er "suEXEC" aktivieren, damit jedes CGI-Programm und jede SSI-Direktive mit der User-ID und nicht der ID des Webservers startet. Um Anfragen an den suexec-Wrapper weiterzuleiten, hat der Administrator zwei Möglichkeiten: Entweder er definiert innerhalb eines virtuellen Hosts eine "SuexecUserGroup" nach dem Schema

```
SuexecUserGroup user gruppe
```

oder er legt mit der "UserDir"-Direktive Benutzerverzeichnisse fest:

```
UserDir /home/*/www
UserDir disabled root
```

Dies definiert beispielsweise im Homeverzeichnis jedes Benutzers das www-Verzeichnis für den eigenen Web-Auftritt. Dieser wird angezeigt, wenn im Browser jemand *http://beispiel.de/~user/* eingibt. Wichtig ist vor allem die zweite Zeile, denn sie schließt ab der Apache-Version 1.3 das Home-Verzeichnis des Benutzers root explizit aus. Dann haben auch versehentliche Anweisungen wie "UserDir ./" keine Auswirkungen. Im anderen Fall würde "~root" auf das Wurzelverzeichnis des Systems gemappt.

Wer sich mit derlei Dingen nicht herumschlagen will, schaltet CGI und SSI mit *Options +IncludesNOEXEC* einfach ab. Vollständigen Schutz bietet aber auch das noch nicht, denn mit der Anweisung

```
<-#include virtual="..." ->
```

können noch CGI-Skripte aus dem Verzeichnis ausgeführt werden, auf das die "Script Alias"-Direktive verweist.

Weitere Sicherheitsmodule für Apache

Ähnlich wie Makejail arbeitet das nur wenige KByte kleine Apache-Modul mod-chroot [6], das unter anderem als Paket in Debian und Ubuntu vorhanden ist. Es übertragt den Webserver in eine geschützte chroot-Umgebung. Das Modul für die Apache-Version 2.2 bringt drei Dateien mit: das eigentliche Modul, eine Konfigurationsdatei sowie eine Datei mit der Dokumentation. Die Konfigurationsdatei *mod_chroot.load* steht nach der Installation im Verzeichnis "/etc/apache2/mods-available". Um es in die Konfiguration zu laden, wird im Verzeichnis "/etc/apache2/mods-enabled" ein symbolischer Link auf das Modul erzeugt:

```
#cd /etc/apache2/mods-enabled
#ln -s ../mods-
  available/mod_chroot.load
```

Um das Modul zu aktivieren, ist nur die "ChrootDir"-Direktive erforderlich. Die legt das Verzeichnis für die chroot-Umgebung fest, in Debian und Ubuntu beispielsweise *ChrootDir /var/www*. ChrootDir muss in der Hauptkonfiguration stehen, es darf nicht in "Directory"-, "Files"- oder "Location"-Bereichen beziehungsweise htaccess-Dateien vorkommen. Zum Schluss starten Sie den Webserver mit *#/etc/init.d/apache2 restart* neu.

Sollte ein Webserver DoS- oder Brute-Force-Angriffen ausgesetzt sein, bietet das Modul mod-evasive [7] Schutz. Das Debian- und Ubuntu-Paket ist vorkompiliert für Apache-2.x-Server. Um es in die Konfiguration zu laden, wird im Verzeichnis "/etc/apache2/mods-enabled" ein symbolischer Link auf das Modul erzeugt:

```
#cd /etc/apache2/mods-enabled
#ln -s ../mods-available/mod_evasi-
  ve.load
```

Das Modul berichtet per E-Mail und protokolliert seine Aktivitäten im Systemlog mit. IP-Adressen, die Webseiten öfter als ein paar Mal pro Sekunde anfordern, werden in eine Blacklist geschrieben. Das Gleiche gilt für mehr als 50 gleichzeitige Anfragen. Trifft eine der Bedingungen zu, schickt der Server als Antwort die 403-Meldung "Der Zugriff ist nicht erlaubt". Anschließend wird die IP-Adresse für zehn Sekunden geblockt. Fordert der Host in dieser Zeit eine Seite an, muss er noch länger warten.

Soll zusätzlich bei Angriffen eine Mail verschickt werden, kann die Direktive *DOSEmailNotify sie@ihreDomain.tld* hinzugefügt werden. Die mitgelieferte Readme-Datei gibt Auskunft über die einzelnen Direktiven. Unter "/usr/share/doc/libapache2-mod-evasive/examples/" steht außerdem das kleine Perl-Programm *test.pl*, welches eine Prüfung erlaubt, ob der Webserver den Zugang verweigert. *(jp)*

[1] **Injektionen unerwünscht**
IT-Administrator 01/2009

[2] **Makejail**
www.floc.net/makejail/

[3] **Apache-Wiki**
http://wiki.apache.org/httpd/DistrosDefaultLayout

[4] **Apache-Dokumentation zu htaccess**
http://httpd.apache.org/docs/2.2/howto/htaccess.html

[5] **Zu schützende Apache-Verzeichnisse**
http://wiki.apache.org/httpd/DistrosDefaultLayout

[6] **mod-chroot**
http://core.segfault.pl/~hobbit/mod_chroot/dist/

[7] **mod-evasive**
www.zdziarski.com/projects/mod_evasive/

Weitere Links

CGI-Tutorial
http://httpd.apache.org/docs/2.2/howto/cgi.html

SSI-Tutorial
http://httpd.apache.org/docs/2.2/howto/ssi.html

htaccess-How-To
http://httpd.apache.org/docs/2.2/howto/htaccess.html

UserDir-Verzeichnisse
http://httpd.apache.org/docs/2.2/howto/public_html.html

Aktuelle Sicherheitslücken in Apache – "Apache Server Announcements"-Liste
http://httpd.apache.org/lists.html#http-announce.

Links und Ressourcen


Quelle: Pixelio.de

Automatische Installation von Windows 7 (1)

Wie von Geisterhand

von Thomas Joos

Mit Windows 7 stellt Microsoft auch zahlreiche kostenlose Zusatztools zur Verfügung, über die sich das Betriebssystem effizient im Unternehmen verteilen lässt. Dazu gehört die neue Version des Windows Automated Installation Kit (WAIK), das für Windows 7 und Windows Server 2008 R2 optimiert ist. Dieses kostenlose Werkzeug stellt eine Umgebung bereit, mit der auch Installationen in großen Stückzahlen ausgerollt werden können. Außerdem bietet Microsoft noch das Microsoft Deployment Toolkit 2010 an, das Unternehmen ebenfalls bei der Migration zu Windows 7 unterstützt. Im ersten Teil unserer Workshopserie beschäftigen wir uns neben diesen Werkzeugen mit Windows PE und erstellen eine Antwortdatei zur automatischen Installation.

Windows 7 arbeitet mit dem WIM-Imageformat (Windows Imaging). Statt eines sektorbasierten Imageformats ist das WIM-Format dateibasiert. Dies hat mehrere Vorteile: So ist WIM hardwareunabhängig, Administratoren müssen also nur ein Image für verschiedene Hardware-Konfigurationen erstellen. Mit WIM lassen sich mehrere Images in einer zentralen Datei speichern. Außerdem nutzt WIM eine Kompression und das Single-Instance-Verfahren, was die Größe von Imagedateien deutlich reduziert. Single-Instancing ist eine Technologie, bei der jede Datei nur einmal gespeichert wird. Wenn zum Beispiel Image 1, 2 und 3 alle die gleiche Datei A enthalten, dann sorgt Single-Instancing dafür, dass Datei A nur einmal tatsächlich gespeichert wird.

WIM-Images ermöglichen die Offline-Bearbeitung von Images. So können Administratoren Betriebssystemkomponenten, Patches und Treiber hinzufügen oder löschen, ohne ein neues Image erstellen zu müssen. Damit ist es beispielsweise möglich, einen Treiber auszutauschen, ohne das Administratoren-Image komplett neu erstellen zu müssen. Ein weiterer Vorteil des WIM-Formats ist das sogenannte "non-destructive Deployment". Das bedeutet, dass beim Einspielen des Images die Daten, die sich bereits auf der Festplatte befinden, nicht gelöscht oder überschrieben werden müssen. Bei Windows XP verhinderten technische Einschränkungen die Erstellung eines einzigen Image, das auf allen Computern funktioniert. Unterschiedliche HAL-Schichten (Hardware Abstraction Layer) bedeuteten, dass Administratoren mehrere Images pflegen müssen. In Windows 7 bestehen diese technischen Einschränkungen nicht mehr; das Betriebssystem ist in der Lage, die benötigte HAL festzustellen und sie automatisch zu installieren.

Antwortdateien und Kataloge

Windows Systemabbild-Manager (Windows System Image Manager, Windows-SIM) ist ein Tool aus dem WAIK, mit dem Administratoren einfach Antwortdateien auf XML-Basis erstellen. Auch Netzwerkfreigaben lassen sich so konfigurieren, dass diese Konfigurationen zur Verteilung von Windows 7 und zusätzliche Treiber enthalten. Die Antwortdatei enthält das Grundgerüst, das Windows für die einzelnen Konfigurationsphasen benötigt. Dadurch lassen sich Eingaben wie PC-Namen, Seriennummer und weitere Eingaben in einer Datei vorgeben, so dass während der Installation keinerlei Eingaben mehr notwendig sind.

Die Katalogdatei eines Image (*.clg) enthält die Einstellungen und Pakete, die in einem Image auf WIM-Basis enthalten sind. Da auch die normale Installation von Windows 7 auf einem WIM-Image basiert, finden Sie auf der Windows 7-Installations-DVD im Ordner "\sources" die CLG-Dateien der verschiedenen Windows-Editionen. WIM-Images haben als Dateityp die Bezeichnung *.wim. In diesen Dateien ist festgelegt, welche Komponenten Windows 7 bei den einzelnen Windows 7-Editionen installiert. Windows 7-Antwortdateien speichern Sie am besten als *AutoUnattend.xml*. Beim Starten der Installation durchsucht Windows 7 standardmäßig das Stammverzeichnis von

Laufwerken, auch USB-Sticks, auf diese Datei und verwendet die hinterlegten Antworten zur Installation.

Windows Preinstallation Environment (Windows PE)

Bei Windows PE handelt es sich um eine Minimalversion von Windows 7, welche die Kernelfunktionen des Betriebssystems enthält. Auch die Basisinstallation von Windows 7 basiert auf Windows PE, es gibt keinen textorientierten Teil der Installation mehr wie noch bei Windows XP oder Windows Server 2003. Für Windows 7 gibt es daher keine DOS-Bootdisketten mehr, diese hat Microsoft durch Windows PE ersetzt. Während der Installation von Windows 7 lädt die Installationsroutine die Windows PE-Version auf der DVD (*\sources\boot.wim*) mit einer Größe von etwa 140 MByte. Auf dieser Basis wird dann Windows 7 installiert. Auch die Computerreparaturoptionen von Windows 7 sind auf Basis von Windows PE aufgebaut und keine eigenständigen Programme mehr.

Nachdem Sie die Antwortdatei erstellt oder einen Master-PC installiert haben, können Sie ein Image des PCs erstellen, auf dessen Basis Sie die Windows 7-Installationen im Netzwerk verteilen. Die dazu notwendigen Tools sind im WAIK enthalten. Neben der Möglichkeit, Antwortdateien zu verwenden, können Sie auch einen Computer mit Windows 7 installieren und als Image zur automatisierten Installation verwenden. Microsoft stellt dazu das Tool ImageX (das Tool befindet sich im Verzeichnis "C:\Windows\system32\sysprep") aus dem WAIK zur Verfügung. Wenn Sie die Installation von Windows 7 auf dem Mastercomputer abgeschlossen haben, führen Sie in der Befehlszeile *sysprep.exe /oobe /generalize /shutdown* aus. Bei diesem Vorgang bereinigt der Assistent den Computer von den Benutzer- und Computereinstellungen.

Sysprep startet nur auf Computern, die sich in einer Arbeitsgruppe befinden. Die Ausführung auf Computern, die Mitglied einer Domäne sind, unterstützt Sysprep dagegen nicht. Um bei einem solch vorbereiteten Computer ein Image zu erstellen, sollten Sie eine Windows PE-CD verwenden oder Windows PE über die Windows-Bereitstellungsdienste im Unternehmen zur Verfügung stellen.

Windows-Abbilder erstellen mit ImageX

Nachdem auf dem Mastercomputer Windows 7 oder Windows Server 2008 installiert und vorbereitet wurde, booten Sie den Computer mit Windows PE. Anschließend verwenden Sie in der Befehlszeile den Befehl

```
Imagex.exe /compress fast
  /capture C: C:\mein-image.wim
  "{Beschreibung}"
  /verify
```

um ein Image der Installation zu erstellen. Statt "mein-image.wim" können Sie eine beliebige Bezeichnung für das Image verwenden. Booten Sie einen Computer mit Windows PE, legt Windows drei Partitionen an:

- C: In dieser Partition befindet sich das installierte Windows 7, von dem Sie ein Image erstellen.
- D: Hierbei handelt es sich um die CD mit den Windows PE-Installationsdateien. Hier finden Sie auch ImageX.
- X: Diesen Laufwerkbuchstaben verwendet Windows PE für die Laufzeitumgebung. Diese Partition befindet sich im Arbeitsspeicher.

Nachdem Sie die Erstellung des Image gestartet haben, beginnt ImageX, die angegebene Partition zu scannen und das Image zu erstellen. Dieses können Sie über die Windows-Bereitstellungsdienste von Windows Server 2008 verteilen.

Sie können das bereitgestellte Image auch bearbeiten, zum Beispiel ein Betriebssystemimage bereitstellen, Gerätetreiber hinzufügen und die Bereitstellung wieder aufheben. Für das Mounten eines Image verwenden Sie den Befehl

```
imagex /mountrw {Pfad zum Image und
  *.wim-Datei} {Pfad in den das
  Image gemounten wird}.
```

Mit dem Befehl

```
peimg.exe /inf={Pfad zur *.inf-Datei
  des Treibers} {Gemounteter Pfad}
```

kopieren Sie Treiber in das Image. Über *imagex /unmount /commit {Gemounteter Pfad}* heben Sie die Bereitstellung wieder auf und speichern die Änderungen. Das Image enthält jetzt den kopierten Treiber. Um das erstellte Image wieder auf andere Computer zu installieren, verwenden Sie Windows PE, ImageX oder am besten die Windows-Bereitstellungsdienste.

Verteilen von Windows 7 über die Windows-Bereitstellungsdienste

Sobald ein WDS-Server installiert und eingerichtet ist, können Sie die Abbilder hinzufügen. Hier gibt es verschiedene Typen:

- Ein Startabbild kommt zum Einsatz, wenn auf dem Client Windows PE starten soll.
- Installationsabbilder dienen der Installation von Windows und erfordern eine Abbildgruppe. Eine Abbildgruppe ist ein Ordner, der sich unterhalb des Knotens "Installationsabbilder" befindet. Für alle Client-Computer, die keine Unterstützung für PXE bieten, gibt es die Möglichkeit, ein Startabbild zu exportieren. Somit lassen sich auch diese Client-Computer durch den WDS-Server bedienen.
- Suchstartabbilder erhalten vor der Generierung die Information, welchen Bereitstellungsserver sie verwenden.
- Aufzeichnungsabbilder bieten eine Alternative zum Befehlszeilenprogramm *ImageX.exe*. Beim Start eines Clients mit einem Aufzeichnungsabbild ruft der Server das Aufzeichnungsdienstprogramm der Windows-Bereitstellungsdienste auf. Es führt den Benutzer durch die erforderlichen Schritte zum Aufzeichnen und Hinzufügen eines neuen Abbildes. Das Aufzeichnungsabbild müssen Sie als Startabbild hinzufügen.

Bild 1: In der Konfiguration der Windows-Bereitstellungsdienste wird festgelegt, welche Netzwerk-Bootprogramme verwendet werden

Für das Booten über das Netzwerk (PXE) stellen die Bereitstellungsdienste verschiedene Network-Bootstrap-Programme (NBP) zur Verfügung. Das Tool *PXEboot.com* erfordert, dass der Benutzer beim Starten des Computers die Taste F12 drücken muss, um einen Netzwerkboot durchzuführen. Nutzen Sie *PXEboot.n12*, erfolgt der Boot über das Netzwerk ohne Drücken der Funktionstaste. Mit *AbortPXE.com* legen Sie fest, dass ein Computer direkt das nächste verfügbare Bootmedium nutzt. Es erfolgt kein Netzwerkboot. Steht in der Bootreihenfolge des Rechners das Booten über Netzwerk vor dem Booten von Festplatte und nutzen Sie *PXEboot.n12*, bootet der Client bei jedem Hochfahren über das Netzwerk und verwendet nicht das eigentliche Betriebssystem. Dieses Verhalten lässt sich dadurch vermeiden, indem Sie PXEboot oder AbortPXE verwenden.

Automatisierte Installation von Windows 7 über WDS

Ein Client-Computer startet mit PXE im Netzwerk. Nach dem Laden des BIOS sendet das PXE-ROM auf der Netzwerkkarte eine Netzwerk-Dienstanforderung an den nächstgelegenen DHCP-Server. Mit der Anforderung sendet der Client seine GUID (Globally Unique Identifier). Der DHCP-Server erteilt dem Client eine IP-Lease mit Optionen für DNS (006), Domäne (015) und PXE-Server (060). Als Nächstes startet das Bootimage als Startabbild mit Windows PE, das in das RAM geladen wird. Über einen Eintrag in der Antwortdatei passt der Assistent die Festplatte an. Das Setup führt die in der Antwortdatei enthaltene Anmeldung an den WDS-Server aus. Existiert dieser Eintrag nicht, erhalten Sie eine Authentifizierungsanforderung.

Um WDS auf einem Server zu installieren, sollten Sie im Netzwerk zunächst die Voraussetzungen schaffen. Sie benötigen ein Active Directory, eine funktionsfähige DNS-Infrastruktur und einen DHCP-Server. Die Installation des WDS erfolgt unter Windows Server 2008 als Serverrolle. Startabbilder kommen dann zum Einsatz, wenn Sie eine automatisierte Windows 7-Installation über Antwortdateien durchführen wollen. Bei dieser Installationsmethode findet die Installation von Windows 7 unabhängig von den Windows-Bereitstellungsdiensten über eine Antwortdatei statt. Der WDS startet dazu auf dem Client lediglich die Windows PE-Umgebung. Hier lässt sich entweder ein eigenes Abbild erstellen und bearbeiten oder Sie verwenden das Standardabbild *boot.wim* aus dem Verzeichnis "\sources" auf der Windows 7-DVD. Dieses sollten Sie vorher auf die Festplatte des Servers kopieren.

Sobald die Windows-Bereitstellungsdienste installiert und konfiguriert sind und Sie ein Startabbild hinzugefügt haben, können Computer über das Netzwerk booten. Achten Sie darauf, dass die Netzwerkkarte des Computers PXE beherrscht und der DHCP-Server korrekt mit der Option 60 konfiguriert ist. Sobald sich der Computer erfolgreich mit dem WDS-Server verbindet, erhält er eine IP-Adresse und Windows PE startet auf diesem Computer.

Erstellen einer Antwortdatei zur automatisierten Installation von Windows 7

Im folgenden Abschnitt zeigen wir Ihnen in mehreren Schritten, wie Sie eine automatisierte Installation von Windows 7 über eine Antwortdatei erstellen. Nach der Installation des WAIK finden Sie die Beispielantwortdatei *Corp_autounattended_sample.xml* unter "C:\Programme\Windows AIK\Samples".

Installieren Sie zunächst das WAIK auf einem Computer. Nun kopieren Sie die Datei *install.wim* von der Windows 7-DVD aus dem Verzeichnis "\sources" in ein temporäres Verzeichnis auf der Festplatte, zum

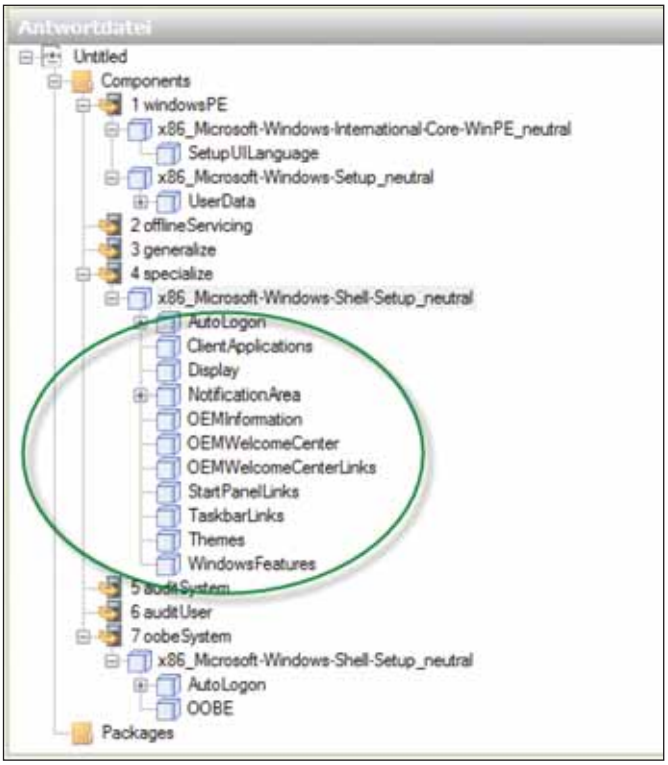


Bild 2: Die nicht benötigten Komponenten aus dem Bereich der Antwortdatei können gelöscht werden

Beispiel "c:\unattend". Starten Sie über "Alle Programme / Microsoft Windows AIK" den Windows Systemabbild-Manager (Windows System Image Manager) und öffnen Sie über "Datei / Windows-Abbild auswählen" die zuvor kopierte Datei *install.wim* auf der Festplatte. Jetzt legen Sie fest, welche Windows 7-Edition Sie installieren wollen. Anschließend müssen Sie das Erstellen einer neuen Katalogdatei bestätigen. Das Paket wird jetzt eingelesen und im Windows System Image Manager angezeigt. Das Erstellen des Katalogs kann einige Zeit dauern.

Nun starten Sie die Erstellung einer neuen Antwortdatei über "Datei / Neue Antwortdatei". Die Antwortdatei wird mit ihren sieben verschiedenen Bereichen in der Mitte des Fensters angezeigt. Die Bereiche stellen die verschiedenen Phasen während der Installation dar. Im Bereich "Windows-Abbild" erweitern Sie "Components". Hier nehmen Sie verschiedene Einstellungen vor, um die Installation an Ihre Bedürfnisse anzupassen (die wichtigsten Beispiele zeigen wir Ihnen in der nachfolgenden Anleitung). Klicken Sie hierzu mit der rechten Maustaste auf die Komponente und wählen Sie die gewünschte Konfigurationsphase aus. So wird die Komponente der Antwortdatei in der Phase der Windows-Installation hinzugefügt. Jetzt klicken Sie unterhalb von "x86_Microsoft-Windows-International-Core-WinPE_..." mit der rechten Maustaste auf "SetupUILanguage" und wählen "Einstellungen zu Pass 1 windowsPE hinzufügen". Anschließend fügen Sie noch den Bereich "x86_Microsoft-Windows-Setup\UserData" zum gleichen Bereich hinzu. Die drei Bereiche "x86_Microsoft-Windows-Shell-Setup\OOBE" (zu Bereich 7), "x86_Microsoft-Windows-Shell-Setup\AutoLogon" (zu Bereich 7) und "x86_Microsoft-Windows-Shell-Setup" (zu Bereich 4) fügen Sie ebenfalls hinzu. Im Bereich 4 bei der Antwortdatei können Sie über die rechte Maustaste alles unterhalb "x86_Microsoft-Windows-Shell-Setup_neutral" löschen, den "Hauptpunkt x86_Microsoft- Windows-Shell-Setup_neutral" aber nicht.

Anschließend füllen Sie die verschiedenen Bereiche der Antwortdatei mit den Daten, die für die Installation notwendig sind. Klicken Sie auf "x86_Microsoft-Windows-International-Core-WinPE". Hier setzen Sie die Spracheinstellungen unterhalb des Bereiches "Einstellungen". Dabei spielen die Werte "InputLocale" (Eingabe während der Installation), "SystemLocale" (Standardsprache der Programme), "UILanguage" (Standardsprache der Benutzeroberfläche) und "UserLocale" (Benutzereinstellung für Datum, Zeit, Währung und Zahlen) eine wichtige Rolle. Tragen Sie bei diesen Werten jeweils "de-DE" ein. Klicken Sie dann im Bereich "Antwortdatei" auf den Wert "SetupUILanguage". Bei "UILanguage" (Sprache der Menüs während der Installation) tragen Sie ebenfalls "de-DE" ein. Bei "WillShowUI" (legt fest, wann ein Meldefenster erscheinen soll) tragen Sie "OnError" ein.

Klicken Sie als Nächstes bei "Antwortdatei" auf "UserData". Bei "AcceptEula" tragen Sie "true" ein. In diesem Fall werden

die Lizenzbedingungen (EULA) automatisch bestätigt. Bei "FullName" und "Organization" tragen Sie ein, für wen das Betriebssystem registriert ist. Klicken Sie danach bei Antwortdatei auf "ProductKey". In den Einstellungen können Sie den Produktschlüssel von Windows 7 eintragen und wieder "OnError" bei "WillShowUI". Klicken Sie nun auf "x86_Microsoft-Windows-Shell-Setup_neutral" im Bereich 4 und tragen Sie bei "Computername" den Namen des Computers ein. Wählen Sie als Nächstes "x86_Microsoft-Windows-Shell-Setup_neutral" im Bereich 7 aus und tragen unter "TimeZone" "W. Europe Standard Time" ein.

Klicken Sie jetzt auf "AutoLogon" im Bereich 7. Bei "Enabled" tragen Sie "true" ein, bei "LogonCount" setzen Sie den Wert mindestens auf "1". Tragen Sie hier "2" ein, werden die ersten zwei Anmeldungen automatisch durchgeführt. Bei "Username" tragen Sie "Administrator" ein. Klicken Sie dann im mittleren Bereich auf "Password" und geben dann im rechten Bereich das Kennwort unter "Value" an.

Jetzt wählen Sie im mittleren Bereich "OOBE". Diese Option steht für die "Out of the Box Experience", das Verhalten des Betriebssystems direkt nach der Installation. Anschließend werden die Werte für OOBE auf der rechten Seite gepflegt: "HideEULAPage" setzen Sie auf "true", bei "NetworkLocation" (Netzwerkstandort) wählen Sie "Home" oder "Work" aus. Bei "ProtectYourPC" wird das Sicherheitsverhalten festgelegt (1 = Empfohlene Einstellungen, 2 = Nur automatische Updates aktivieren, 3 = Schutz deaktivieren). Mit "SkipMaschineOOBE" legen Sie fest, ob die Willkommensseite angezeigt wird, "true" blendet diese aus. Der Wert "true" bei SkipUserOOBE blendet das Willkommenscenter aus.

Im Anschluss daran überprüfen Sie die Antwortdatei über "Extras / Antwortdatei überprüfen" auf eventuelle Fehler. Im Bereich "Meldungen" dürfen keine Fehler erscheinen. Nur die Meldung, dass die Einstellung SkipOOBE veraltet ist, stellt kein Problem dar. Speichern Sie die Antwortdatei über "Datei / Antwortdatei speichern" als *AutoUnattend.xml* ab. Die Erstellung der Datei ist damit abgeschlossen. Speichern Sie die Datei auf einem USB-Stick und verbinden diese mit dem Rechner, auf dem Sie Windows 7 mit der Datei automatisiert installieren wollen. Booten Sie von der Windows 7-DVD, verwendet der Setup-Assistent die Antwortdatei zur automatisierten Installation. Die Installation über diese Antwortdatei ist allerdings noch nicht vollkommen automatisiert. Dazu müssen Sie auch die Festplattenkonfiguration automatisch steuern. Dahin kommen wir in den nächsten Abschnitten.

So installieren Sie Windows 7 über einen USB-Stick

Verbinden Sie den USB-Stick mit einem Windows 7-Computer. Sie benötigen für den Betrieb das Befehlszeilen-Tool "Diskpart". Booten Sie vom USB-Stick, können Sie mit einer Antwortdatei einfach automatisiert Windows 7 über einen USB-Stick installieren, was auf Computern ohne DVD-Laufwerk, beispielsweise Netbooks, durchaus hilfreich sein kann:

1. Starten Sie eine Befehlszeile über das Kontextmenü im Administratormodus.
2. Starten Sie die Festplattenverwaltung in der Befehlszeile mit Diskpart.
3. Geben Sie nacheinander folgende Befehle ein:

```
list disk
select disk {Nummer des USB-Sticks aus list disk}
clean
create partition primary
```

4. Geben Sie *active* ein, um die Partition zu aktivieren. Dies wird für den Bootvorgang benötigt.
5. Formatieren Sie den Datenträger mit *format fs=fat32 quick*.
6. Geben Sie den Befehl *assign* ein.
7. Beenden Sie Diskpart mit *exit*.
8. Wechseln Sie in der Befehlszeile in das Verzeichnis "\boot" der Windows 7-DVD.
9. Geben Sie optional den Befehl *bootsect /nt60 {Laufwerksbuchstabe des USB-Sticks}* ein.
10. Kopieren Sie den Inhalt der Windows 7-DVD in das Stammverzeichnis des USB-Sticks.
11. Verbinden Sie den USB-Stick mit dem Zielgerät und stellen Sie im Bios oder dem Bootmenü die Option ein, dass der Rechner von USB bootet.
12. Starten Sie den Rechner und stellen Sie sicher, dass der Bootvorgang über USB startet.

Erweitern einer Antwortdatei zur automatisierten Partitionierung der Festplatten

Wollen Sie nicht nur die Windows-Installation automatisieren, sondern auch die Partionierung, können Sie auch diese Vorgaben in der Antwortdatei hinterlegen. Zunächst öffnen Sie die erstellte Antwortdatei *AutoUnattend.xml* im Windows-Systemabbild-Manager. Er-

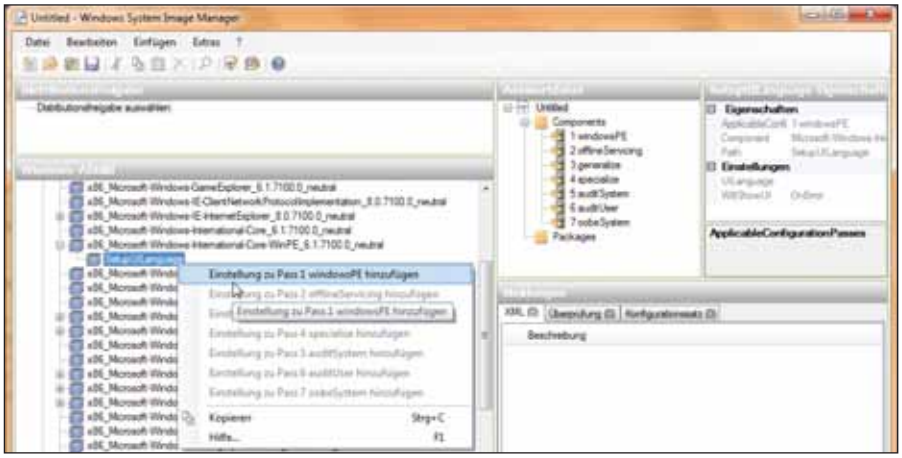


Bild 3: Hinzufügen der ersten Komponente zur automatisierten Installation

weitern Sie im Bereich "Windows-Abbild" die Komponente "x86_Microsoft-Windows-Setup_neutral" und dann "DiskConfiguration". Klicken Sie mit der rechten Maustaste auf "Disk" und fügen Sie diesen Wert dem Bereich 1 hinzu. Fügen Sie dann noch die Option "InstallTo unter x86_Microsoft-Windows-Setup_neutral/ImageInstall/OSImage" zum Bereich 1 hinzu.

Die hinzugefügten Werte konfigurieren Sie jetzt wieder im Bereich "Antwortdatei". Klicken Sie mit der rechten Maustaste auf "CreatePartitions" und wählen Sie "Neue CreatePartition einfügen". Den Befehl können Sie so oft wiederholen, wie Sie Windows-Partitionen auf dem Rechner automatisch erstellen wollen. Klicken Sie anschließend mit der rechten Maustaste auf "ModifyPartitions" und wählen Sie "Neue ModifyPartition einfügen" aus. Den Befehl müssen Sie ebenfalls so oft wiederholen, wie es Partitionen auf dem Computer geben soll. Wollen Sie eine Konfiguration mit zwei Partitionen, fügen Sie der Antwortdatei eine zweite Komponente "CreatePartition" und eine zweite Komponente "ModifyPartition" hinzu, indem Sie im Bereich "Windows-Abbild" mit der rechten Maustaste auf die Komponente klicken und anschließend die entsprechende Konfigurationsphase auswählen.

Klicken Sie dann auf "DiskConfiguration" und legen Sie für den Wert "WillShowUI" wieder "OnError" fest. Klicken Sie dann auf "Disk" und tragen beim Wert "DiskID" "0" ein. Windows wird dann auf der ersten Platte im Computer installiert. Mit "true" bei "WillWipeDisk" wird vor der Installation der Inhalt der Platte gelöscht. Navigieren Sie nun im mittleren Bereich auf "CreatePartition" unterhalb von "CreatePartitions". Mit dem Wert "Extend" legen Sie im Gegensatz zu "true" mit "false" fest, dass der Assistent die Partition nicht auf die gesamte Festplattengröße erweitert. Bei Size geben Sie den Wert in MByte ein, wenn Sie nicht die ganze Platte bei "Extend" verwenden, also "true" eintragen. Mit "Type" legen Sie die Art der Partition fest, bei der ersten am besten "Primary". Bei Order tragen Sie "1" ein.

Als Nächstes klicken Sie den Eintrag "ModifyPartition" unterhalb von "ModifyPartitions" an. Hier konfigurieren Sie die erstellte Partition noch genauer. Der Wert "Active" setzt mit "true" die Partition auf aktiv, nur so kann Windows 7 von der Partition starten. Mit "Extend" und "true" verwendet Windows die gesamte Platte. Über die Option "Format" legen Sie mit dem Wert "NTFS" das Dateisystem fest. Mit "Label" können Sie den Namen des Laufwerks auf einen beliebigen Wert setzen und über "Letter" konfigurieren Sie den Laufwerkbuchstaben, also am besten "C". Der Wert "1" bei "Order" gibt die Reihenfolge an, in der die Partition angepasst werden soll, wenn Sie mehrere Partitionen erstellen lassen. "PartitionID" mit dem Wert "1" legt die ID der Partition fest, welche modifiziert werden soll.

Nun klicken Sie im Bereich "Antwortdatei" auf "OS Image". Hier tragen Sie bei "InstallToAvailablePartition" den Wert "false" ein. So verwendet der Assistent nicht die erste verfügbare Festplatte zur Installation des Betriebssystems, sondern die in der Antwortdatei konfigurierte Partition (siehe nächster Schritt). Bei "WillShowUI" aktivieren Sie wieder "OnError". Jetzt klicken Sie im Bereich "Antwortdatei" auf "InstallTo". Hier legen Sie fest, auf welcher Platte (daher bei "DiskID" der Wert "0") und auf welcher Partition Sie Windows 7 installieren wollen. Tragen Sie bei "PartitionID" den Wert "1" ein, also die erste Partition auf der ersten Platte. Anschließend überprüfen Sie die Antwortdatei wieder und speichern anschließend erneut.

Im zweiten Teil dieser Workshopserie wenden wir uns der Windows 7-Installation per Computerabbild und ImageX sowie der Einbindung von Windows 7 in virtuelle Festplatten zu. *(jp)*

Quelle: drizzd - Fotolia.com

Web-Applikationen absichern

Trutzburg PHP

von Thomas Drilling

Seitdem sich PHP von der einfachen Skriptsprache für die Entwicklung dynamischer Webseiten zur objektorientierten Allzweckwaffe für Millionen von Web-Anwendungen entwickelt hat, steht PHP im Zentrum der Sicherheitsdebatte. Denn PHP-basierte Web-Applikationen bilden anno 2010 entweder als Web 2.0-Anwendungen oder in Form eines der zahlreichen PHP-basierten CMS-Systeme das Gros des modernen Web-Angebotes und stehen damit im Fokus der meisten Angriffs-Szenarien. In diesem Workshop zeigen wir Ihnen die wichtigsten Maßnahmen, um Ihre PHP-Umgebung gegen Angriffe zu härten.

PHP hat sich zu einer der beliebtesten Sprachen zur Entwicklung für Web-Anwendungen entwickelt, steht aber auch seit Jahren in der Kritik. Tief verankert sind vor allem Bedenken hinsichtlich der Sicherheit von PHP. Dabei ist zunächst zu klären, was eigentlich mit "PHP-Sicherheit" gemeint ist. PHP ist insbesondere in Version 5 eine häufig genutzte Sprache zur Erstellung moderner Web-Anwendungen. Sicherheitskritischer PHP-Code gilt heute als wichtigstes Einfallstor für Angriffsszenarien wie Cross Site Scripting, Parametermanipulation, Pishing oder SQL-Injection. Neben den mittelbar betroffenen Internetnutzern betrifft die Frage nach der Sicherheit vor allem zwei Interessengruppen: Entwickler, die beim Einsatz von PHP-Skripten elementare Implementierungsregeln beachten müssen und Administratoren, die mit der Wartung von Web- und Datenbankservern betraut sind. Geht hier etwas schief, kann ein ernsthafter wirtschaftlicher Schaden die Folge sein.

Oft gerät die Programmiersprache selbst ins Zentrum der Kritik. Zweifelsohne weist PHP eine Reihe von Merkmalen auf, die fast zwangsläufig eine Sicherheitsdiskussion notwendig machen. Dieser Workshop erörtert jedoch nicht die Sicherheitsmerkmale der Sprache selbst, sondern konzentriert sich auf die Rolle des Administrators eines Webservers. Der IT-Verantwortliche sieht sich tagtäglich mit fehlerhaften oder unsicher programmierten PHP-Anwendungen konfrontiert und steht in der Pflicht, Kernel und Webserver so zu härten, dass über anfällige Skripte eingeschleuster Code möglichst keinen Schaden anrichtet oder gar den gesamten Webserver in den Abgrund reißt. Hinsichtlich der dabei verfügbaren Mittel besteht ein erheblicher Unterschied darin, ob Sie Ihre PHP-Anwendungen auf dem eigenen Server hosten oder auf die LAMP-/XAMP-Konfiguration Ihres Service Providers angewiesen sind. Denn der ISP ist zwar selbst an einer sicheren PHP-Konfiguration interessiert, muss aber zwischen den Bedürfnissen seiner Kunden, auf die Konfiguration virtueller Hosts Einfluss nehmen zu können, und einer sicheren, aber unflexiblen Gesamtkonfiguration abwägen.

Mehrstufige Sicherheitskonzepte

Der Webserver sollte stets Teil eines typischen "Defense in Depth"-Sicherheitskonzeptes sein, das wie die Schichten einer Zwiebel von einer Sicherung auf mehreren Ebenen ausgeht. Dabei ist schon die Netzwerkebene Teil des Sicherheitskonzeptes, die den Webserver vom internen Netz durch einen Paketfilter abschirmt. Auf dem Webserver selbst kommt ein gehärteter Kernel zum Einsatz, der von sich aus Angriffe gegen den IP-Stack abwehrt und das Nachladen oder Ausführen von Kernel-Modulen verbietet. Außerdem sorgt eine im Kernel implementierte chroot-Umgebung dafür, Anwendungen voneinander zu isolieren. Eine Web Application Firewall (WAF) schließlich kann webbasierte Angriffe abwehren und aus dem regulären Netzwerkverkehr herausfiltern.

Weitere Maßnahmen dieser tiefgreifenden Sicherheitskonzeption können auf Betriebssystem-Ebene implementiert sein. Dabei sollten Sie einen Unix/Linux-Server bevorzugen, weil Unix von jeher über ein differenziertes Berechtigungsmodell mit Benutzern und Gruppen verfügt, das für den Einsatz der meisten PHP-Konfigurationstipps und Skripte Voraussetzung ist. Außerdem funktionieren auch die meisten PHP-Module und Erweiterungen nur auf Apache-Servern zuverlässig. Auf die Serverarchitektur des ISPs ist zwar keine direkte Einflussnahme möglich, aber bei

der Auswahl des Betriebssystems für den Vserver oder Rootserver haben Sie bei faktisch jedem Provider die freie Wahl. Wer allerdings in seiner Firma mit der Entwicklung und Implementierung eines tragfähigen Sicherheitskonzeptes beauftragt ist, sollte sich klar machen, dass die eigentliche Sicherheit von PHP beziehungsweise des Webservers nur ein kleiner Baustein eines Sicherheitskonzeptes sein kann; Verschlüsselungstechnologien, Benutzerkonten und Verhaltensregeln für den Umgang mit Daten gehören ebenfalls dazu. Die wichtigsten Informationsquellen zur PHP-Sicherheit sind die Mailinglisten "Full Disclosure", "BugTraq" und insbesondere für Entwickler von Webapplikationen "WebAppSec". Außerdem gehört das Buch "PHP-Sicherheit" [1] zu den besten deutschsprachigen Standardwerken zum Thema.

Wege zum sicheren Webserver

Der IT-Verantwortliche für den Betrieb eines Webservers kann auf die Sicherheit der eingesetzten PHP-Anwendungen und Skripte – einmal abgesehen von deren Konfiguration bei der Installation – meist wenig Einfluss nehmen. Er kann aber dafür sorgen, dass fehlerhafte oder unsichere Webapplikationen nicht den eigenen Server kompromittieren oder die Integrität von Kundendaten gefährden. Die Absicherung eines PHP-Servers betrifft konkret drei Bereiche, nämlich den eigentlichen Webserver, die PHP-Installation und den Datenbankserver (MySQL). Die meisten Möglichkeiten bei der Einflussnahme hat der Administrator bei der PHP-Installation selbst. Der Server dagegen muss sowohl gegen Angriffe von außen als auch gegen böswillige Attacken von innen geschützt sein. Das kann beispielsweise bei Hostern der Fall sein, wenn bösartige "Kunden" auf dem gleichen Server benachbarte Vhosts angreifen. Sofern ein Webhoster nicht einfach mehrere Vserver (virtuelle Linux-Installationen) auf einem einzigen physischen Server betreibt, muss er eine effiziente Möglichkeit finden, solche Angriffe von innen nach außen zu unterbinden. Allerdings zieht jede Maßnahme Einschränkungen in der dem Kunden gebotenen Funktionalität nach sich.

PHP sicher installieren

Wie angedeutet bietet die PHP-Installation selbst die meisten Möglichkeiten zur Einflussnahme auf die Sicherheit des PHP-Servers. Für die Installation von PHP auf dem Apache-Webserver gibt es konkret zwei Methoden:

- Das Installieren von **PHP als Apache-Modul** erzielt zwar die bestmögliche Integration mit dem Webserver und damit auch die bestmögliche Funktionalität, bringt aber eine ganze Reihe von Sicherheitsproblemen mit sich.
- Das Installieren von **PHP als CGI** ermöglicht dagegen eine effizientere gegenseitige Abgrenzung von PHP-Skripten, verursacht aber Geschwindigkeitseinbußen und verringert den Funktionsumfang.

PHP-interne Sicherheitsmaßnahmen wie "PHP Safe Mode" oder "open_basedir" sind immer von der jeweiligen Unterstützung der PHP-Extension abhängig. Aus Sicherheitsgründen ist es daher schon für sich empfehlenswert, nicht zu viele PHP-Erweiterungen zu benutzen, denn nicht jede beachtet den Safe Mode.

PHP als Apache-Modul

PHP enthält für eine ganze Reihe von verfügbaren Webserver-Architekturen je ein eigenes Server-API (SAPI), so auch für jede neue Apache-Version. Die Installation von PHP verläuft aber bei allen auf UNIX-Systemen eingesetzten Webservern ähnlich. PHP lässt sich hierbei als "Dynamic Shared Object" (DSO) installieren, was übrigens keinen Geschwindigkeitsnachteil gegenüber dem statischen Übersetzen des Moduls auf dem Server bedeutet, die Konfiguration und Wartung aber erheblich vereinfacht. Sie müssen dann nämlich nicht für jede neue PHP-Version den Webserver neu kompilieren. Wenn Sie PHP als Apache-Modul konfigurieren möchten, müssen Sie sicherstellen, dass der Webserver mit Unterstützung für dynamische Module kompiliert ist. Der zugehörige Aufruf für das configure-Skript könnte in diesem Fall so aussehen:

```
./configure –prefix=/usr/local/
  apache –sysconfdir=/etc/httpd
  –exable-suexec –enable-module=most
  –suexec-caller=httpd –enable-
  shared=max –server-uid=httpd
```

Jeder DSO-fähige Apache ist leicht daran zu erkennen, dass sich im Binärverzeichnis außer den ausführbaren Dateien wie *httpd* oder *htpasswd* noch das Skript *apxs* befindet. Auch für das Einrichten und Übersetzen von PHP selbst kommt das zur verwendeten Quell-Distribution gehörige configure-Skript zum Einsatz. Hier sollte der Administrator ebenfalls darauf achten, nur so wenige Erweiterungen wie unbedingt nötig einzubinden. Wer seinen eige-

Der Sicherheitsmechanismus "suExec" erlaubt, dass das PHP-CGI (oder andere SCG-Skripte) nicht mit der UID/GID des Webservers laufen, sondern nur mit einer extra angegebenen UID/GID

nen Firmen-Webserver einrichtet, weiß natürlich in der Regel genau, welche Erweiterungen er benötigt. Ein allgemeingültiges Beispiel könnte so aussehen:

```
./configure –with-
  mysql=/usr/local/mysql –with-
  apxs=/usr/local/apache/bin/apxs
  –with-gd –with-png-dir –with-free-
  type-dir –with-jpeg-dir  –with-dom
  –with-zlib –with-openssl –disable-
  cgi –enable-memory-limit
```

Die gewählten Parameter und Module sind als Vorschlag und Beispiel zu verstehen. Eine sehr gute Anleitung zur Installation von PHP5 als Apache-Modul oder CGI findet sich unter [2] im Internet. Entscheidend für die PHP-Installation als Apache-Modul ist der Parameter *--with-apxs*, der den vollständigen Pfad zum apxs-Skript enthalten muss. Das Skript stellt PHP quasi exakt auf die genutzte Apache-Version ein und konfiguriert selbstständig alle für die Installation von PHP als Apache-Modul erforderlichen weiteren Parameter. Mit *--disable-cgi* lässt sich das auch beim Übersetzen von "mod-php" voreingestellte Erzeugen eines CGI-Binaries von PHP von vorneherein unterbinden. Ist das configure-Skript ohne zu meckern durchgelaufen, lässt sich PHP mit *make; make install* wie gewohnt übersetzen, ebenso wie oben Apache. Dabei wird dank des apxs-Parameters das übersetzte PHP-Modul direkt in der Apache-Konfigurationsdatei aktiviert. Nach dem Neustart des Webservers sollte PHP dann als Apache-Modul aktiviert sein.

PHP als CGI

Ganz ähnlich verläuft das Konfigurieren und Übersetzen von PHP als CGI. Hier ist allerdings das oben erwähnte apxs-Skript nicht erforderlich. Ein CGI wird per Default automatisch erzeugt, sofern dies nicht mit dem oben erwähnten Parameter *--disable-cgi* unterbunden wird. Der Webserver muss auch nicht DSO-fähig sein. Ein sehr wichtiger sicherheitsrelevanter Konfigurationsparameter der CGI-Variante ist allerdings *--enable-force-cgi-redirect*, was die Möglichkeit eines direkten Aufrufs des PHP-Binary etwa über eine URL oder aus einem Skript heraus unterbindet, denn dabei würden zwangsläufig wichtige Server-abhängige PHP-Einstellungen wie der PHP Safe Mode umgangen. Ein typischer configure-Aufruf für die Übersetzung von PHP als CGI sieht daher in weiten Teilen nicht viel anders aus wie das Apache-Beispiel. Wer aus Sicherheitsgründen von der Standardkonfiguration abweichende Pfade für die beteiligten Komponenten bevorzugt, kann auch diese im Rahmen des configure-Aufrufs unterbringen:

```
/configure …
... –program-prefix= –
  prefix=/usr/local/php5 –
  datadir=/usr/share/php5 –
  mandir=/usr/share/man/php5
  –bindir=/usr/local/php5/bin –exec-
  prefix=/usr/local/php5 –include-
  dir=/usr/include/php5 –sysconf-
  dir=/etc/php5 –localstatedir=/var
  –with-config-file-path=/etc/hphp5
  –with-exec-dir=/usr/lib/php5/bin
```

Normalerweise sollte das PHP-Binary aber vom Installer im Verzeichnis "/usr/local/bin/php" abgelegt worden sein. Allerdings ist die Integration zwischen PHP und Apache bei der Installation von PHP als CGI nicht automatisch so weit fortgeschritten wie bei der Übersetzung als Apache-Modul. Da ein solches nicht beteiligt ist, ist es jetzt erforderlich, die komplette Apache-Konfiguration in *httpd.conf* manuell anzupassen. Dazu kopieren Sie am besten das fertige PHP-Binary aus "/usr/local/bin/php" in das gewünschte Zielverzeichnis, welches unbedingt außerhalb des Document-Root des Webservers liegen sollte, etwa "/home/www/cgi". Jetzt genügt es, in httpd-conf einen Alias auf dieses Verzeichnis einzurichten.

Abschließend müssen Sie nur noch die zugehörigen Dateitypen einrichten, damit PHP-Dateien richtig ausgeführt werden können. Dazu sind in der httpd.conf folgende Einträge zu ergänzen:

```
AddTyp application/x-httpd-php .php5
  .php
Action application/x-httpd-php
  /cgi-bin/php
```

Der wichtigste Vorteil einer Installation von PHP als CGI besteht darin, dass sich damit der Apache-Sicherheitsmechanismus "suExec" nutzen lässt. Hierbei handelt es sich um einen Wrapper, der CGI-Skripte unter einer anderen UID/GID als der des Webservers ausführt, mit der sehr praktischen und nützlichen Konsequenz, dass der Administrator für jeden virtuellen Host seines Webservers einen eigenen Nutzer und eine eigene Gruppe festlegen kann. Der Webserver kann dann durch Aufruf der Funktion *setuid()* vor der Skriptausführung in diese Gruppe beziehungsweise diesen Benutzer wechseln. Damit darf dann das CGI-Skript nur Dateien verändern, die diesem Benutzer ge-

Apache für suExec vorbereiten

Um Apache suExec-fähig zu machen, muss der Webserver mit folgenden Direktiven übersetzt werden:

`–enable-suexec`

aktiviert die suExec-Funktion. Daher muss diese Direktive vor allen Folgenden angegeben werden.

`–suexec-caller={username}`

gibt den Benutzernamen an, unter dessen UID das suExec-Binary aufgerufen wird. Hier ist daher der Benutzername anzugeben, unter dem der Webserver läuft, meist "httpd" oder "www-data".

`–suexec-docroot={path}`

ist die wichtigste Direktive von suExec, denn mit dieser zwingend erforderlichen Pfadangabe lässt sich das Basisverzeichnis angeben, unter dem die Funktion suExec arbeitet. In der Regel ist das der zu verwendende Document-Root, also "/home/www/srv" oder "/usr/local/apache/htdocs".

`–suexec-logfile={file}`

definiert den gewünschten Pfad zu den Log-Files von suExec. Per Default speichert suExec diese an gleicher Position wie Apache selbst.

```
–suexec-uidmin={uid}
–suexec-gidmin={gid}
```

geben an, welche UID beziehungsweise GID der suExec-Nutzer mindestens haben muss. Damit lässt sich wirkungsvoll verhindern, dass ein virtueller Host durch einen Konfigurationsfehler root-Rechte oder die eines anderen hoch privilegierten Nutzers erhält.

hören, was auf einem Schlag die meisten der im Verlauf des Beitrages noch erläuterten Sicherheitsprobleme von PHP löst. Bei der Variante als Apache-Modul läuft PHP stets unter der UID des Webservers.

Die Apache-Erweiterung *--enable-suexec* ist somit der wichtigste Parameter bei der Übersetzung von Apache und allein schon ein Grund, PHP als CGI zu übersetzen und auf die Vorteile der Übersetzung als Apache-Modul zu verzichten. suExec arbeitet außerdem vor dem Ausführen des CGI eine Reihe von zusätzlichen Sicherheitsüberprüfungen ab, was eine missbräuchliche Verwendung verhindern soll. So prüft es etwa, ob das auszuführende Programm (hier das eigentliche PHP-Binary) auch tatsächlich dem ausführenden Benutzer gehört, ob alle beteiligten Verzeichnisse lesbar sind oder dass das CGI nur über die unbedingt notwendigen Rechte verfügt. Leider gehört suExec nicht zur Default-Konfiguration von Apache, so dass Sie den Webserver mit einigen Direktiven für die Verwendung von suExec vorbereiten müssen. Welche das genau sind, zeigt der Kasten "Apache für suExec vorbereiten".

Nach der Installation findet sich im Binärverzeichnis des Webservers die Datei *suexec*, die ab jetzt für den Benutzerwechsel zuständig ist und bei der auf jeden Fall das Set-UID-Bit gesetzt sein sollte, was sich im Zweifel mit *chmod +s* leicht nachholen lässt. Jetzt bleibt nur noch, für jeden virtuellen Host einen Benutzer und eine Gruppe anzulegen, wozu seit Apache2 die Konfigurationsdirektive "SuexecUserGroup" dient. Die Direktive erwartet wahlweise einen Benutzernamen oder eine numerische UID, der dann ein "#" voranzustellen ist. Nach dem Eintragen der gewünschten Benutzer und Gruppen im jeweiligen VirtualHost-Block ist die Installation von suExec abgeschlossen, so dass sämtliche CGI-Anwendungen und darunter natürlich auch das PHP-CGI ab jetzt unter der in der Webserver-Konfiguration angegebenen UID laufen und nicht unter der des Webservers. Selbstverständlich muss dann aber für jeden virtuellen Host beziehungsweise Benutzer ein eigenes PHP-Binary zur Verfügung gestellt werden, denn suExec führt natürlich im Umkehrfall keine Dateien aus, die nicht dem zugehörigen Benutzer gehören.

Sicherheit mit Bordmitteln: Der PHP Safe Mode

Der Safe Mode gehört zu den bekanntesten Sicherungsmaßnahmen von PHP. Der Safe Mode lässt sich entweder im globalen Teil der *php.ini* oder in der VirtualHost-Konfiguration aktivieren und sorgt bei sämtlichen auszuführenden PHP-Skripten für eine automatische Zugehörigkeitsprüfung. Versucht nämlich das gerade ausgeführte PHP-Skript auf Dateien zuzugreifen, die einem anderen Benutzer gehören, unterbindet der Safe Mode sofort den Zugriff.

Wurde von einem Benutzer mit der UID 1001 und der Gruppe "www" ein PHP-Skript angelegt, das versucht, eine Textdatei zu öffnen (etwa */etc/shadow*), die root gehört (UID 0), überprüft PHP bei eingeschaltetem Safe Mode die UID und die

Weitere Sicherheitsrelevante PHP-Einstellungen

Neben den im Text erläuterten Sicherheitseinstellungen sind noch eine ganze Reihe weiterer PHP-Einstellungen sicherheitsrelevant. Eine nicht vollständige Auswahl finden Sie in diesem Kasten. Mit der Direktive

```
–memory_limit
```

können Sie wirkungsvoll verhindern, dass ein PHP-Skript den vollständigen vorhandenen Arbeitsspeicher belegt. Zwar lässt sich solch ein Memory-Limit bei *mod_php* sogar für jede VirtualHost-Sektion getrennt einrichten, aber leider auch durch einen Eintrag in der jeweiligen htaccess-Datei wieder aufheben. Wenn Sie ein festes, nicht änderbares Speicherlimit benötigen, können Sie auf den "Hardening-Patch" [3] zurückgreifen, der noch weitere Sicherheitsprobleme von PHP löst. Obwohl es sich bei memory_limit nicht direkt um einen Sicherheits-Parameter handelt, ist ein wirksamer Schutz gegen Speicherfresser trotzdem sicherheitsrelevant, weil ein per Speicherüberlauf lahmgelegter Webserver angreifbar ist. Außerdem können Sie mit

```
–disable_functions
```

sämtliche als gefährlich oder nicht erwünscht eingestufte Systemfunktionen global deaktivieren. Die gewünschten Funktionen lassen sich durch Kommata getrennt hinter der Direktive aufzählen, beispielsweise:

```
–disable_functions shell_exec
```

Leider lässt sich die Einstellung ausschließlich im globalen Teil der php.ini verwenden und der Kunde oder Benutzer kann die benötigten Funktionen auch nicht mehr nachträglich in seiner VirtualHost-Sektion anschalten. Da aber viele PHP-Funktionen ganz typische Verursacher von Sicherheitsproblemen sind, ist die Direktive trotzdem recht nützlich. Ganz ähnlich verhält sich die PHP-Einstellung

```
–disable_classes
```

mit der sich die Verwendung der angegebenen Klassen wirkungsvoll und schnell unterbinden lässt. Das kann sich insbesondere bei PHP 5.x als nützlich erweisen, da nach und nach immer mehr PHP-Erweiterungen eine objektorientierte Schnittstelle erhalten.

Gruppe des Skriptes (1001), vergleicht diese mit jeder durch das Skript zu öffnenden Datei und unterbindet den Zugriff bei Nichtübereinstimmung. Zum Aktivieren des Safe Mode genügt entweder der Schalter *safe_mode = On* oder *safe_mode = 1* im globalen Teil der php.ini oder das Einfügen von *php_admin_value safe_mode = On* oder *php_admin_value safe_mode = 1* in jeder oder der gewünschte VirtualHost-Sektion der php.ini, sofern virtuelle Hosts zum Einsatz kommen. Nach einem Neustart des Webservers ist der Safe Mode dann entweder für den entsprechenden virtuellen Host oder die gesamte Apache-Instanz (*php.ini*) aktiviert. Außerdem gibt es einige Direktiven, mit denen sich der Safe Mode noch sicherer gestalten lässt.

Mit *safe_mode_exec_dir* lässt sich etwa explizit festlegen, welche Dateien sich überhaupt durch die Funktionen *xec()* oder *passthru()* ausführen lassen. Das trifft dann nur für solche Dateien zu, die in den mit *safe_mode_exec_dir* angegebenen Pfaden liegen. Mit der Konfigurationsdirektive *safe_mode_include_dir*, die sich ebenfalls in den jeweiligen VirtualHost-Sektionen der php.ini einsetzen lässt, kann der Zugriff durch die Funktionen *include()* oder *require()* auf die angegebenen Dateien und Pfade beschränkt werden. Getrennt durch einen Doppelpunkt lassen sich leicht mehrere Pfade angeben:

```
safe_mode_include_dir=/usr/local/lib/
php:/usr/local/lib/PEAR
```

Der Safe Mode schützt außerdem wichtige Umgebungsvariablen vor Veränderung von außen. Obwohl der Safe Mode sehr populär ist und von vielen Befürwortern als wichtigste Sicherung von PHP gegen Angriffe von außerhalb angesehen wird, hat er auch prominente Gegner, darunter einige Entwickler des PHP-Teams, die dem Safe Mode konzeptionelle Fehler und Implementierungslücken ankreiden. Als Konsequenz soll es den Safe Mode in PHP6 nicht mehr geben.

Safe Mode reloaded: open_basedir

Die Konfigurationsdirektive *open_basedir* stellt für viele PHP-Profis und Kritiker des Safe Mode einen wesentlich wirksameren Schutz dar, wenngleich sich auch diese Maßnahme mit ausreichend krimineller Motivation aushebeln lässt. So dürfen etwa PHP-Skripte mit open_basedir nur Dateien lesen und schreiben, die in offenen Basisverzeichnissen liegen; alle anderen Verzeichnisse sind verboten. Damit ist open_basedir eine Art chroot für PHP, das allerdings nicht auf Betriebssystemebene implementiert und somit weniger wirksam ist als ein echtes chroot. In vielen Fällen ist open_basedir aber ein wirksamer Schutz und bringt im Gegensatz zum Safe Mode keine Einschränkungen in der Funktionalität mit sich. Diese Direktive lässt sich ebenfalls in der php.ini oder im jeweiligen VirtualHost-Block einschalten:

```
open_basedir =
  /usr/local/lib/php:/home/www/
  kunde001
```

Beim Einsatz von open_basedir ist darauf zu achten, dass der Zugriff auf die PEAR-Bibliotheken nicht ausgeschlossen wird. PEAR (PHP Extension and Application Repository) ist eine wichtige Bibliothek für Module und Erweiterungen für PHP. Die PEAR-Bibliothek stellt Skripte und Referenzimplementierungen zur Verfügung. PEAR ist für PHP vergleichbar wichtig wie die Standardbibliotheken "Standard C Library" für C oder CPAN für Perl. Es ist also empfehlenswert, neben dem Pfad zum Wurzelverzeichnis des jeweiligen virtuellen Hosts auch den Pfad zu PEAR zu den mit open_basedir freigegebenen Verzeichnissen hinzuzufügen.

Fazit

Auf schlecht programmierte und sicherheitskritische PHP-Anwendungen kann der Administrator eines PHP-/Webservers naturgemäß wenig Einfluss nehmen. Er kann aber seinen Server wirkungsvoll vor durchlässigen PHP-Skripten und Angriffen aller Art von außen und innen schützen. Mit der Übersetzung von PHP als CGI, der Verwendung von Apache "suExec" und der PHP Konfigurationsdirektive "open_basedir" lässt sich jeder Webserver nahezu wasserdicht absichern. *(ln)*

Links und Ressourcen

[1] **PHP-Sicherheit:**
"PHP/MySQL-Webanwendungen sicher programmieren"
von Christopher Kunz und Stefan Esser, 351 Seiten, ISBN-10: 3898645355

[2] **Installationsanleitung für PHP 5**
www.serversupportforum.de/forum/faqs-anleitungen/2097-howto-install-php5.html

[3] **Hardened-PHP Project**
www.hardened-php.net

Openfiler und DRBD-Cluster für Hochverfügbarkeit in SAN-Infrastrukturen (2)

Gesunder Herzschlag

von Thomas Gronenwald

Im ersten Teil unseres Workshops setzten wir die Grundpfeiler unseres hochverfügbaren SAN, indem wir DRBD, Heartbeat und Openfiler installierten. Anschließend erfolgten die ersten Schritte zur Konfiguration des Systems. Diese führen wir im zweiten Teil der Serie fort und verbinden die Systeme mit dem Storage.

Zunächst müssen wir die Konfiguration der Clusterdienste auf den beiden Filern abschließen.

Initialisieren von DRBD0 und DRBD1

Um die Metadaten zu initialisieren, müssen Sie nun einige drbd-Konfigurationsbefehle auf den Systemen ausführen. Im Vorfeld muss das Filesystem noch bearbeitet werden.

Sollten Sie in der manuellen Partitionierung andere Partitionen angelegt haben, müssen Sie darauf achten, dass diese auch die richtigen Partitionen sind. Ansonsten droht an dieser Stelle Datenverlust! Zunächst Filer01:

```
root@filer01 ~# dd if=/dev/zero
  of=/dev/sda3
```

Dann wenden wir uns Filer02.prod.zz zu:

```
root@filer02 ~# dd if=/dev/zero
  of=/dev/sda3
```

Zurück zu Filer01.prod.zz:

```
root@filer01 ~# drbdadm create-md
  cluster_metadata
root@filer01 ~# drbdadm create-md
  vg0drbd
```

Und abschließend noch einmal Filer02.prod.zz:

```
root@filer02 ~# drbdadm create-md
  cluster_metadata
root@filer02 ~# drbdadm create-md
  vg0drbd
```

Waren diese Schritte erfolgreich, können wir nun die standardmäßig bereits als "mounted" markierte Partition "sda3" als "unmounted" kennzeichnen. Auf Filer01.prod.zz mit

```
root@filer01 ~# umount /dev/sda3
```

Der entsprechende Befehl für Filer02:

```
root@filer02 ~# umount /dev/sda3
```

Jetzt starten Sie den DRBD-Dienst auf beiden Systemen. Auf Filer01.prod.zz mit:

```
root@filer01 ~# service drbd start
```

Und auf Filer02.prod.zz nutzen Sie:

```
root@filer02 ~# service drbd start
```

Um nun den aktuellen Status und die Funktionalität zu prüfen, lässt sich mit den folgenden Befehlen der Status des DRBD einsehen:
- Filer01: *root@filer1 /# service drbd status*
- Filer02: *root@filer2 /# service drbd status*

Primären Knoten wählen

Nun muss einer unserer Server die initiale Rolle des primären Knotens einnehmen. Wir wählen dafür den Filer01 aus. Mit folgendem Befehl erhält dieser den Status "primary" für drbd0 und drbd1:

```
root@filer01 ~# drbdsetup /dev/drbd0
  primary -o
root@filer01 ~# drbdsetup /dev/drbd1
  primary -o
```

Der Status zeigt nun, dass der Abgleich der Daten gestartet wurde und unser Filer01 als primärer Knoten konfiguriert ist. Um den Status der Replikation zu erfahren, erhalten Sie über diesen Befehl einen dynamischen Fortschrittbalken:

```
root@filer1 ~# watch cat /proc/drbd
```

Sollten Sie für die Datenpartition (LVM) eine größere Partition gewählt haben, kann die Replikation entsprechend länger dauern.

Bootoptionen von DRBD

Nun wollen wir natürlich, dass DRBD bei einem unerwarteten Systemabsturz oder Neustart automatisch startet. Dazu muss mittels *chkconfig* der drbd-Service als Systemdienst hinzugefügt werden. Für Filer01.prod.zz mit

```
root@filer01 ~# chkconfig –level
  2345 drbd on
```

Und, wie bereits gewohnt, für Filer02 entsprechend:

```
root@filer02 ~# chkconfig –level
  2345 drbd on
```

Erstellen des Dateisystems

Um unsere Cluster-Konfigurationen und -Dienste später für beide Systeme verfügbar zu machen, muss nun noch das Dateisystem für drbd0 erstellt werden. Auf unserem Filer01.prod.zz nutzen wir dafür das Kommando:

```
root@filer01 ~# mkfs.ext3 /dev/drbd0
```

Diese Partition müssen Sie nicht in die "/etc/fstab" einbinden. Das ist im weiteren Verlauf Aufgabe des Heartbeats. Um später unsere LUNs (Logical Unit Number, virtuelle Festplatte) auf dem Openfiler ablegen zu können, müssen wir nun "/dev/drbd1" als eigenständiges Volume für unsere "Volume Groups" anlegen. Dies erledigen Sie auf dem Filer01 über:

```
root@filer01 ~# vim
  /etc/lvm/lvm.conf
```

Den Inhalt der *lvm.conf* ändern Sie nun wie folgt:

```
filter = [ "r|/dev/sda5|" ]
```

Diese Einstellung müssen Sie auf beiden Systemen vornehmen. Der Einfachheit halber kopieren Sie die editierte Datei mittels SCP auf den Filer02:

```
root@filer01 ~# scp
  /etc/lvm/lvm.conf
  root@filer02.prod.zz:/etc/
  lvm/lvm.conf
```

Nun erstellen Sie das eigentliche Volume. Wichtig hierbei ist, dass dies nur auf unserem Filer01 erfolgt – drbd übernimmt diese Aufgabe auf unserem Filer02 und repliziert diese:

```
root@filer1 /# pvcreate /dev/drbd1
```

Konfiguration von Heartbeat

Wie bereits beschrieben, überwacht Heartbeat die Verfügbarkeit der Knoten und übernimmt zusätzlich das An-, Ab- und Umschalten der Dienste auf den jeweiligen Knoten. Mittels eines Prüfungsintervalls, dem sogenannten "Heartbeat-Pulse", überprüft es dann die Verfügbarkeit der beiden Knoten. Um den "Herzschlag" zu konfigurieren, müssen Sie die Dateien */etc/ha.d/ha.cf* und */etc/ha.d/authkeys* erstellen, die auf beiden Systemen identisch sein müssen. Für Filer01 gehen Sie wie folgt vor:

```
root@filer01 ~# vim /etc/ha.d/
  authkeys
```

Die Datei sollte dann so aussehen:

```
auth 2
2 crc
```

Auf Filer01.prod.zz folgt nun:

```
root@filer01 ~# scp /etc/ha.d/
  authkeys
  root@filer02.prod.zz:/etc/ha.d/
  authkeys
```

Anschließend beschränken wir den Zugriff auf diese Datei noch auf unseren "root User". Zunächst auf Filer01 über:

```
root@filer01 ~# chmod 600
  /etc/ha.d/authkeys
```

Und erneut analog auf Filer02:

```
root@filer02 ~# chmod 600
  /etc/ha.d/authkeys
```

Jetzt erstellen wir die zweite Datei, die */etc/ha.d/ha.cf*. Diese enthält unsere HA-Informationen und muss auf beiden Systemen identisch sein (auf Filer01):

```
root@filer01 ~# vim /etc/ha.d/ha.cf
```

Die Datei sollte dann so aussehen wie in Listing 1. Die Datei kopieren Sie nun auch wieder auf den zweiten Knoten:

```
root@filer01 ~# scp /etc/ha.d/ha.cf
  root@Filer02.prod.zz:/etc/ha.d/
  ha.cf
```

Nachdem Sie die benötigten Heartbeat-Parameter eingestellt haben, konfigurieren Sie Heartbeat nun noch als Systemdienst, damit dieser bei jedem Systemstart automatisch startet. Der Befehl

```
root@filer01 ~# chkconfig –level
  2345 heartbeat on
```

erledigt dies auf Filer01 und Filer02:

```
root@filer02 ~# chkconfig –level
  2345 heartbeat on
```

Verschieben der benötigten Cluster-Dienste

Damit die benötigten Dienste später bei einem Failover für den Zugriff beider Systeme verfügbar sind, müssen Sie diese in das Verzeichnis"/cluster_metadata" verschieben. Anschließend werden diese Dienste wieder mit einer symbolischen Verknüpfung neu verlinkt. Auf Filer01 gehen Sie dazu wie folgt vor:

```
root@filer01 ~# mkdir
  /cluster_metadata
root@filer01 ~# mount /dev/drbd0
  /cluster_metadata
root@filer01 ~# mv /opt/openfiler/
  /opt/openfiler.local
root@filer01 ~# mkdir
  /cluster_metadata/opt
root@filer01 ~# cp -a /opt/
  openfiler.local /cluster_
  metadata/opt/openfiler
root@filer01 ~# ln -s
  /cluster_metadata/opt/openfiler
  /opt/openfiler
root@filer01 ~# rm
  /cluster_metadata/opt/openfiler
  /sbin/openfiler
root@filer01 ~# ln -s
  /usr/sbin/httpd
  /cluster_metadata/opt/openfiler
  /sbin/openfiler
root@filer01 ~# rm
  /cluster_metadata/opt/openfiler
  /etc/rsync.xml
root@filer01 ~# ln -s /opt
  /openfiler.local/etc/rsync.xml
  /cluster_metadata/opt/openfiler
```

```
  /etc/
root@filer01 ~# mkdir -p
  /cluster_metadata/etc/httpd/conf.d
```

Damit die Synchronisierung zwischen beiden Knoten funktioniert, müssen die Parameter innerhalb der *rsync.xml* editiert beziehungsweise hinzugefügt werden. Zunächst wieder für Filer01.prod.zz:

```
root@filer01 ~# vim
  /opt/openfiler.local/etc/rsync.xml
```

Die Datei sollte dann so aussehen:

```
<?xml version="1.0" ?>
<rsync>
<remote hostname="10.10.1.2"/>
<item path="/etc/ha.d/haresources"/>
<item path="/etc/ha.d/ha.cf"/>
<item path="/etc/ldap.conf"/>
<item
  path="/etc/openldap/ldap.conf"/>
<item path="/etc/ldap.secret"/>
<item path="/etc/nsswitch.conf"/>
<item path="/etc/krb5.conf"/>
</rsync>
```

Nun wenden Sie sich Filer02.prod.zz zu:

```
root@filer02 ~# mkdir
  /cluster_metadata
root@filer02 ~# mv /opt/openfiler/
  /opt/openfiler.local
root@filer02 ~# ln -s
  /cluster_metadata/opt/openfiler
  /opt/Openfiler
```

Ist dies erledigt, bleiben Sie auf Filer02:

```
root@filer02 ~# vim
  /opt/openfiler.local/etc/rsync.xml
```

Die Datei sollte dann so aussehen:

```
<?xml version="1.0" ?>
<rsync>
<remote hostname="10.10.1.1"/>
<item path="/etc/ha.d/haresources"/>
<item path="/etc/ha.d/ha.cf"/>
<item path="/etc/ldap.conf"/>
<item path="/etc/openldap/
  ldap.conf"/>
<item path="/etc/ldap.secret"/>
<item path="/etc/nsswitch.conf"/>
<item path="/etc/krb5.conf"/>
</rsync>
```

Alternativ können Sie an dieser Stelle auch SCP nutzen. Wichtig dabei ist nur, den "remote hostname" zu ändern.

Konfiguration des Cluster-Heartbeats

Nun editieren Sie die */cluster_metadata/opt/openfiler/etc/cluster.xml* und vergeben hier auch die virtuelle IP-Adresse für den Cluster. Zudem übernimmt diese Konfigurationsdatei das eigenständige "mounten" von LVM und drbd0. Außerdem generiert die *cluster.xml* aus den gesetzten Konfigurationen dann die Ressourcen ("/etc/ha.d/haresources"). Die Datei brauchen wir nur einmal auf unserem Filer01 editieren. Die Datei sollte dann Listing 2 entsprechen.

Bereitstellen der benötigten Cluster-Dienste

Um die einzelnen Pakete wie Samba, NFS oder das später von uns benötigte iSCSI-Target über drbd (cluster_metadata) bereitzustellen, müssen diese in den richtigen Pfad verschoben und neu verlinkt werden. Den Samba-Support richten Sie auf Filer01 mit diesen Befehlen ein:

```
root@filer01 ~# mkdir
  /cluster_metadata/etc
root@filer01 ~# mv /etc/samba/
  /cluster_metadata/etc/
root@filer01 ~# ln -s
  /cluster_metadata/etc/samba/
  /etc/samba
root@filer01 ~# mkdir -p
  /cluster_metadata/var/spool
root@filer01 ~# mv /var/spool/samba/
  /cluster_metadata/var/spool/
root@filer01 ~# ln -s
  /cluster_metadata/var/spool/samba/
  /var/spool/samba
```

Es folgt der NFS-Support:

```
root@filer01 ~# mkdir -p
  /cluster_metadata/var/lib
root@filer01 ~# mv /var/lib/nfs/
  /cluster_metadata/var/lib/
root@filer01 ~# ln -s /cluster_
  metadata/var/lib/nfs/ /var/lib/nfs
root@filer01 ~# mv /etc/exports
  /cluster_metadata/etc/
root@filer01 ~# ln -s /cluster_
  metadata/etc/exports /etc/exports
```

Auf Filer02.prod.zz müssen Sie an dieser Stelle, da wir bereits unsere Dienste auf Filer01 verschoben haben, nur noch die alten Verzeichnisse löschen und neu verlinken. Für den Samba-Support gehen Sie wie folgt vor:

```
root@filer02 ~# rm -rf /etc/samba/
root@filer02 ~# ln -s
  /cluster_metadata/etc/samba/
  /etc/samba
root@filer02 ~# rm -rf
  /var/spool/samba/
root@filer02 ~# ln -s
  /cluster_metadata/var/spool/samba/
  /var/spool/samba
```

Und den NFS-Support richten Sie über

```
debugfile /var/log/ha-debug
logfile /var/log/ha-log
logfacility local0
bcast eth1
keepalive 5
warntime 10
deadtime 120
initdead 120
udpport 694
auto_failback off
node filer01.prod.zz
node filer02.prod.zz
```

Listing 1: HA-Konfigurationsdatei

```
<?xml version="1.0" ?>
<cluster>
<clustering state="on" />
<nodename value="filer01.prod.zz" />
<resource value="MailTo::uhd@prod.zz::ClusterFailover"/>
<resource value="IPaddr::192.168.1.3/24" />
<resource value="drbddisk::">
<resource value="LVM::vg0drbd">
<resource value="Filesystem::/dev/drbd0::/cluster_metada-
   ta::ext3::defaults,noatime">
<resource value="MakeMounts"/>
</cluster>
```

Listing 2: Konfigurationsdatei *cluster.xml*

```
root@filer02 ~# rm -rf /var/lib/nfs/
root@filer02 ~# ln -s
  /cluster_metadata/var/lib/nfs/
  /var/lib/nfs
root@filer02 ~# rm -rf /etc/exports
root@filer02 ~# ln -s
  /cluster_metadata/etc/exports
  /etc/exports
```

ein. Nun wenden wir uns der Unterstützung des iSCSI-Targets auf Filer01 zu:

```
root@filer01 ~# mv /etc/ietd.conf
  /cluster_metadata/etc/
root@filer01 ~# ln -s
  /cluster_metadata/etc/ietd.conf
  /etc/ietd.conf
root@filer01 ~# mv
  /etc/initiators.allow
  /cluster_metadata/etc/
root@filer01 ~# ln -s
  /cluster_metadata/etc/initiators.
  allow/etc/initiators.allow
root@filer01 ~# mv
  /etc/initiators.deny
  /cluster_metadata/etc/
root@filer01 ~# ln -s
  /cluster_metadata/etc
  /initiators.deny
  /etc/initiators.deny
```

Und auch auf Filer02 benötigen wir iSCSI:

```
root@filer02 ~# rm /etc/ietd.conf
root@filer02 ~# ln -s
  /cluster_metadata/etc/ietd.conf
  /etc/ietd.conf
root@filer02 ~# rm
  /etc/initiators.allow
root@filer02 ~# ln -s
  /cluster_metadata/etc/
  initiators.allow
  /etc/initiators.allow
root@filer02 ~# rm
  /etc/initiators.deny
root@filer02 ~# ln -s
  /cluster_metadata/etc/
  initiators.deny
  /etc/initiators.deny
```

Abschließend richten Sie den FTP-Support ein. Zunächst auf Filer01.prod.zz:

```
root@filer01 ~# mv /etc/proftpd
  /cluster_metadata/etc/
root@filer01 ~# ln -s
  /cluster_metadata/etc/proftpd/
  /etc/proftpd
```

Und schließen nun die Konfiguration auf Filer02 ab:

```
root@filer02 ~# rm -rf /etc/proftpd
root@filer02 ~# ln -s
  /cluster_metadata/etc/proftpd/
  /etc/proftpd
```

Anlegen der ersten Volume Group

Eine "Volume Group" in Openfiler bezeichnet eine Gruppe von einzelnen Volumes. Diese muss stets vorhanden sein, bevor ein Volume hinzugefügt werden kann. Dazu erstellen Sie auf Filer01 eine neue "Volume Group" mit dem Namen "vg0drbd".

```
root@filer1 etc# vgcreate vg0drbd
  /dev/drbd1
```

Im nächsten Schritt muss noch das "httpd-Module" neu verlinkt werden (noch immer auf Filer01):

```
root@filer01 ~# rm
  /opt/openfiler/etc/httpd/modules
root@filer01 ~# ln -s
  /usr/lib32/httpd/modules
  /opt/openfiler/etc/httpd/modules
```

Sollten Sie eine x64-Architektur nutzen, ersetzen Sie "/usr/lib32" durch "/usr/lib64". Starten Sie nun Filer01 neu:

```
root@filer01 ~# service openfiler
  restart
```

Bevor wir anschließend den eigentlichen Heartbeat-Dienst starten können, müssen wir zunächst noch ein "logical volume" erstellen. Wir wählen dafür eine Größe von 2.048 MByte mit dem Namen "Xen01" in unserer Volume Group "vg0drbd" (Filer01):

```
root@filer01 ~# lvcreate -L 2048M -n
  Xen01 vg0drbd
```

Um jetzt das Anlegen der "haresources" zu initiieren, reicht es aus, über das Webinterface unseres primären Knotens (*https://192.168.1.1:446*) den iSCSI-Dienst zu starten. Diesen finden Sie unter dem Menüpunkt "Services". Nun wird die Datei unter "/etc/ha.d/haresources" geschrieben. Diese muss dann wieder mittels SCP auf den zweiten Knoten kopiert werden.

```
root@filer01 ~# scp /etc/ha.d/
  haresources
  root@filer02.prod.zz:/etc/ha.d/
  haresources
```

Wenn bis hierher alles funktioniert hat, können Sie jetzt zuerst den Filer01 und anschließend den Filer02 neu starten. Im Anschluss sollte unser primärer Knoten unter der HA-IP-Adresse (virtuelle IP) erreichbar sein (*https://192.168.1.3:446*).

Vorbereitung iSCSI-Target und LUN für XenServer

Um nun eine LUN (Logical Unit Number) für unser SAN anzulegen, müssen im Vorfeld drei generelle Schritte durchgeführt werden:

- das Hinzufügen eines iSCSI-Targets
- das LUN Mapping
- Zugriff auf iSCSI-Target erlauben

Bild 1: Die Bestätigung nach dem erfolgreichen LUN Mapping

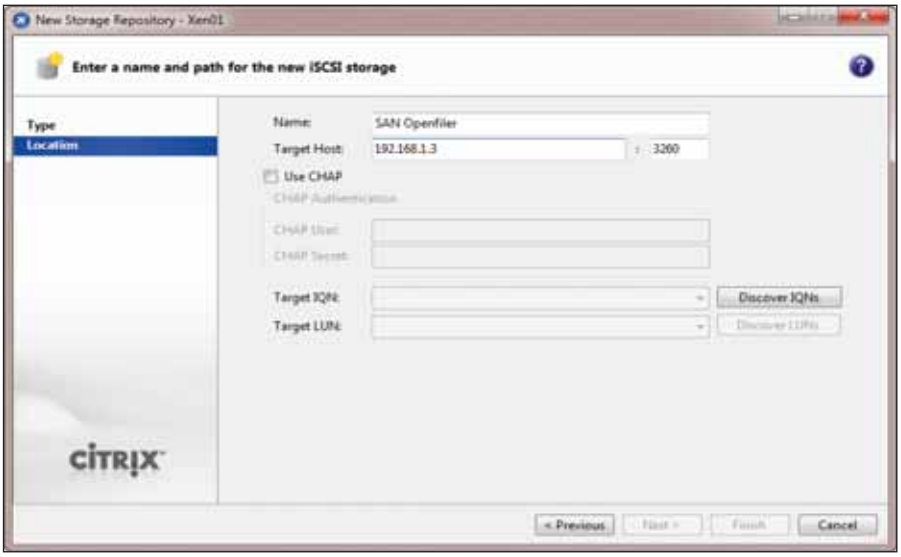


Bild 2: Das Storage Repository benötigt noch IQN und LUN

Bevor wir unser iSCSI-Target anlegen, überprüfen wir unsere erstellte "Volume Group" und das angelegte Volume. Dies lässt sich unter dem Menüpunkt "Volumes" einsehen.

Um nun ein iSCSI-Target hinzuzufügen, wechseln wir in das Menü unter "Volumes / iSCSI Target". Dort können wir jetzt über die Schaltfläche "add" ein neues "target" hinzufügen. Im zweiten Schritt muss nun die erstellte LUN unserem Volume zugewiesen werden. Dies geschieht unter dem Menüpunkt "Volumes / iSCSI Target / LUN Mapping". Mit der Schaltfläche "map" fügen wir die LUN unserer "Volume Group" hinzu. Zu guter Letzt muss nur unser XenServer [1,2] auf die LUN berechtigt werden. Dies konfigurieren wir unter dem Eintrag "Volumes / iSCSI Target / Network ACL".

Erstellen des Storage Repository auf dem XenServer

Für unseren Xen-Server-Pool erstellen wir jetzt im Xen-Center ein neues "Storage Repository". Als Typ wählen Sie "iSCSI" aus, geben die IP-Adresse des Clusters ein und nutzen die Schaltfläche "Discover IQNs" zur Auswahl des angelegten Targets. Nun nutzen Sie die Schaltfläche "Discover LUNs" und wählen Ihre LUN aus. Jetzt muss nur noch die LUN formatiert werden und schon können im Anschluss VMs auf unserem SAN abgelegt werden. Nun kann das Storage Repository zum Speichern von virtuellen Maschinen genutzt werden. Zudem stehen uns auch die kostenlosen Funktionen wie "XenMotion" zur Verfügung.

Fazit

Wie dieser Workshop zeigt, ist es alles andere als ein Hexenwerk, einen Hochverfügbarkeits-Cluster unter Linux zu realisieren. Dank der Open Source-Projekte Openfiler, DRBD und Heartbeat lässt sich so mit einfachen Mitteln eine Hochverfügbarkeits-Storage-Infrastruktur realisieren. In Verbindung mit dem kostenlosen Hypervisor XenServer 5.5 lässt sich so eine leistungsstarke und dennoch kostengünstige Infrastruktur aufbauen. *(jp)*

Thomas Gronenwald ist Security Consultant bei der adMERITia GmbH in Langenfeld und Autor auf blog.port389.de

Links

[1] Produktseite XenServer
www.citrix.de/produkte/schnellsuche/xenserver/

[2] Download Citrix XenCenter
www.citrix.com/lang/English/lp/lp_1688615.asp

Lizenzierung von Microsoft-Produkten (2)

Wer die Wahl hat...

Ganz so groß wie hier ist die Auswahl bei den Lizenzen zwar nicht, dennoch ist eine gut überlegte Entscheidung zu treffen

von Thomas Joos

Neben der Lizenzierung der Microsoft-Produkte als solche, muss der IT-Verantwortliche auch Entscheidungen hinsichtlich der Bindung der Zugriffslizenzen an PCs oder Anwender treffen. Eine Entscheidung, die sich massiv auf die Lizenzkosten auswirkt. Wir betrachten in diesem Beispiel eine Reihe unterschiedlicher Lizenz-Szenarien und beleuchten zum Abschluss dieser Serie die Lizenzierung des neuen Windows Server 2008 R2.

Microsoft bietet für viele Produkte, zum Beispiel Small Business Server und auch Essential Business Server 2008, aber auch für die Terminaldienste, die beiden Lizenzvarianten für Geräte (Device-CALs) und Benutzer an (User-CALs). Die beiden Lizenzen unterscheiden sich preislich nicht voneinander. Sie müssen bereits bei der Bestellung Ihrer Lizenzen im Voraus planen, welchen Lizenztyp Sie einsetzen wollen. Sie können auch die verschiedenen Lizenzen miteinander mischen, je nach optimaler Lizenzierung.

Geräte-Lizenzen versus Benutzer-Lizenzen

Es ist jedoch nicht erlaubt, die einzeln erhältlichen Lizenzpacks in Geräte- und Benutzer-Lizenzen aufzusplitten. Sie dürfen also ein 5er-Pack Geräte-Lizenzen und ein 5er-Pack Benutzerlizenzen kaufen und lizenzieren. Es ist aber nicht erlaubt, dass Sie diese Pakete aufsplitten und zum Beispiel als 2er-Geräte-Lizenz und 8er-Benutzerlizenz verwenden. Wenn Sie mit Geräte-CALs lizenzieren, müssen Sie für jeden PC, der auf diesen Server zugreift, eine Lizenz kaufen – unabhängig davon, wie viele Benutzer an diesem PC arbeiten. Betreiben Sie PCs zum Beispiel im Schichtbetrieb, an denen zu unterschiedlichen Zeiten unterschiedliche Benutzer arbeiten, benötigen Sie für diese PCs nur jeweils eine Geräte-CAL. Im umgekehrten Fall, wenn also ein Benutzer mit mehreren PCs, Notebooks oder Smartphones auf den Server zugreift, benötigen Sie für diesen Benutzer mehrere Geräte-CALs, da dieser Benutzer mit mehreren PCs auf den Server zugreift. Alternativ können Sie auch eine Benutzer-CAL kaufen. Jeder Benutzer mit einer Benutzer-CAL kann an beliebig vielen PCs eine Verbindung mit einem Server aufbauen.

Die CALs müssen eindeutig zugewiesen werden. Sie können daher nicht nur so viele CALs kaufen, wie gleichzeitig Benutzer arbeiten, sondern müssen die Gesamtzahl Ihrer Arbeitsstationen, Pocket-PCs und sonstiger Geräte lizenzieren, wenn Sie Geräte-Lizenzen kaufen. Bei Benutzer-Lizenzen müssen diese genau der Anzahl der Benutzer zugewiesen werden, die insgesamt mit dem Server arbeiten.

Szenario: Lizenzen bei weniger PCs als Mitarbeiter

In Ihrem Unternehmen sind beispielsweise 100 Mitarbeiter beschäftigt, von denen jedoch lediglich 63 mit PCs am Server arbeiten. Da etwa im Lieferumfang von Small Business Server 2008 bereits Lizenzen enthalten sind, benötigen Sie noch 58 Lizenzen für die PCs, wenn fünf Lizenzen enthalten sind.

Kaufen Sie Geräte-CALs, wird jede gekaufte Lizenz einem bestimmten PC zugeordnet. Mit diesen PCs können sich jetzt beliebig viele Mitarbeiter mit dem Server verbinden, wenn sich diese zum Beispiel PCs im Schichtbetrieb teilen. Wenn neue PCs hinzukommen, müssen Sie für diese PCs weitere Geräte-Lizenzen kaufen.

Szenario: Lizenzen bei mehr PCs als Mitarbeiter

Im nächsten Beispiel gehen wir von einer IT-Firma aus, in der 40 Mitarbeiter beschäftigt sind. Von diesen 40 Mitarbeitern arbeiten 25 mit der Windows-Domäne und dem Small Business Server 2008. Jeder dieser Mitarbeiter hat einen PC und ein Notebook, mit denen er am Small Business Server 2008 arbeitet, um Dateien auszutauschen oder auf sein Postfach zurückzugreifen.

Obwohl in diesem Unternehmen nur 40 Mitarbeiter beschäftigt sind, verbinden sich 50 PCs mit dem Small Business Server 2008. Es müssen in diesem Beispiel daher 50 Geräte-Lizenzen erworben werden. Wenn das Unternehmen seine Lizenzen jedoch als Benutzer-Lizenz erwirbt, werden lediglich 25 Lizenzen be-

nötigt, da nur 25 Benutzer mit dem Small Business Server 2008 arbeiten.

Szenario: Anbindung von Firmen-PCs und Heimarbeitsplätzen

In einem Unternehmen gibt es 45 PCs. Von diesen 45 PCs werden 30 PCs im Schichtbetrieb von jeweils 2 Mitarbeitern geteilt. Zusätzlich gibt es 15 Mitarbeiter, die berechtigt sind, sich zu Hause ins Netzwerk einzuwählen und auf den Small Business Server 2008 zuzugreifen, um E-Mails abzurufen oder Dateien zu öffnen. Diese Mitarbeiter können auch mit Smartphones über das Internet auf den Exchange Server im Small Business Server 2008 zugreifen. Diese 15 Mitarbeiter arbeiten jeweils an einem der 45 PCs des Unternehmens. Da zum Lieferumfang bereits fünf Lizenzen dazugehören, sollten diese bei der Lizenzierung berücksichtigt werden. Die beste Lizenzierung in diesem Beispiel sieht folgendermaßen aus:

1. Das Unternehmen deklariert die enthaltenen fünf Lizenzen des Small Business Server 2008 als Benutzer-Lizenzen für fünf der Heimarbeitsplatz-Benutzer.
2. Zusätzlich werden weitere 10 Benutzerlizenzen erworben und den Heimarbeitsplätzen zugewiesen. Mit diesen Lizenzen dürfen jetzt diese Heimarbeitsplatz-Benutzer sowohl von zu Hause mit Ihrem PC als auch mit dem Smartphone und dem PC am Arbeitsplatz auf den Small Business Server 2008 zugreifen.
3. Für die restlichen 30 PCs werden Geräte-Lizenzen erworben, die es einer beliebigen Anzahl Benutzern erlaubt von den 30 fest definierten PCs auf den Small Business Server 2008 zuzugreifen.

In diesem Beispiel ist also ein Mischbetrieb der Lizenzierung sinnvoll.

Lizenzierung von Terminalservern

Wenn Sie einen Terminalserver integrieren, müssen Sie für diesen Server eine normale Windows Server 2003/2008-Lizenz kaufen. Diese Lizenz berechtigt auch zur Installation eines Terminal-Servers und eines Terminal-Lizenz-Servers, der die Benutzerzugriffe und -Lizenzen verwaltet. Zusätzlich benötigen Sie für jeden Benutzer, der mit dem Terminalserver arbeitet, eine Terminalserver-Lizenz (TS-CAL). Seit dem Erscheinen von Windows Server 2008 R2 heißen TS-CALs jetzt RDS-CALs, da die Terminaldienste in Remotedesktopdienste umbenannt wurden. Sie benötigen für einen Terminalserver (Remotedesktopserver) außerdem zusätzliche Benutzer-CALs für den Benutzerzugriff, nicht nur TS- (RDS-)CALs [1].

Diese Lizenz wird pro PC oder pro Benutzer vergeben, die mit dem Server ständig arbeiten und gilt also nicht pro Zugriff. Das heißt, Sie müssen nicht so viele Lizenzen kaufen, wie gleichzeitig Benutzer mit dem Terminalserver arbeiten, sondern so viele Lizenzen, wie Benutzer überhaupt mit dem Terminalserver innerhalb eines Zeitraums arbeiten. Wenn Sie nicht genügend Lizenzen einspielen, können Benutzer nur begrenzte Zeit mit einem Terminalserver arbeiten. Wenn Sie einen Windows Server 2003/2008-Terminalserver einsetzen, sind keine Lizenzen für Windows integriert. Diese müssen wie bei den anderen Betriebssystemen auch erworben werden, bei Windows 2000 Server war das noch anders, dies wurde jedoch mit Windows Server 2003 geändert.

Microsoft bietet für die Lizenzierung der TS-CALs die gleichen Lizenzierungsmöglichkeiten wie bei den normalen Server-CALs. Es gibt TS-Geräte-CALs und TS-Benutzer-CALs mit den bereits beschriebenen Möglichkeiten. Daneben gibt es eine External Connector Lizenz für TS-CALs. Mit ihr dürfen sich alle Geschäftspartner oder Lieferanten mit einem Terminalserver verbinden und benötigen keine zusätzlichen TS-CALs. Dies gilt aber nur für außen Stehende, nicht für Mitarbeiter des Unternehmens. Wenn Sie zusätzlich auf einem Terminalserver Citrix einsetzen, benötigen Sie darüber hinaus eine Citrix Presentation Server-Produktlizenz sowie Verbindungslizenzen für Citrix. Die Verbindungslizenzen bei Citrix sind meistens pro Zugriff. Sie benötigen also nur so viele Lizenzen, wie sich Benutzer gleichzeitig mit dem Server verbinden. Melden sich die Benutzer vom Terminalserver ab, wird die Lizenz wieder freigegeben.

Das ist bei den Microsoft-Lizenzen nicht so. Diese Lizenzen bleiben auf dem Benutzer-PC erhalten, auch wenn sich der Benutzer vom Server abgemeldet hat. Auch wenn Ihre Benutzer ausschließlich mit dem Citrix-Client per ICA auf den Terminalserver zugreifen, werden für alle Benutzer zusätzlich zu den Citrix-Lizenzen TS-CALs benötigt. Sie müssen daher den Einsatz von Citrix immer als Zusatzkosten sehen. Arbeiten Sie im Administrator-Modus für den Remotedesktop, verwendet dieser zwar auch die Terminalservertechnik, lässt aber nur zwei gleichzeitige Verbindungen zu. Bei diesen Verbindungen benötigen Sie keine Terminalserver-Zugriffs-Lizenzen. Installieren Sie Office auf einem Terminalserver, benötigen Sie so viele Lizenzen, wie Anwender mit den Terminaldiensten arbeiten. Allerdings lassen sich nicht alle Editionen und Lizenzen von Office auf einem Terminalserver installieren. Sie benötigen dazu Volumenlizenzen, ansonsten bricht die Installation von Office 2007 ab [2].

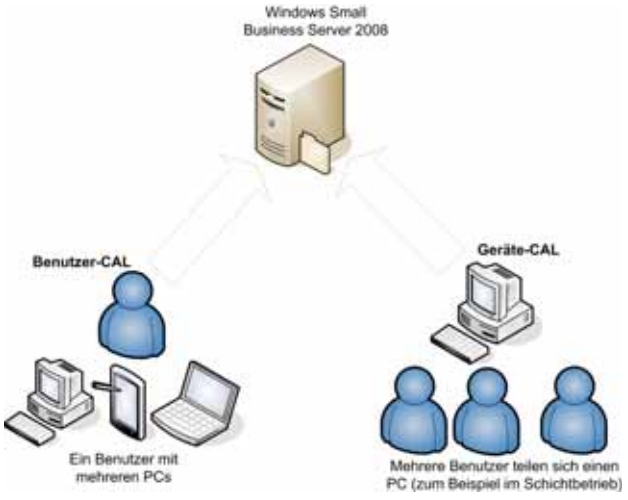


Bild 1: Zugriffslizenzen können pro Anwender oder pro Gerät erworben werden

Aktivierung für Unternehmen: Volume Activation (VA) 2.0

Für Windows Vista, Windows Server 2008 und Windows 7 gibt es keine Seriennummern mehr, welche die notwendige Aktivierung ersetzen. Bei den Vorgängerversionen hatte Microsoft noch die Volume Activation 1.0 eingesetzt. Dabei erhielten Unternehmen Seriennummern, die keiner Aktivierung bedurften. Bei der neuen Volume Activation 2.0 besteht diese Möglichkeit nicht mehr. Alle Produkte, die unter die VA 2.0 fallen, müssen aktiviert werden.

Microsoft stellt aber Tools und Funktionen wie das Volume Activation Management Tool (VAMT) oder den Key Management Service (KMS) zur Verfügung, über die sich die Aktivierung automatisiert abwickeln lässt. Auch wenn Sie einen aktivierten Windows-PC klonen wollen, müssen Sie die installierten Klone erneut aktivieren. Das gilt auch für Windows Server 2008 R2 und Windows 7. Unternehmen stellt Microsoft für die Aktivierung eine neue Serverfunktionalität zur Verfügung, sodass sich die Aktivierung der Arbeitsstationen nicht über das Internet, sondern automatisiert über das Netzwerk abwickeln lässt. Dieser Dienst kann auch auf einem Windows-PC installiert werden, setzt aber voraus, dass es im Netzwerk mindestens 25 PCs oder fünf Windows Server 2008-Computer gibt, wobei der Dienst bei Windows Server 2008 virtuelle Maschinen nicht mitrechnet.

Die Lizenzschlüssel für Unternehmen laufen auch nach Aktivierung nicht mehr unbegrenzt, sie erlauben aber eine mehrfache Aktivierung. Mit Volume Activation 2.0 steht für Microsoft das Verhindern des Missbrauchs von Volumen-Lizenzschlüsseln im Vordergrund. Heute können sich Unternehmen nicht wirksam dagegen wehren, wenn ein Mitarbeiter, Dienstleister oder Dritte die eigenen Schlüssel weitergeben oder im Internet veröffentlichen. Zukünftig sind derartige Schlüssel wertlos, da nur der Originalinhaber die Verwendung der mit dem Schlüssel abgedeckten Lizenzen festlegen kann. Für Office 2007 gelten diese Einschränkungen nicht. Office 2007 fällt noch unter die Volume Activation 1.0. Hier erhalten Unternehmenskunden eine Seriennummer, die keine Aktivierung erfordert.

Volume Activation 2.0 unterstützt die zentrale Verwaltung der Volumen-Lizenzen über einen Key Management Service (KMS) oder über Multiple Activation Keys (MAK). Der KMS-Dienst wird auf einem Computer mit einem eigenen Schlüssel aktiviert, der lediglich auf dem KMS-Host und nicht auf jedem einzelnen Computer zu finden ist. Der MAK ist auf den einzelnen Computern gespeichert, jedoch verschlüsselt und in einem vertrauenswürdigen Speicher, so dass Benutzer diesen Schlüssel nie zu sehen bekommen und auch nicht nachträglich auslesen können. Als Schlüssel verwendet Microsoft Cipher Block Chaining Message Authentication Code (CBC-MAC) mit dem Advanced Encryption Standard (AES) als grundlegende Verschlüsselungstechnologie. Dabei können Unternehmen zwischen zwei verschiedenen Arten von Schlüsseln (MAK und KMS) und drei Aktivierungsmethoden (MAK Proxy Activation, MAK Independent Activation und KMS Activation ab 25 Windows-Clients) wählen. Für die Verwaltung und die Abfrage von Lizenzinformationen auf Windows Vista/7- und Windows Server 2008-Computern stellt Microsoft das Skript *Slmgr.vbs* zur Verfügung.

Neben diesen Aktivierungsmethoden gibt es weiterhin die OEM Activation und Retail Activation: Bei der OEM Activation erfolgt eine Aktivierung vorab durch den OEM-Hersteller. Sie können an dem Computer beliebige Änderungen vornehmen. Lediglich das BIOS des Mainboards muss die OEM-spezifischen Informationen enthalten. Es wird nie eine Aktivierung erforderlich. Die Retail Activation kann ebenfalls durch den OEM erfolgen – in der Praxis führt diese aber der Endbenutzer durch. Er übermittelt während der Aktivierung die Product-ID und einen Hardware-Hash von unterschiedlichen Teilen des PCs, die einzeln gewichtet werden. Im Gegensatz zu Windows XP ist bei Windows Vista keine Neuaktivierung erforderlich, solange Sie die Festplatte nicht wechseln. Bei der MAK-Aktivierung findet ein ähnlicher Prozess statt wie bei MSDN- oder Action Pack-Versionen für Microsoft Partner. Jeder Produktschlüssel lässt sich für eine bestimmte Anzahl an Computern verwenden. Die MAK-Aktivierung müssen Sie nur einmal durchführen, Sie erlaubt beliebige Änderungen an der Hardware des Computers. Bei der Key Management Service (KMS)-Activation können Sie die Aktivierung der eingesetzten Windows-Computer über einen lokalen Server durchführen. Eine Verbindung zu Microsoft ist nicht notwendig. Die Clients müssen sich nach Aktivierung alle 180 Tage erneut beim KMS-Server reaktivieren.

Lizenzierung von Windows Server 2008 R2

Windows Server 2008 R2 gibt es in den Editionen Standard, Enterprise, Datacenter, für Itanium-basierte Systeme, Windows Web Server 2008 R2 und Windows Server 2008 R2 Foundation. Windows Server 2008 R2 Foundation ist eine neue Edition, die ausschließlich als OEM-Lizenz verfügbar ist. Jede Serverlizenz berechtigt dazu, einen Server zu installieren, außerdem dürfen nur 15 Benutzer mit dem Server arbeiten, weitere

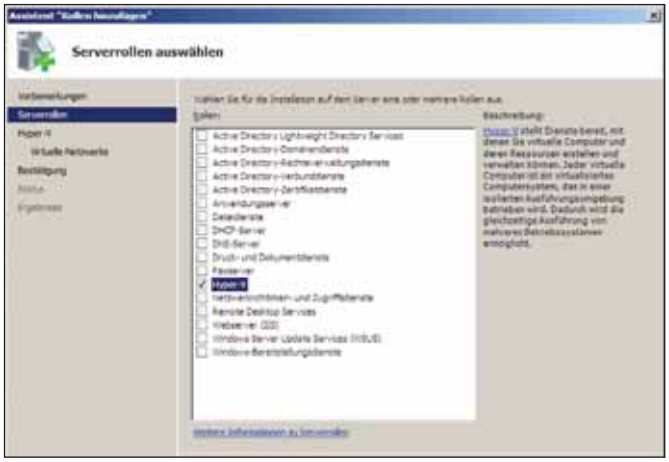


Bild 2: Hyper-V 2.0 ist kostenloser Bestandteil aller Editionen von Windows Server 2008 R2

Lizenzen, auch Benutzer-CALs, benötigen Sie bei dieser Edition nicht. Lizenzen müssen Sie einzelnen Benutzerkonten fest zuweisen. Lizenzierte Nutzer der Foundation-Edition dürfen mit ihren Lizenzen nur auf den Foundation-Server zugreifen, keinen anderen Windows-Server. Für Windows Server 2008 R2 Foundation benötigen Sie keine Server-CALs. Nutzen Sie allerdings die Active Directory-Rechteverwaltung, benötigen Sie für die Anwender auch CALs für die Rechteverwaltung. Beim Verwenden als Terminal-/Remotedesktopserver benötigen Anwender eine eigene RD-CAL. Die Foundation-Edition darf in einer Domäne betrieben werden, allerdings darf diese maximal 15 Benutzer enthalten und muss die Stammdomäne der Gesamtstruktur sein, der Betrieb in einer untergeordneten Domäne ist nicht erlaubt. Bemerkt der Server einen Lizenzverstoß, fährt er sich selbst nach elf Tagen herunter. Serverlizenzen für Windows Server 2008 berechtigen nicht zur Installation von Windows Server 2008 R2, Sie benötigen jeweils eigene Serverlizenzen für die Betriebssysteme, Benutzer-CALs für Windows Server 2008 gelten aber auch für Windows Server 2008 R2 und umgekehrt.

Alle Editionen enthalten jetzt eine Hyper-V-Lizenz, es gibt keine Versionen mehr ohne Hyper-V, wie noch bei Windows Server 2008. Für Windows Server 2008 R2 Foundation, Standard und Enterprise benötigen Sie für jeden Server eine Serverlizenz. Die Standard Edition deckt mit einer solchen Lizenz die Installation auf einem Host und eine virtuelle Maschine unter Hyper-V ab. Bei der Enterprise Edition dürfen Sie mit einer Lizenz bis zu vier virtuelle Maschinen mit Hyper-V installieren. Windows Web Server 2008 R2 enthält nur die Installation als Gast, Windows Server 2008 R2 Foundation nur eine Hostinstallation. Bei den Editionen Datacenter und Windows Server 2008 R2 für Itanium-basierte-Systeme dürfen Sie unbegrenzt virtuelle Maschinen erstellen, die Lizenzierung bei diesen Versionen ist prozessorbasiert.

Betreiben Sie Windows Server 2008 R2 Standard Edition mit einer Serverlizenz als Host für eine virtuelle Maschine, dürfen Sie auf dem Host keine anderen Serverdienste als Hyper-V ausführen, die gleichen Einschränkungen gelten für die Enterprise-Edition, nur dürfen Sie hier bis zu vier virtuelle Maschinen betreiben. Bei den Editionen Datacenter und Windows Server 2008 R2 müssen Sie alle physischen Prozessoren lizenzieren, nicht die enthaltenen Prozessorkerne. Die Mindestlizenz beträgt zwei Prozessoren, darunter dürfen Sie die Datacenter-Edition nicht installieren. Windows Web Server 2008 R2 dürfen Sie nur als Frontend-Server über das Internet zur Verfügung stellen.

Für Benutzerzugriffe benötigen Sie aber weiterhin Benutzer-CALs und CALs für die Remotedesktopdienste (RD-CALs). Microsoft bietet auch für Windows Server 2008 keine TS-CALs an, durch die Umbenennung der Terminaldienste in Remotedesktopdienste tragen diese CALs die Bezeichnung RD-CALs. Für den Zugriff auf die Microsoft Application Virtualization (App-V) für Terminaldienste benötigen Sie keine App-V-CAL für Terminaldienste mehr, die Lizenzierung ist jetzt durch die RD-CALs abgedeckt. Externe Anwender dürfen Sie auch über eine External Connector-Lizenz anbinden. Anwender, die sich über das Internet mit einem Server verbinden, benötigen keine Lizenz, wenn keine Authentifizierung am Server stattfindet, zum Beispiel bei öffentlichen Webseiten. Diese Benutzerzugriffe müssen Sie also nicht lizenzieren. Auch bis zu zwei Administratoren, die einen Server nur verwalten, benötigen keine Benutzer-CAL. Für Server, die nur als Hyper-V im Einsatz sind, benötigen Unternehmen ebenfalls keine Benutzer-CAL, allerdings für die virtuellen Maschinen auf dem Hyper-V-Server.

Zur Aktivierung von Windows 7 und Windows Server 2008 R2 müssen Sie KMS 1.2 verwenden, also die Version in Windows Server 2008 R2 und Windows 7. Die Version 1.0, die in Windows Server 2008 enthalten ist, kann kein Windows Server 2008 R2 oder Windows 7 aktivieren. Die Version in Windows Vista/7 ist Version 1.0. Die Version 1.2 berücksichtigt virtuelle Maschinen mit gleichem Gewicht wie physische Maschinen, in den Vorgängerversionen war die Anzahl der virtuellen Maschinen eingeschränkt.

Microsoft-Kunden mit aktiver Software Assurance mit Windows Server 2008-Lizenzen dürfen auf Windows Server 2008 R2 aktualisieren. Kunden ohne Assurance müssen für Windows Server 2008 R2 neue Lizenzen erwerben, Serverlizenzen für Windows Server 2008 sind bei Windows Server 2008 R2 nicht gültig. Wer Windows Server 2003 einsetzt, benötigt neue Benutzer-Lizenzen, Benutzer-CALs für Windows Server 2008 sind auch für Windows Server 2008 R2 gültig.

Fazit

Microsofts Lizenz-Politik ist alles andere als leicht durchschaubar. Es lohnt sich aber für Unternehmen aller Größenordnung, sich auch einmal die Volumenlizenzmodelle anzusehen. Zwar ist auch der Erwerb von OEM-Editionen mittlerweile legal und auch weit verbreitet, aber in verschiedenen Konstellationen lassen sich mit etwas Finesse einige Kosten einsparen, wenn Sie ein Volumenlizenzprogramm eingehen. Was Unternehmen aber beachten müssen, ist das Kleingedruckte in den Verträgen. Da steht zum Beispiel auch, dass Microsoft berechtigt ist, die Lizenzen vor Ort zu kontrollieren. Microsoft gibt solche Aufträge an Partnerunternehmen weiter, die genau Lizenzen und Software kontrollieren. Dokumentieren Sie daher ausführlich, welche Produkte Sie einsetzen. Ehrliche Kunden haben aber nichts zu befürchten und wer gut dokumentiert, hat mit den Kontrollen auch keine eigene Arbeit. *(jp)*

Links

[1] RD-CALs
http://support.microsoft.com/kb/823313/

[2] MS Office-Lizenzen für Terminalserver
http://support.microsoft.com/default.aspx/kb/924622/en-us.

Exchange Server 2007

Unzustellbarkeitsberichte als Kopie weiterleiten

von Robert Lindermeier

Für den Exchange-Administrator kann es durchaus sehr hilfreich sein, automatisch darüber informiert zu werden, welche unzustellbaren Nachrichten die Exchange-Organisation betreffen. Damit lassen sich beispielsweise fehlerhafte Konfiguration oder nicht funktionierende Konnektoren schnell erkennen.

In den Versionen bis Exchange Server 2003 war es relativ einfach, von jeder unzustellbaren Nachricht eine Kopie etwa an den Postmaster zu schicken. Dazu musste lediglich die gewünschte E-Mailadresse bei den Eigenschaften der SMTP-Server eingetragen werden. In diesem Workshop zeigen wir Ihnen, wie Sie Exchange 2007 konfigurieren, um von allen NDRs (Non Delivery Report) eine Kopie an Ihr E-Mailkonto zuzustellen. Wie Sie bereits aus vorangegangenen Workshops wissen, findet in Exchange 2007 die tiefer gehende Konfiguration meist in der Exchange Shell statt, so auch in diesem Fall. Sie können konfigurieren, wie mit Unzustellbarkeitsberichten an interne oder auch externe Absender verfahren wird.

Wird eine Unzustellbarkeitsnachricht an einen externen Absender generiert, erhält diese als Absenderangabe *Postmaster@{akzeptierte Standard-Domäne}*, also etwa Postmaster@your-admin.com. Per Default ist diese Adresse keinem Postfach zugeordnet, so dass Sie diese Adresse als zusätzliche SMTP-Adresse eintragen oder ein spezielles Postfach dafür erzeugen können. Unzustellbarkeitsnachrichten an interne Absender werden über den sogenannten "Microsoft Exchange Empfänger" verarbeitet. Hierbei handelt es sich um ein Empfängerobjekt, das von diversen internen Exchange-Funktionen benutzt wird, um vom System erstellte Nachrichten zu kennzeichnen.

Um nun Unzustellbarkeitsberichte an interne Absender als Kopie an das Postmaster-Postfach zu leiten, müssen Sie den "Microsoft Exchange Empfänger" dem Postmaster-Postfach zuordnen. Dies geschieht mit dem Kommando

```
Set-OrganizationConfig -Microsoft-
  ExchangeRecipientReplyRecipient
  {Empfänger-Identität}
```

Im nächsten Schritt müssen Sie nun die externe Postmasteradresse mit dem Cmdlet *set-TransportServer* definieren. Hier das Beispiel für unsere Workshopumgebung:

```
Set-TransportServer YA-HUB2
  -ExternalPostmasterAddress
  postmaster@your-admin.com
```

Dieses Kommando muss auf allen Hub-Transport-Servern ausgeführt werden. Dazu können Sie auch ein kombiniertes Kommando absetzen:

```
Get-TransportServer | Set-Transport-
  Server -ExternalPostmasterAddress
  postmaster@your-admin.com
```

Zur weiteren Konfiguration der Edge-Transport-Server verwenden wir das folgende Kommando

```
Set-TransportServer YA-Edge1
  -ExternalPostmasterAddress
  postmaster@your-admin.com
```

Unzustellbarkeitsberichte werden über sogenannte DSN-Codes gesteuert (Delivery Status Notification). Per Default werden die wichtigsten Codes überwacht. Nähere Informationen dazu finden sich unter [1]. Es ist durchaus möglich, weitere Codes zur Überwachung zu aktivieren. Im Regelfall sind die Default-Codes völlig ausreichend. Die zu überwachenden DSN-Codes können mit dem Cmdlet *Set-TransportConfig* konfiguriert werden. Beispiele finden sich ebenfalls unter [1].

Aufgrund der vorangegangenen Konfiguration werden nun auf den Hub-Transport-Servern alle betreffenden Unzustellbarkeitsnachrichten als Kopie in das Postmaster-Postfach zugestellt. Edge-Transport-Server senden die Kopie an die zugeordnete externe Postmasteradresse. Damit behalten Sie als Administrator den Überblick über unzustellbare Nachrichten. *(dr)*

Robert Lindermeier ist Inhaber und Senior Messaging Consultant bei YOUR-ADMIN.

Links

[1] DSN-Codes
http://technet.microsoft.com/de-de/library/bb232118.aspx

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

Windows

Ich arbeite unter Windows XP regelmäßig mit der **Kommandozeile**. Dabei sind mir die wichtigsten Befehle geläufig. Manchmal jedoch brauche ich auch mir unbekannte Kommandos und muss erst aufwändig danach suchen. Gibt es hierfür eine einfachere Lösung?

Sie können die Befehlszeilenreferenz bei Bedarf auch auf Ihrem Desktop als Verknüpfung ablegen. Dadurch entfällt die Suche danach. Erstellen Sie hierfür einen neuen Link und tragen Sie als Inhalt die Zeile

```
hh.exe ms-its:C:\WINDOWS\Help\
  ntcmds.chm::/ntcmds.htm
```

ein, sofern C: Ihr Systemlaufwerk ist. Mit einem Doppelklick auf diese Verknüpfung öffnet sich nun die Befehlsreferenz. *(dr)*

Wir arbeiten auf manchen Rechnern mit **Netzwerkapplikationen**, die jedoch auf **lokale DLL-Bibliotheken** zugreifen sollen. Auf welchem Weg können wir den Library Search-Ordner unter Windows XP anpassen?

Hierfür bietet sich eine kleine Änderung in der Registry an. Öffnen Sie den Registry-Editor mit *regedit* und gehen Sie zum Schlüssel "HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Control \ Session Manager". Dort liegt der Wert "SafeDllSearchMode" als DWORD – falls er nicht vorhanden ist, legen Sie ihn einfach an. Tragen Sie nun für diesen Wert eine "0" ein, damit Windows zunächst im gerade geöffneten Verzeichnis nach den nötigen DLLs sucht. Das kann in Ihrem Fall das momentan benutzte Programmverzeichnis sein, in dem sich dann auch die zugehörigen DLLs befinden sollten. Mit einer "1" sucht das Betriebssystem dagegen erst im System- und Windows-Verzeichnis. *(dr)*

Wir nutzen in unserem Netzwerk ein **Active Directory**. Dabei fragen wir auch immer wieder die **Mitglieder von Gruppen** ab und nutzen hierfür den Befehl *LDAP://cn=Domänen-Benutzer, cn=Users,dc=xyz,dc=local*. Doch leider tauchen dabei die Nutzer der Gruppe **Domänen-Benutzer** nicht auf. Stattdessen bekomme ich nur den Administrator angezeigt. Woran liegt das und wie kann ich diesen Fehler beheben?

Über diese Befehlszeile funktioniert die Abfrage der Domänen-Benutzer im Active Directory in der Tat nicht. Die Ursache liegt darin, dass die Gruppe der Domänen-Benutzer bei den Usern die primäre Gruppe ist. Dementsprechend sind die Nutzer nicht in der Liste der Mitglieder aufgeführt. Vielmehr tragen diese User die primaryGroupID 513, die sie als Domänen-Benutzer ausweist. Dementsprechend müssen Sie Ihre Suche auf die genannte primaryGroupID ausweiten. Dann sollten Ihnen die Domänen-Benutzer korrekt angezeigt werden. *(dr)*

Apple

Ich verwende einen Mac OS X-Rechner im Netzwerk. Möchte ich dabei **mehrere Dateien von einer Server-Freigabe löschen** und diese dauerhaft aus dem Papierkorb entfernen, muss ich diese Aktion immer bestätigen. Da ich mit sehr vielen Dateien arbeite, ist dies auf Dauer nervend. Wie kann ich diese **Abfragen deaktivieren**?

Mac-Rechner besitzen diese Abfrage zur Sicherheit, damit nicht versehentlich Dateien gelöscht werden – insbesondere, wenn es sich um Dateien aus dem Netzwerk handelt. Möchten Sie dennoch diese Dateien ohne Rückfrage aus dem Papierkorb entfernen, so müssen Sie lediglich die Tastenkombination "Befehl-Wahl-Tabulator" beim Verschieben der Dateien in den Papierkorb gedrückt halten. Entfernen Sie diese dann dauerhaft, erscheint keine weitere Rückfrage mehr. *(dr)*

Jedes Mal, wenn ich in Microsoft Word 2003 / 2007 ein **Seriendruck-Dokument öffnen** möchte, erscheint ein Fenster mit einer zusätzlichen **Sicherheitsabfrage**. Diese muss ich erst mit "Ja" bestätigen, um die Datei anzuzeigen. Da ich recht oft mit Serienbriefen arbeite, würde ich mir diese unnötige Nachfrage gerne ersparen. Geht das irgendwie?

Die Extra-Nachfrage soll verhindern, dass Nutzer auf Dokumente mit manipulierten SQL-Abfragen zugreifen, mit denen ein Angreifer Informationen in der Datenbank verändern kann. Wenn Sie jedoch nur selbst erstellte Dokumente verwenden, ist eine derartige Infektion der Dateien kaum zu befürchten und Sie können die Sicherheits-Abfrage mit folgenden Schritten unterdrücken: Starten Sie zunächst mit *regedit* den Registrierungseditor. Navigieren Sie dann zum Schlüssel "HKEY_CURRENT_USER \ SOFTWARE \ Microsoft \ Office\ 12.0 \ Word \ Options", wenn Sie Word 2007 verwenden. Bei Word 2003 lautet der Pfad "… \ Office \ 11.0 \ Word \ Options". Klicken Sie nun auf "Bearbeiten \ Neu \ DWORD-Wert" und tippen Sie unter "Name" "SQLSecurityCheck" ein. Dem neuen Eintrag wird automatisch der Wert "0" zugewiesen, womit die Sicherheitsabfrage abgeschaltet ist. Mit "1" können Sie diese bei Bedarf wieder aktivieren. Um die Änderungen in die Tat umzusetzen, schließen Sie noch den Editor und starten Sie Word neu. *(ln)*

In unserer Citrix-Umgebung mit **HDX 3D Professional Graphics** haben die Anwender immer wieder Probleme mit der **Fenstergröße**. Dies liegt an der **Connection-Bar** (Desktop Toolbar). Wie können wir diese deaktivieren und stattdessen im Fenstermodus arbeiten?

Der Fenstermodus lässt sich verwenden, wenn die Desktop Toolbar deaktiviert wird. So sind Anwender in der Lage, mit einer spezifizierten Fenstergröße zu arbeiten. Loggen Sie sich als Administrator auf der Maschine ein, die den Xen-Desktop Delivery Controller (DDC) hostet. Navigieren Sie in das Verzeichnis "C:\Inetpub\wwwroot\Citrix\DesktopWeb\conf" für den Web Interface Client sowie in den Ordner "C:\Inetpub\wwwroot\Citrix\PNAgent\conf" für den Program Neighborhood Agent. Editieren Sie die Datei *default.ica* in beiden Verzeichnissen und fügen Sie die Zeile *ConnectionBar=OFF* in die Sektionen "WFCLIENT" sowie "APPLICATION" ein. Diese Einträge ermöglichen die Anfrage Fenster-basierter Sitzungen und verhindern, dass die Auflösung und Farbtiefe der Desktop Toolbar im Cache beim Aushandeln der Sessions verwendet wird. Beachten Sie jedoch, dass die USB-Remote-Nutzung und Client-seitige Skalierung damit ebenfalls deaktiviert werden. Beide Features sind wieder aktiv, wenn Sie die Zeile "ConnectionBar=OFF" löschen und somit auch die Connection Bar wieder aktivieren. Sie können die Desktop Toolbar auch lediglich für eine Session deaktivieren. Klicken Sie hierfür vor der Verbindung mit dem Desktop mit der rechten Maustaste auf den Desktop und wählen Sie "Ziel speichern als". Speichern Sie die Datei *launch.ica* als Typ Citrix ICA Client und editieren Sie diese mit dem Windows-Editor. Suchen Sie nach dem Desktop-Namen und ändern Sie die Zeile *ConnectionBar=1* in *ConnectionBar=0*. Diese Einstellung startet den Desktop ohne die Desktop-Toolbar und gilt lediglich während der laufenden Session. *(Citrix/dr)*

Zum Erstellen einer **Abwesenheitsnotiz** unter Lotus Notes haben wir im Unternehmen bisher immer auf einen Agenten in der Maildatenbank zurückgegriffen. Insgesamt ist diese Funktion jedoch leider recht fehleranfällig. Steht hier nicht auch ein wirkungsvollerer und **stabilerer Mechanismus** zur Verfügung?

Ab der Domino-Version 8 besteht die Möglichkeit, den Abwesenheitsagenten als Dienst auf dem Domino-Server zu betreiben. Diese Vorgehensweise spart Server-Ressourcen und bietet zudem erweiterte Funktionen. So ist der Nutzer zum einen in der Lage, eine Abwesenheitsdauer von weniger als einem Tag einzustellen. Zum anderen reagiert der im Mail-Router verankerte Dienst prompt auf eingehende Nachrichten. Damit lassen sich die bislang zwangsläufig erduldeten Wartezeiten auf null reduzieren. Im Administratorclient sind die aktivierten Abwesenheitsagenten unter der Maildatenbank übersichtlich aufgelistet. Die Aktivierung des Abwesenheitsagenten über den Typ "Service" wird im Konfigurationsdokument – etwas versteckt – über die Registerkarte "Router – SMTP / Erweitert / Steuerung" vorgenommen. Einziger Wehrmutstropfen: Die Funktion setzt eine Mailschablone und einen Client der Version 8.x voraus. In gemischten Umgebungen ist es trotzdem ohne Probleme möglich, die Funktion zu aktivieren. Alle Benutzer des Servers, die noch nicht über eine 8.x Maildatenbank verfügen, arbeiten dann jedoch weiterhin mit der klassischen Variante des Agenten. Weitere Informationen zum neuen Abwesenheitsagenten finden Sie unter *www.ibm.com/developerworks/lotus/library/notes8-ooo/* *(acocon/ln)*

Tools

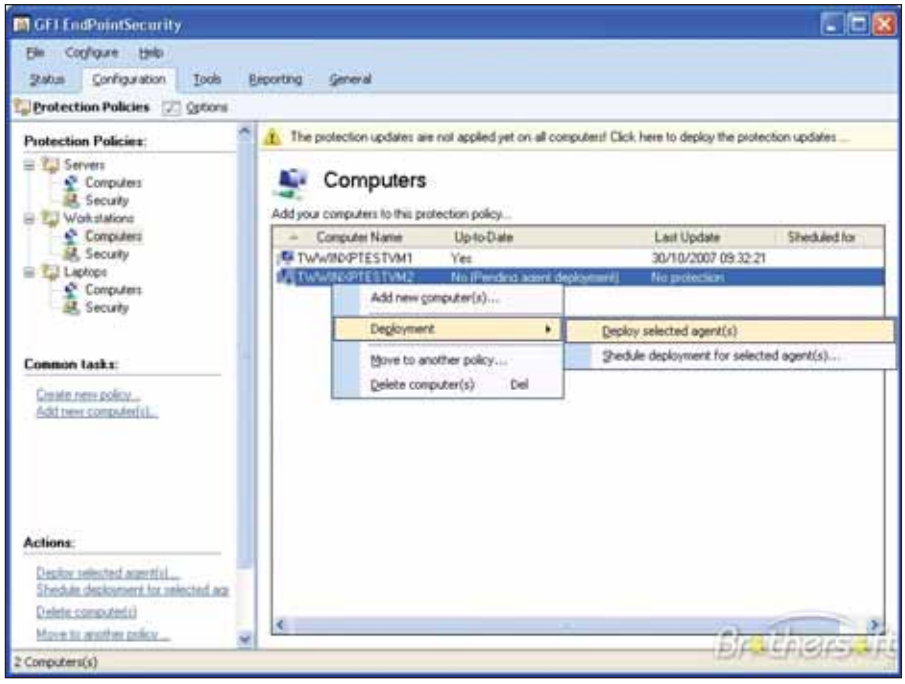
Der zunehmende Einsatz von USB-Sticks, Speicherkarten, Smartphones und anderen **mobilen Datenträgern** sowie die wachsende Speicherkapazität solcher Geräte entwickeln sich immer mehr zu einer ernsten Bedrohung für die Informationssicherheit in den Unternehmen. Unzureichende oder nichtexistente Sicherheitsmechanismen begünstigen sowohl den Datendiebstahl als auch das Einschleusen schädlichen Codes. Jedoch ist eine umfassende Sicherung aller Schnittstellen für mobile Speichermedien gerade für kleine und mittlere Unternehmen ein kostspieliges Unterfangen. Hier bietet sich die kostenlose Version von **GFI EndPointSecurity** an.

Die kostenlose Software ermöglicht das **Monitoring mobiler Speichermedien** im Netzwerk und gibt den Verantwortlichen einen Überblick darüber, wer welche Geräte einsetzt und welche Daten darauf überträgt. Zwar erlaubt das Werkzeug in der freien Version nicht, solchen Datenabfluss zu stoppen, in kleineren Umgebungen sind jedoch hierfür andere Vorgehensweisen naheliegend. Das Tool ermöglicht dabei, folgende Speichermedien zu beobachten:

- Media-Player, darunter iPods, Creative Zens und andere mobile Unterhaltungsgeräte
- USB-Laufwerke, CompactFlash- und ähnliche Speicherkarten, CDs, Disketten sowie weitere tragbare Medien
- PDAs, BlackBerry-Handhelds, Mobiltelefone, Smartphones und ähnliche Kommunikationsgeräte
- Netzwerkkarten, Laptops und andere Netzwerkverbindungen

Die aktuelle Version von GFI EndPointSecurity unterstützt zudem Microsoft Windows 7 sowie den Einsatz von mobilen Endgeräten, die mit BitLocker to Go verschlüsselt sind. Zur Nutzung der freien Version müssen Administratoren die 30-Tage-Version des Produktes herunterladen, die mit einem Lizenzschlüssel daherkommt und nach Ablauf der 30 Tage als Freeware weiter funktioniert. *(jp)*

Quelle: www.gfi.com/endpointsecurity



GFI EndPointSecurity schützt vor unerwünschten Datenströmen von oder zu mobilen Datenträgern

Ein weiteres Feld der IT, in dem die Anschaffung einer professionellen, kostenpflichtigen Lösung dem sprichwörtlichen Beschuss von Spatzen mit Kanonen ähnelt, ist die Virtualisierung. Betreibt ein Unternehmen nur einen oder zwei Server virtuell, lohnt sich die Anschaffung eines speziellen **Backupwerkzeuges für die virtuellen Server** kaum. Andererseits ist es ebenso wenig eine Option, diese Server ungesichert zu betreiben. Hier kann eine **kostenlose virtuelle Appliance** für den Backup virtueller Maschinen, wie sie Arkeia zur Verfügung stellt, sicher helfen.

Die "Free Use Edition" der virtuellen Appliance besteht aus der Backup-Lösung von Arkeia auf einem optimierten Linux-System, das in Form einer virtuellen Maschine für VMware ausgeliefert wird. Mit dabei sind **uneingeschränkte Lizenzen für den Backup zweier virtueller Maschinen**. Damit steht Anwendern ein kostenloses Werkzeug für die Datensicherung in kleinen VMware-Umgebungen zur Verfügung. Die Virtual Appliance kann sowohl mit VMware ESX als auch mit VMware ESXi eingesetzt werden. Die Virtual Appliance lässt sich mit wenigen Mausklicks installieren und konfigurieren. Es wird weder zusätzliche Hardware noch Software benötigt, und auch die Installation oder ein Update des Betriebssystems entfallen. Eine einzelne Appliance kann TBytes von Daten sichern; wächst die virtuelle Umgebung weiter, lassen sich auch mehrere Appliances parallel betreiben und gemeinsam mit physischen Appliances oder traditionellen Software-Installationen zentral verwalten. Zum Download der Freeware ist lediglich eine verifizierte Registrierung erforderlich. *(jp)*

Quelle: www.arkeia.com/freevmwarebackup/

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

Quelle: Markus Langer - Fotolia.com

Kosten beim Umstieg auf Windows 7

Wider der Kostenfalle

von Oliver Bendig

Microsoft Windows 7 gilt als der gesetzte Kandidat für die Nachfolge des überaus erfolgreichen Windows XP. Gemäß einer aktuellen IDC-Studie werden weltweit bis Ende 2010 etwa 177 Millionen Lizenzen von Windows 7 auf den Markt kommen. Bei der Umstellung auf den jüngsten Microsoft-Spross gilt es, neben dem reinen Preis für das neue Betriebssystem auch weitere Kosten im Auge zu behalten.

Mit Windows Vista ist es Microsoft nicht so recht gelungen, im Unternehmensumfeld Fuß zu fassen. Über die Gründe der verhaltenen Akzeptanz von Vista zu spekulieren, ist mittlerweile müßig. Seit dem 22. Oktober 2009 ist klar: Vista wird eher zu einer Randnotiz der Computergeschichte werden. Alle Hoffnungen von Microsoft liegen nun auf Windows 7. Die Analysten von IDC sagen eine Marktverbreitung von 59 Prozent innerhalb von drei Jahren voraus, was eine Verdoppelung im Vergleich zu Windows XP darstellen würde.

Generelle Migrationspfade

Die Umstellung von Windows XP zu Windows 7 als Client-Betriebssystem im Unternehmen ist grundsätzlich über zwei Wege möglich: Entweder werden die bisherigen XP-Maschinen sukzessive durch neue Windows 7-PCs ersetzt, oder die vorhandenen Computer sind neu zu installieren. Ein Inplace-Upgrade von XP nach Windows 7 bietet Microsoft nicht an. Der aktuell mit XP installierte PC muss für Windows 7 definitiv neu aufgesetzt werden.

Alle Programme, Einstellungen und Daten gehen bei diesem Vorgang zwangsläufig verloren, da die Neuinstallation sämtliche Informationen auf der Systemfestplatte löscht. Für die Übernahme von Dateien und Einstellungen hat Microsoft zwar den so genannten "Windows Easy Transfer" im Angebot, dieses Tool eignet sich jedoch in erster Linie für den Einsatz bei privat genutzten Einzel-PCs. Eine firmenweite Umstellung der Windows-Einstellungen oder der Konfigurationsinformationen von Drittherstellern sind mit dem kleinen Programm nicht möglich.

Wie die Vorgänger wird auch Windows 7 in verschiedenen Editionen angeboten. Die Varianten Home Premium, Professional und Ultimate sind primär für den Endbenutzermarkt abgestimmt und liegen bei den Vollversionen zwischen 120 und 300 Euro. Was im Privatumfeld als "Ultimate" bezeichnet wird, ist für das Unternehmen passenderweise die "Enterprise"-Edition.

Die einfachsten Versionen "Starter" und "Home" scheiden in der Mehrzahl der Fälle aus, da sie keinen Domänenbeitritt zulassen. BitLocker und Branch Cache sind Innovationen, die nur in den größten Ausprägungen angeboten werden. Je nach Unternehmensgröße, Vertrag und Konditionen fallen die Windows-Preise sehr unterschiedlich aus. Sie sind jedoch im Vergleich zu den anderen Kosten der Migration sehr leicht zu identifizieren und zu berechnen.

Mehrkosten durch Client-Aufrüstung

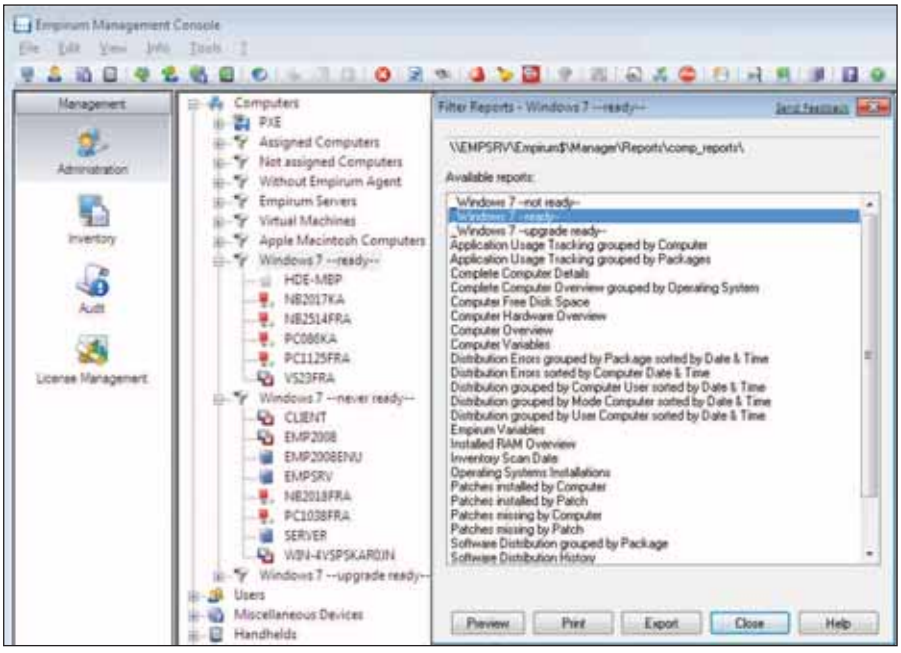
Glücklicherweise sind die Systemvoraussetzungen von Windows 7 insgesamt recht moderat, so dass eine große Anzahl der derzeitigen Windows XP- oder Vista-PCs auch mit dem neuesten Windows betrieben werden kann. Bekanntlich handelt es sich bei den in Tabelle 1 beschriebenen Systemvoraussetzungen eher um Mindestanforderungen denn um eine Empfehlung für einen agil reagierenden PC.

Für einfachere Büro-Aufgaben, bei denen typischerweise nur eine oder zwei Applikationen gleichzeitig verwendet werden, sind diese Angaben jedoch durchaus ausreichend. Die Prozessorleistung von 1 GHz erfüllen sehr viele Computer, da selbst im Jahre 2003 ein Einstiegs-PC mit 1,2 GHz Rechenleistung ausgestattet war. Die geforderte Festplattengröße dürfte lediglich bei einigen Notebooks zu einem Problem werden, da eine 40 GByte-Festplatte seit weit mehr als fünf Jahren die typische Mindestausstattung eines Büro-Computers darstellt.

Schwierig wird es indes bei der Forderung nach einem Gigabyte Hauptspeicher. Vor gut fünf Jahren wurden Computer mit lediglich 256 MByte Arbeitsspeicher ausgestattet. Die Ausprägung des

Arbeitsspeichers in dieser Zeit war vorwiegend SDRAM. Diese Bausteine werden heute noch von verschiedenen Versendern angeboten, aber bei weitem nicht mehr in der Vielfalt und zudem zu einem Preis, der eine Aufrüstung häufig unattraktiv macht. Zwei 512 MByte große SDRAM-Riegel liegen aktuell bei einem Anschaffungspreis von über 100 Euro. Zu diesem Preis addiert sich der manuelle Aufwand beim Einbau und etwaigen BIOS-Updates, die eine effektive Nutzung des Speichers erst ermöglichen.

Für die Bedarfsermittlung im Unternehmen bieten sich die Report-Funktionen von Systems-Management-Programmen förmlich an. Mit entsprechend gesetzten oder durch den Hersteller vorbereiteten Reports und Filtern lassen sich Computer in drei Kategorien einteilen: PCs, die mit Windows 7 sofort funktionieren werden, Rechner, die eine Aufrüstung erfordern und ältere Maschinen, die die Voraussetzungen unter vertretbarem Aufwand nicht erreichen.



Welche Computer im Unternehmen für eine Umstellung auf Windows 7 überhaupt geeignet sind, ist mit den richtigen System-Management-Programmen sehr leicht feststellbar

Kostenkriterium Treiberverfügbarkeit

Im Gegensatz zu Windows XP basieren Windows 7 und Vista auf einem gänzlich anderen Treibermodell. In der Praxis hat dies zur Folge, dass für jede Systemkomponente und für jedes Peripherie-Gerät die aktualisierten und passenden Treiber zur Verfügung gestellt werden müssen. Ohne korrekte Geräte-Treiber lässt sich Windows 7 nicht automatisiert installieren oder das Gerät funktioniert nicht korrekt. Windows Vista-Treiber lassen sich durchaus auch in Windows 7 nutzen. Eine genaue Prüfung vor der Umstellung ist dennoch erforderlich, da einige Hersteller die Windows-Versionsnummer fest in ihren Installationsroutinen abprüfen. In solchen Fällen bietet Windows 7 die Funktion "Troubleshoot Compatibility", die einer Software eine andere Windows-Versionsnummer vorgaukelt. Primär handelt es sich bei dieser Funktion jedoch um eine Möglichkeit, Software in einem Kompatibilitätsmodus zu betreiben, weniger um Treiber ins System einzubinden.

Bei der Suche nach den richtigen Treibern für Systemkomponenten und externe Geräte wie Scanner oder Drucker ist die Inventarisierungsdatenbank einer Systems-Management-Lösung einmal mehr die Grundlage für die richtige Planung. Welche Komponenten und Geräte im Unternehmen in welcher Anzahl überhaupt eingesetzt werden, ist mit einem Report in wenigen Mausklicks beantwortet. Bietet ein Hersteller nicht die passenden Treiber an, so muss dieses Gerät, sofern möglich, durch ein anderes ersetzt werden. Dies ist in der Berechnung der Gesamtkosten für die Migration entsprechend zu berücksichtigen.

Großbaustelle Softwarekompatibilität

Die Hauptaufgabe eines Betriebssystems ist das Betreiben von Anwendungen. Folgerichtig gilt es, alle Applikationen, die im Unternehmen genutzt werden, auf ihre Funktionstüchtigkeit unter Windows 7 zuvor zu erproben. Während bei Programmen wie Microsoft Office oder SAP GUI kaum mit Inkompatibilität zu rechnen ist, sieht das bei Branchenlösungen oder Eigenentwicklungen möglicherweise etwas anders aus. Microsoft bietet unter [1] ein kostenfreies Programm mit dem Namen "Application Compatibility Toolkit 5.5", um Software auf ihre Zusammenarbeit mit Windows Vista / Windows 7 hin zu prüfen. Welche Programme überhaupt im Unternehmen betrieben werden, beantwortet wieder einmal der Report ei-

So sehen laut Microsoft die Systemvoraussetzungen für Windows 7 aus

	32-Bit (x86) Windows 7	64-Bit (x64) Windows 7
CPU	1 GHz	1 GHz
RAM	1 GByte	2 GByte
HDD	16 GByte	20 GByte
Grafik	Direct-X 9 mit WDDM 1.0 oder höher	Direct-X 9 mit WDDM 1.0 oder höher

ner Systems-Management-Software oder der Blick in eine hoffentlich akribisch geführte manuelle Liste. Zwar empfiehlt es sich, jedes einzelne Programm in einer Teststellung intensiver auf die fehlerfreie Zusammenarbeit mit Windows 7 zu prüfen, doch sollte der Blick zunächst auf die Hauptanwendungen fallen. Bei welchen Applikationen es sich um Hauptanwendungen handelt, lässt sich entweder durch den rhythmischen Einsatz von WMI-Skripten feststellen, die aktive Programm-Prozesse in einer Datenbank ablegen, oder mit Hilfe einer Systems-Management-Software. Das Migrationsvorhaben eignet sich somit, Kosteneinsparpotentiale direkt zu nutzen, um teure und zu gering frequentierte Software auszusondern.

Für eine Migration müssen die Kosten für die Umstellung auf neue Programmversionen in die Kalkulation mit aufgenommen werden. Den direkten Kosten stehen die Mehrwerte, die eine neue Version eines Programms bietet, gegenüber. Möglicherweise ist eine Verjüngung der Applikationen schon im Vorfeld des Migrationsvorhabens eine Alternative, um Benutzer nicht mit einer zu großen Anzahl von Neuerungen an einem Tag zu überfordern. Auch wenn bereits eine Systems-Management-Lösung im Einsatz ist, so muss, je nach Umfang des Softwarepakets, mit bis zu zwei Tagen an zeitlichem Aufwand gerechnet werden, bis eine Business-Applikation für den Roll-Out bereitsteht.

So identifizieren Sie Upgrade-Kosten bei der Migration auf Windows 7

- Überlegen Sie sich vor dem Umstieg genau, welche Windows-Versionen Sie wirklich benötigen.
- Stellen Sie vorab fest, welche PCs Sie austauschen oder aufrüsten müssen.
- Identifizieren Sie diejenigen Arbeitsplätze, die sich möglicherweise besser für den Terminal Server-Betrieb eignen.
- Fertigen Sie eine Liste der unbedingt erforderlichen Anwendungen an.
- Bedenken Sie die Auswirkung der Umstellung auf das Lizenzmanagement.

Ist eine für das Unternehmen benötigte Software aktuell nicht für Windows 7 verfügbar, so kann diese im "XP Mode" in einer virtualisierten Umgebung weitergenutzt werden. Dieser Modus ist in den drei Versionen Professional, Enterprise und Ultimate verfügbar. Die Lizenz für das virtuelle Windows XP ist in diesen Editionen im Lizenz-Preis von Windows 7 inbegriffen. Da die Leistungen in einer auf dem Client-Computer virtualisierten Umgebung gesenkt und der zu erwartende administrative Aufwand durch den XP-Modus erhöht werden, ist diese Variante eher der Notnagel denn die geeignete Dauerlösung. Zudem setzt diese Funktion einen Hauptprozessor voraus, der Virtualisierung unterstützt, was bei vielen älteren Rechnern nicht der Fall sein dürfte.

Auswahl des Migrationszeitpunkts

Windows 7 hat grundsätzlich das Potential, die Arbeitsweisen in Unternehmen zu vereinfachen und zu beschleunigen. Mit Blick auf die bereits begonnene, erweiterte Produktsupport-Phase von XP ist Windows 7 andererseits eine Art Zwangskandidat. Nach einer Analyse der zu erwartenden Kosten für die Migration gilt es für die IT-Abteilung, den geeigneten Zeitpunkt für die Umstellung zu wählen. Wird eine Systems-Management-Lösung für die Migration eingesetzt, so bietet es sich an, den Zeitpunkt durch den Anwender selbst wählen zu lassen. Der Benutzer weiß selbst am besten, wann er auf einen funktionierenden PC für rund zwei Stunden verzichten kann. Diese Form der Mitsprache dürfte in vielen Fällen wohlwollend aufgenommen werden. Es versteht sich von selbst, dass eine solche Entscheidungsphase nicht unbegrenzt lang sein darf, da der IT-Support ansonsten über sehr lange Zeit zwei Betriebssysteme zu betreuen hat. Die errechneten Kosten für die Umstellung den Benutzern und deren Vorgesetzten über einen Service-Katalog offenzulegen, ist ein weiterer wichtiger Schritt in Richtung Transparenz – die Umstellung geschieht ja nicht zum Selbstzweck der IT.

Eine nirgends festgeschriebene, aber vielen Administratoren bekannte Regel besagt, dass eine Migration im Windows-Umfeld vor einem Service Pack 1 als überaus mutige Entscheidung einzustufen ist. Sollte das Migrationsvorhaben aktuell noch auf einen unbestimmten Zeitpunkt in der Zukunft terminiert sein, so bietet sich die Zeit für einige Vorbereitungen an. Eine im Vorfeld definierte und standardisierte Benutzer-Umgebung reduziert manuelle Arbeitsschritte und die Komplexität. Möglicherweise ist ein Leasing von PC-Arbeitsplätzen eine Alternative zum Kauf – Angebote lassen sich mit der nötigen Ruhe besser vergleichen als unter Zugzwang. Nur gering genutzte Arbeitsplätze bieten sich vielleicht für eine Umstellung auf ThinClients im Windows Terminal Server 2008-Betrieb an.

Fazit

Das Zusammenspiel aller Gattungen im Systems-Management, vom Lizenz-Management über das Asset- hin zum Contract-Management, erlaubt in der Summe ein effektives und im Vorfeld kalkuliertes Umstellen auf Windows 7. Wird überhaupt kein Automatismus eingesetzt, so erreichen die Umstellungskosten ungeahnte Höhen mit mindestens vier Stunden Zeitaufwand je Arbeitsstation – bei der der EDV-Mitarbeiter primär damit beschäftigt ist einem Installationsprozessbalken von links nach rechts beim Wandern zuzusehen. In vielen Unternehmen ist eine manuelle Umstellung aufgrund der Masse von PCs zudem ohnehin nicht möglich. *(ln)*

Oliver Bendig ist Direktor Produktmanagement bei der Matrix42 AG in Neu-Isenburg.

Links

[1] Microsoft Application Compatibility Toolkit (ACT) 5.5
http://msdn.microsoft.com/en-us/library/dd562082%28VS.85%29.aspx

Windows 7 für Administratoren

Einer der ersten Windows 7-Ratgeber für Admins kommt vom Microsoft-Profi Ulrich B. Boddenberg. Sein "Windows 7 für Administratoren" ist mit 800 Seiten ein Klotz von einem Buch. Doch der Funktionsumfang und vor allem die Interaktion von Windows 7 mit dem Netzwerk erfordert viel Platz für Erklärungen. Selbst bei diesem üppigen Umfang hätten es hier und da noch ein paar Details mehr sein dürfen. Doch ist Boddenberg wirklich kein Vorwurf zu machen. Er hat langwierige Einleitungen komplett gestrichen und beschränkt sich auf die Dinge, die einen Administrator interessieren. Beschreibungen der geänderten Systemsteuerung und grafischer Spielereien sucht man vergebens. Und da gibt es wahrlich genug zu beschreiben. Nach einem kurzen Einstieg, in dem die Änderungen zu den vorigen Betriebssystemversionen und deren Technologiegrundlagen aufgelistet werden, nähert sich der Autor dem Thema zunächst, ganz logisch, über das Deployment. Der Umgang mit dem WAIK wird erläutert und die WDS als Deployment-Methode beschrieben.

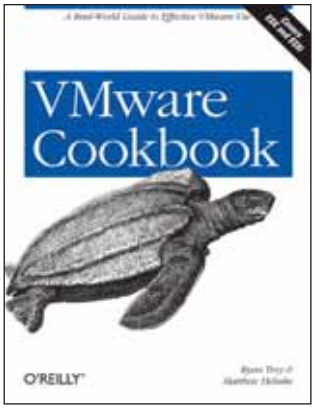
Generell setzt dieses Kapitel Zeichen für den Rest des Buchs. Administratoren mit Vorkenntnissen erhalten genug Infos, um sich selbst durch weiterführende Aufgaben zu hangeln. Neulinge dürften oft von den Querverweisen zur Microsoft Knowledge-Base Gebrauch machen. Insgesamt sind technisches Level und Erklärungsfokus auf den Betreuer mittlerer und größerer Netze zugeschnitten, Gelegenheitsadmins benötigen vermutlich noch etwas mehr Grundlageninfos. Nach dem Deployment geht es über Aktivierung, Applikationen und Gruppenrichtlinien weiter. Sehr gelungen: das große und umfangreiche Kapitel zum Thema Sicherheit. Man muss zwar sattelfest in den Sicherheitstechnologien sein, erfährt aber schnell und sehr klar, welche Ansätze Windows 7 für Sicherheitsmaßnahmen bietet. Zum Ende gibt es noch einen Abschnitt, in dem viele typische Administrationsaufgaben anhand des System Center Configuration Manager 2007 R2 beschrieben werden. Das ist gut für alle, die dieses Tool einsetzen, bringt aber den Nutzern von Drittprodukten wenig.

Fazit: Trotz manchmal etwas knapper Anleitungen ist " Windows 7 für Administratoren" ein absolut empfehlenswertes Buch, wenn im Unternehmen das neue Microsoft Client-Betriebssystem eingesetzt und verwaltet werden soll.

Elmar Török

Autor:	Ulrich B. Boddenberg
Verlag:	Galileo Computing
Preis:	49,90 Euro
ISBN:	978-3-8362-1501-5
Bewertung:	★★★★☆

VMware Cookbook



Die Kochbücher von O'Reilly arbeiten bestimmte Problemstellungen auf wenigen Seiten erschöpfend ab – Rezepte sozusagen. Im Fall des "VMware Cookbook" liegt der Schwerpunkt auf VMware ESX 3.x. Allerdings streifen die Autoren auch vSphere 4.0/ESX 4.0 und gehen in einzelnen Rezepten auf die Unterschiede zu ESX 3.x ein. Auch ESX 3.5i wird erwähnt und dessen Besonderheiten berücksichtigt. Generell soll der Leser Lösungen finden, die nicht den Einsatz einer bestimmten Managementapplikation erfordern. Viele Tipps arbeiten mit der Kommandozeile und mit dem VMware zugrunde liegenden Unix-System. Beschrieben wird allerdings die Installation von vCenter Server und Client sowie vConverter und es gibt ein eigenes Kapitel für Aufgaben, die sich per vCenter am besten lösen lassen. Die Kapitel sind logisch angeordnet. Nach der Installation kommen Rezepte zur Speicheranbindung und dem Networking. Während diese Tipps zwar für Einsteiger hilfreich sein können, werden die meisten Admins mit VMware Erfahrung keine Unterstützung mehr beim Anbinden eines iSCSI-Volumes benötigen.

Anders sieht es im Abschnitt "Command-Line Tools" aus. Wahrscheinlich wagt sich ein Großteil der Anwender normalerweise nicht über die GUI hinaus, doch Troy und Helmke zeigen, dass über die Befehlszeile einiges mit weniger Aufwand möglich ist. Gerade, wer über die Automatisierung von Admin-Aufgaben nachdenkt, findet hier interessante Hilfestellungen. Zum Teil sind auch mehrere Wege zum Ziel beschrieben, so kann NTP sowohl per vCenter als auch per CMD-Tool eingeschaltet werden. Seine Stärke zeigt das Buch immer dann, wenn es um Aufgaben geht, die man eigentlich schon immer einfacher lösen wollte, aber zu selten die Notwendigkeit dafür bestand. Spannend sind auch die Tipps im Bereich Sicherheit, wo der Leser beispielsweise erfährt, wie sich ein verloren gegangenes Root-Passwort zurücksetzen lässt.

Fazit: Auch versierte VMware-Admins finden im "VMware Cookbook" garantiert ein paar hilfreiche Tipps, Einsteiger bekommen durch die Rezepte Lust, die Tiefen von VMware auszuloten.

Elmar Török

Autoren:	Ryan Troy, Matthew Helmke
Verlag:	O'Reilly
Preis:	25,90 Euro
ISBN:	978-0-596-15725-8
Bewertung:	★★★★☆

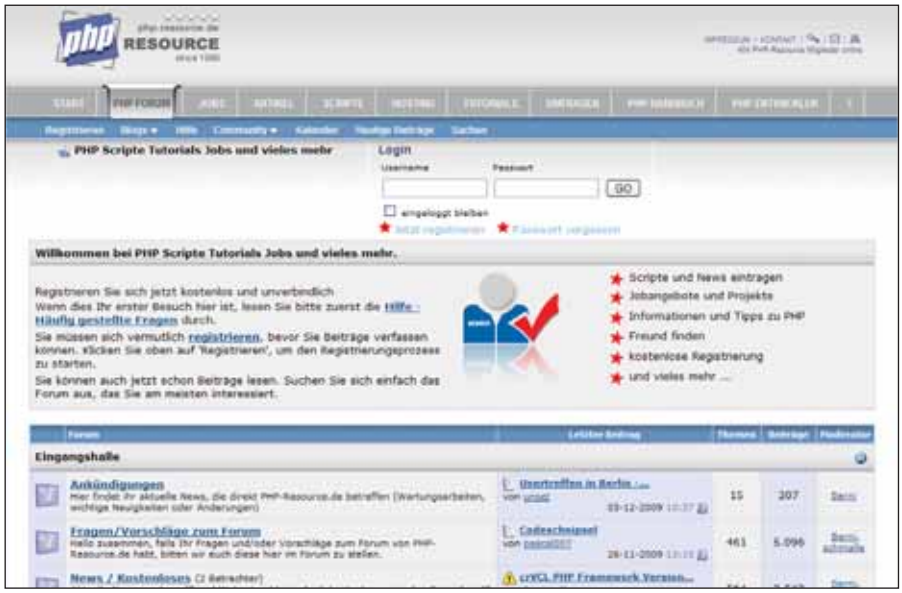
www.php-resource.de

Dynamische Sprachschule

Das Web ist schon lange kein statischer Dienst mehr, sondern lebt vom User-Input und aktiven Seiten. Bekannte Anwendungen sind etwa Foren, Suchfelder oder Feedback-Formulare. Die Sprache, die all dies möglich macht, ist PHP. Ursprünglich standen die drei Buchstaben für "Personal Home Page Tools". Heute bedeutet PHP "Hypertext Preprocessor". Wie dem auch sei – die Open Source-Software ist Standard im Webumfeld und prägt seit nunmehr knapp 15 Jahren die Online-Landschaft. Entwickelt wurde PHP, das übrigens nach wie vor auf der Programmiersprache C basiert, 1995 von Rasmus Lerdorf als Perl-Ersatz. Heute befindet sich die Sprache bereits in Version 5 im Einsatz, die Version 6 steht in den Startlöchern.

Für den System- und Netzwerkadministrator ist PHP im Alltag eher weniger von Bedeutung. Für Admins in kleineren Umgebungen hingegen schon – sind sie doch oft als "Mädchen für alles" auch für die unternehmenseigenen Webseiten zumindest mitverantwortlich. Hier sind Grundkenntnisse gefragt, um etwa kleinere Änderungen vorzunehmen oder ganze Elemente selbst zu entwerfen. Eine Anlaufstelle für PHP-Hilfe und Infos rund um die Sprache ist php-resource.de. Seit 1996, also nur ein Jahr nach der Entwicklung von PHP selbst, bietet die Seite nach eigenen Angaben Infos rund um die Websprache. Sie richtet sich dabei auch an Anfänger, die ihre ersten Schritte mit PHP unternehmen.

Web-Programmierer finden auf mehreren Wegen Unterstützung. Für den direkten Kontakt zu anderen Usern, die gegebenenfalls auch mehr Erfahrung mit PHP mitbringen, eignet sich das Forum. Darin werden in acht Kategorien Themen diskutiert von der eigenen Code-Entwicklung über Webmaster-Fragen hin zu Jobs und Projekten. Über 620.000 Beiträge haben die rund 50.000 User bereits erstellt. Nicht weniger bemerkenswert ist das PHP-Handbuch auf der Website. In neun Kapiteln finden Hilfesuchende alles Wissenswerte rund um PHP – angefangen bei den Grundlagen der Syntax hin zu den einzelnen Funktionen. Rund drei Dutzend Autoren haben an dem in HTML verfügbaren Online-Werk mitgewirkt. Knapp 3.500 fertige PHP-Skripte und eine Jobbörse runden die Webseite schließlich ab. *(dr)*



Im Forum von php-resource.de tummeln sich knapp 50.000 User, die bereits über 620.000 Beiträge erstellt haben

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:**

Dynamische Schutzsysteme für Webapplikationen

Die Verlagerung vieler Anwendungen ins Internet stellt die IT-Security vor Herausforderungen. Der Schutz von Webapplikationen ist in fast jedem Unternehmen ein großes Thema. Oft kommt dabei eine Web Application Firewall (WAF) zum Einsatz, die übermittelte Daten auf Herz und Nieren überprüft. Lesen Sie im Online-Artikel, wieso Sie das komplette Sicherheitsmanagement von nur einer Konsole durchführen sollten und warum dabei auch die Erfassung der Inhalte von Bildern, Audio- und Videostreams wichtig ist.
www.it-administrator.de/themen/sicherheit/fachartikel/74814.html

Zügiges Drucken in virtualisierten Umgebungen

Anbieter von virtuellen Desktop-Umgebungen haben viel Arbeit in die Beschleunigung der Übertragungsprotokolle gesteckt. Trotzdem gilt, dass Druckdaten in ihrer Größe durchaus mit Multimediainformationen konkurrieren können und den schmalen Weg zwischen gehosteten Desktop und Drucker zurücklegen müssen. Unser Online-Beitrag gibt eine Reihe von Praxistipps für den Druckalltag in virtuellen Umgebungen und erklärt, wie sich große Druckjobs verkleinern lassen und ab wann der Einsatz eines Printservers sinnvoll ist.
www.it-administrator.de/themen/server_client/fachartikel/74815.html

Thin Client-Umgebungen mit Sicherheitsvorteil

Server Based Computing bietet den Vorteil, dass viele IT-Risiken erst gar nicht auftreten: Datensicherung, Storage, System- und Datenwiederherstellung erfolgen zentral, auf den Clients ist dafür keine Software erforderlich. Auch dem internen Datendiebstahl lässt sich sehr einfach vorbeugen. Per Remote-Management lassen sich die USB-Ports gruppenbasiert oder individuell für bestimmte Peripheriegerätetypen sperren. Erfahren Sie in unserem Online-Artikel, wie Sie die Sicherheitsvorteile von Thin Client-Umgebungen erfolgreich für Ihre Infrastruktur nutzen.
www.it-administrator.de/themen/sicherheit/fachartikel/74816.html

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

»Die Motivation der Anwender ist eine wichtige Aufgabe«

Marcel Leibenath (31) betreut im Familienunternehmen Gessler als Administrator die IT-Infrastruktur. Das Unternehmen im hessischen Rodgau gehört zu den führenden Herstellern zentraler Sicherheitsbeleuchtungssysteme und Rettungszeichenleuchten. Die Produkte der Hessen finden sich in Flughäfen, Krankenhäusern oder Museen, wo sie beispielsweise die Notausgänge anzeigen.

Welche Ausbildung haben Sie gemacht?

Ich habe zunächst erfolgreich eine Ausbildung zum Elektroinstallateur absolviert. Daneben hatte ich aber immer schon eine Vorliebe für alle Themen rund um die IT.

Warum sind Sie IT-Administrator geworden?

Eigentlich bin ich mehr oder minder durch Zufall in diesen Aufgabenbereich hineingerutscht, da kein hauptamtlicher Administrator vorhanden war und ich nebenher sowieso schon die PC-Betreuung verantwortete.

Welche IT-Umgebung betreuen Sie?

Wir arbeiten derzeit mit sieben Hardware- und zwölf Software-Servern. Zusätzlich sind 55 Arbeitsplätze in das Netzwerk eingebunden. Ich verantworte die Datenbankadministration und die Anwendungsentwicklung ebenso wie das Customizing, das Reporting und das Prozessmanagement sowie Beschaffung und Installation von Hard- und Software. Hinzu kommen die Betreuung der Firmenwebsite, die Organisation und Betreuung unserer Messen, die Katalogentwicklung und Mitarbeiterschulung.

Welches Netzwerk- und Systemmanagement setzen Sie ein?

Wir arbeiten in einer Windows-Domäne und verwenden die hierfür verfügbaren integrierten Werkzeuge. Das Gleiche gilt für unsere Datenbanken unter Oracle 10g.

Welche Vorkehrungen treffen Sie, um Ihre Webserver und Webapplikationen zu schützen?

Zum einen nutzen wir als Firewall eine Watchguard x55e mit integriertem Virenscanner und Spam-Filter. Ein zweiter Virenscanner von Sophos ist lokal auf allen Rechnern installiert. Unser Content-Management-System für die Website haben wir mit kryptischen Passwörtern abgesichert, während unsere Firmeninterna auf einem von außen nicht erreichbaren Rechner liegen.

Geburtstag: 13.04.1978
Familienstand: verheiratet
Hobbys: Media Center-PCs, Fotos (leibenath.com), Standard-Tänze

Marcel Leibenath, IT-Administrator

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

Die größte Herausforderung ist es, täglich die Anwender dazu zu motivieren, alle verfügbaren Lösungen optimal und produktiv zu nutzen, damit die Kernprozesse des Unternehmens möglichst rationell abgewickelt werden können.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Auf der Agenda für die nächsten Wochen und Monate steht die Servervirtualisierung. Als Messebetreuer bereite ich unseren Auftritt auf der Fachmesse Light&Building 2010 vor.

Was macht Ihnen an Ihrem Job am meisten Spaß?

Das ist einmal die permanente Herausforderung, die sich aus dem Arbeitsalltag ergibt. Mir gefällt dabei die Vielseitigkeit, denn ich arbeite immer wieder auch im Außendienst. Ein Tag auf der Baustelle mit Latzhose kann sehr inspirierend sein. Genauso gerne vertrete ich aber auch unser Unternehmen auf der Messe in Anzug und Krawatte.

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

Die Systembetreuung gehört nicht unbedingt zu meinen Favoriten.

Was tun Sie für Ihre Fort- und Weiterbildung?

Fortbildung in Sachen IT läuft meist nach dem Prinzip "learning by doing". Ich informiere mich aber auch im Web und lese Fachzeitschriften oder Fachbücher. Daneben mache ich gerade ein Fernstudium zum Industriemeister Elektrotechnik.

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

Ein Anwender beschwerte sich telefonisch, dass sein PC nicht mehr laufe. Ich ging an den Arbeitsplatz, der zu dem Zeitpunkt verlassen war und betätigte die Tastatur. Der Rechner lief einwandfrei. Das Spiel wiederholte sich, bis sich herausstellte, dass er den Rechner immer mit seiner schnurlosen Maus startet. Und da waren schlichtweg nur die Batterien leer.

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

Durch die wachsende IT-Komplexität kann schnell der Überblick verloren gehen. Bei einer nicht ausgereiften Fehlerbehandlung oder bei fehlendem Monitoring können Fehler in Programmroutinen dann nicht mehr auffallen oder Systeme am Rand ihrer Leistungsfähigkeit laufen. Das zweite Thema ist das Schulen und Motivieren von Anwendern.

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 3/10 erscheint am 1. März 2010

Schwerpunktthema:

Rechenzentrumsausstattung

Im Test: Men & Mice-Suite zur DCHP- und IP-Adressverwaltung

Workshop: Remote-Administration mit UltraVNC

Systeme: 10-GBit-Ethernet im Netzwerk

Know-how: Switches für das Rechenzentrum

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

Unsere Ausgabe im **April** steht unter dem Schwerpunkt **Desktop-Virtualisierung**. In unserer Test-Rubrik nehmen wir VMware View 4 sowie XenDesktop 4 unter die Lupe. In einem unserer Workshops lesen Sie außerdem, wie Sie Red Hat Enterprise Virtualization Desktops virtualisieren.

Als Schwerpunkt im **Mai** folgt dann das Thema **Remote-Access, VPN und Gateway-Schutz**.

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), *Stellv. Chefredakteur*
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, Oliver Bendig, Thomas Drilling, Thomas Gronenwald, Jürgen Heyer, Thomas Hümmler, Thomas Joos, Robert Lindermeier, Sandro Lucifora, Elmar Török

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

Es gilt die Anzeigenpreisliste Nr. 7 vom 01.11.2009

LAC/2008

Produktion / Anzeigendisposition
Lightrays: Lorenz Mueller, Andreas Skrzypnik
dispo@it-administrator.de
Tel.: 089/4445408-88
Fax: 089/4445408-99

Druck
Konrad Triltsch
Print und digitale Medien GmbH
Johannes-Gutenberg-Straße 1-3
97199 Ochsenfurt-Hohestadt

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 eine Teilbeilage der Firma ppedv.

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 0210

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

LANCOM

. . . connecting your business

Made
in
Germany

Das beste WLAN aller Zeiten!

Die höchsten Datenraten aller Zeiten, die beste Funkfeldabdeckung, maximale Kompatibilität – 802.11n setzt neue Maßstäbe im Wireless LAN. Drinnen wie draußen.

Machen auch Sie Ihr Netz zukunftsfähig – und steigen Sie um auf die 802.11n Indoor & Outdoor Access Points, Clients und „11n-ready" WLAN-Controller von LANCOM.

Ob im kleinen Netz mit wenigen Access Points, im Controller-basierten WLAN mit Tausenden von Geräten, für den Hotspot-Betrieb oder im Freien: 802.11n WLAN von LANCOM sorgt überall für ungekannte Leistungsfähigkeit.

LANCOM OAP-310agn

CeBIT
HANNOVER
2.– 6.3.2010
HALLE 13
STAND C28
kostenlose Tickets
www.lancom.de/
cebit2010

LANCOM
Systems

www.lancom.de