IT-ADMINISTRATOR.DE

04/2009

€ 12,60 ISSN 1614-2888

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

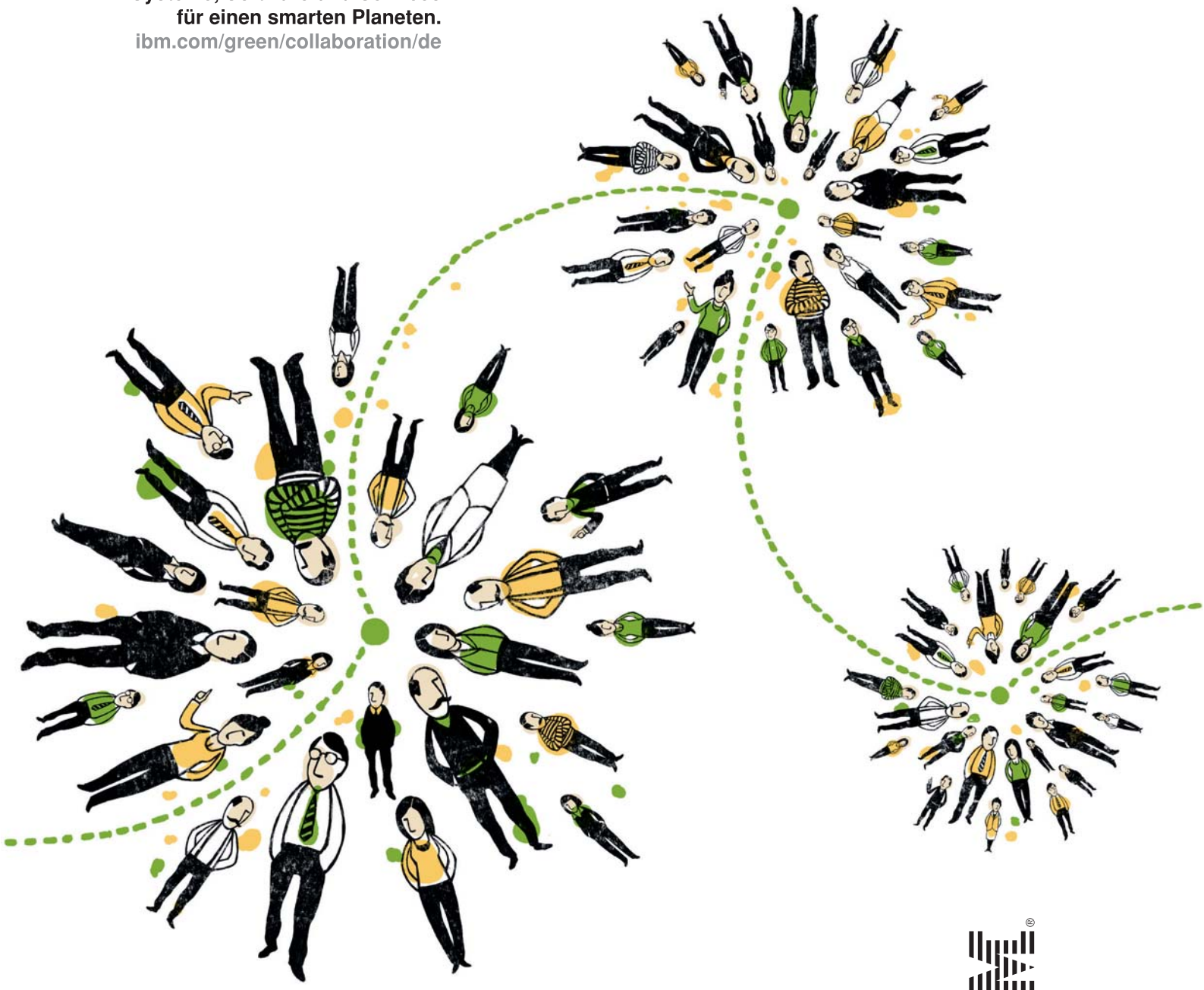
Diesen Monat und nur für Abonnenten: 16 Seiten extra.
Der iladNet Newsletter

E-Mailmanagement

WENIGER REISEN.
WENIGER EMISSIONEN.
WENIGER KOSTEN.

Wie weit würden Sie gehen, um Kosten und Emissionen zu senken? Nun, dank der IBM Lotus Collaboration Software müssen Sie nirgendwohin „gehen“. Denn mit Web-Konferenzen, Instant Messaging und Social Computing lässt Lotus Software Menschen schneller und effizienter zusammenarbeiten – unabhängig davon, wo sie sich gerade aufhalten.
So werden Entscheidungen wie im Flug getroffen, aber ganz ohne Jetlag, Kerosin und CO_2-Emissionen.

Systeme, Software und Services
für einen smarten Planeten.
ibm.com/green/collaboration/de



THINK

IBM, das IBM Logo und Lotus sind Marken oder eingetragene Marken der International Business Machines Corporation in den Vereinigten Staaten und/oder anderen Ländern. Andere Namen von Firmen, Produkten und Dienstleistungen können Marken oder eingetragene Marken ihrer jeweiligen Inhaber sein. © 2009 IBM Corporation. Alle Rechte vorbehalten.
O&M IBM IT 10/09

EDITORIAL

Blickwinkel

Liebe Leser,

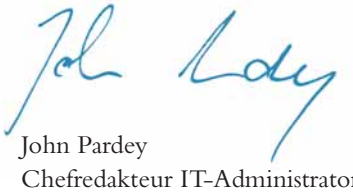
Ende vergangenen Jahres zeigte eine hierzulande unter Administratoren durchgeführte Umfrage, dass sich mittlerweile mehr als die Hälfte aller kleinen und mittelständischen Unternehmen mit regelmäßigen Ausfällen des E-Mailsystems konfrontiert sahen. Hauptursache hierfür war nach Auskunft der Befragten das steigende Datenvolumen, mit dem die Mailserver schwer zu kämpfen hätten. Neben den sowieso schon diffizilen Aufgaben des Admins rund um E-Mail, wie etwa Spam-Schutz oder Archivierung, rollt hier scheinbar eine weitere Problemwelle an.

Nun könnte sich leicht die Auffassung breit machen, die Anwender lieben ihr E-Mail und versenden fröhlich Multimedia-Inhalte an ellenlange Verteilerlisten. Doch genau das Gegenteil scheint der Fall: immer mehr Studien in Unternehmen zeigen, dass die geschäftliche E-Mailnutzung vielen Mitarbeitern zutiefst verhasst ist. Volle, aber unsortierte Posteingänge stehlen wertvolle Zeit ebenso wie die 17. Nachfrage (per E-Mail) des Chefs, ob jeder die Mail vom Freitag gelesen habe.

Und bemerkenswert ist auch die Toleranz von Geschäftsführern: das wichtigste Kommunikationsmittel des Unternehmens ist kriminell verseucht und taucht zu 95 Prozent völlig unverlangt auf. Die Aufbereitung und Aufbewahrung verschlingt Unsummen. Die Gefährdung der Zustellung geschäftsrelevanter E-Mailkommunikation kann für die Unternehmensleitung nichts anderes sein als komplett inakzeptabel.

Es zeigt sich, dass "E-Mailmanagement" keinesfalls Aufgabe des Administrators allein sein kann. Denn eine sauber aufgesetzte, sichere Mailinfrastruktur ist maximal die Grundlage der Lösung der angesprochenen Probleme. Vielmehr ist E-Mail heutzutage von solcher Bedeutung, dass Sie die Geschäftsleitung unbedingt mit ins Boot holen müssen, um beispielsweise interne Richtlinien zum Umgang mit E-Mail festzulegen. Oder sicherzustellen, dass jeder Anwender ein Mindestmaß an Schulung zu seinem Mailclient erhält.

Wenn Sie dies erreichen, haben Sie vielleicht auch mal wieder Zeit, Ihre E-Mails zu lesen. Ihr



John Pardey
Chefredakteur IT-Administrator

LANCOM

. . . connecting your business

Made
in
Germany

Das beste WLAN aller Zeiten!

Wireless LAN-Lösungen von LANCOM bereiten den Weg für eine neue Netzwerkdimension. Modernste Technologien, höchste Sicherheitslevels und herausragende Performance bieten Ihnen eine standortunabhängige Kommunikation mit ungeahnten Möglichkeiten. Drinnen wie draußen, in großen und in kleinen Netzen. Mit LANCOM vernetzen Sie Büros, Gebäude und mobile Mitarbeiter, leuchten Außengelände und Produktionsstätten aus. Kinderleicht, leistungsstark und sicher. Mit Bruttodatenraten bis 300 Mbit/s – bei voller Kompatibilität zu den gängigen 54 Mbit/s-Standards.

Professionelle **WLAN Access Points, Clients** und **Controller** vom deutschen Marktführer. Exzellenter Service, kostenlose Updates und Investitionsschutz inklusive.

INNOVATIONSPREIS-IT
KATEGORIESIEGER
2009
initiative mittelstand
STORAGE/NETZWERKE

LANCOM OAP-310agn

LANCOM
Systems

www.lancom.de

INHALT

IT-Administrator – Ausgabe April 2009

E-Mailmanagement

Einkaufsführer: Sichere E-Mailumgebungen

Unternehmen stellen unterschiedliche Anforderungen an ihre Kommunikationsinfrastrukturen. Immer mehr Firmen rüsten dabei auf und investieren in Insellösungen, die sicher sein und zugleich die Produktivität der Mitarbeiter fördern sollen. Doch steigt so auch die Komplexität der Systeme. Das Ergebnis: Höhere Ausgaben für Pflege und Wartung, unnötige Hindernisse im laufenden Betrieb und eine größere Fehlerquote. IT-Administrator zeigt auf, worauf es in kleinen, mittleren und großen Umgebungen ankommt.

Seite 28

Geschützter Zugang ins Unternehmensnetz

Die "Network Access Protection" ist ein neues Sicherheits-Feature im Windows Server 2008. Über diese Funktion können Unternehmen anhand entsprechender Richtlinien sicherstellen, dass nur solche Clients Zugang zum Firmennetz erhalten, die bestimmten Sicherheitskriterien genügen. Im dritten und abschließenden Teil unserer Workshopserie zeigen wir Ihnen, wie Sie Clients den sicheren Zugang zum Netzwerk ermöglichen.

Seite 45

Exchange-Umgebungen richtig dokumentieren

Das Projekt zur Einführung von Exchange ist abgeschlossen. Nun fehlt nur noch das Betriebshandbuch und das neue System kann in Betrieb gehen. Als Vorlage dient ein Musterbetriebshandbuch, das seit vielen Jahren die Basis aller firmeninternen Betriebshandbücher bildet. Bei dieser weit verbreiteten Vorgehensweise wird jedoch vergessen, dass ein Betriebshandbuch, das beispielsweise einmal dazu diente, den einzigen Windows 2000-Server der Firma zu beschreiben, für eine komplexe Exchange-Umgebung kaum die richtige Vorlage liefert. Worauf bei der Dokumentation einer Exchange-Umgebung zu achten ist und wie sich diese in die Gesamtdokumentation einordnen sollte, zeigt der Beitrag.

Seite 60

Turbo für den Spamfilter

Der Antispam-Spezialist **eleven** bietet seine Lösung **ExpurGate** nun in Version 3 an. Der Spamfilter arbeitet sowohl als Inhouse-Variante als auch als gehosteter Dienst beim Hersteller. Insbesondere bei der Geschwindigkeit hat der Anbieter einen Zahn zugelegt und die Durchsatzrate verzehnfacht. Daneben hat eleven den Funktionsumfang seiner Lösung erweitert. So bietet das Unternehmen jetzt einen vollständigen **Gateway-MTA** sowie die neue Version ihrer Outbound-Prüfung für ISPs an. Zudem stellt eXpurgate ab sofort spezielle Versionen für **SpamAssassin** und **Sendmail Milter** zur Verfügung, um die Einbindung in bestehende Infrastrukturen weiter zu erleichtern. Mit dem Gateway-MTA "eXpurgate.Edge" bietet der Hersteller Unternehmen dabei eine Komplettlösung zum Schutz ihrer E-Mail-Infrastruktur an. eXpurgate.Edge wird an der Schnittstelle zwischen Internet und internem Netzwerk installiert. Die integrierte E-Mailsicherheitslösung prüft die Nachrichten noch während der Einlieferung und ermöglicht die Abweisung als Spam oder Malware erkannter E-Mails noch vor der Annahme durch den E-Mail-Server. Mit Hilfe dieses **Reject-Modus** kann ein Großteil des E-Mail-Volumens bereits abgewiesen werden, bevor er die E-Mail-Infrastruktur des Unternehmens erreicht. Die Erkennungsrate liegt laut Anbieter bei deutlich über 99 Prozent und produziert keine False Positives bei individuellen E-Mails. Die False-Positive-Rate von unter 0,00001 Prozent sei zudem die niedrigste aller verfügbaren Anti-Spam-Lösungen. Version 3 ist ab sofort bei eleven als gehostete Variante im Einsatz und auch für die Inhouse-Nutzung verfügbar. Bei 200 Lizenzen kostet ExpurGate zwei Euro je Nutzer inklusive Virenschutz. *(dr)*

eleven: www.eleven.de

Das Astaro Security Gateway 625 schützt große Umgebungen vor Gefahren aus dem Web

Blick in den HTTPS-Traffic

Astaro bringt **Release 7.4** für seine Security-Gateway-Produkte **Astaro Security Gateway** (ASG), **Astaro Web Gateway** (AWG) and **Astaro Mail Gateway** (AMG) auf den Markt. Die Software enthält in ihrer neuen Version neben einem **HTTPS-Proxy**, **WAN-Link-Balancing**, **Site-to-Site SSL-VPN-Fähigkeiten** und **anonymisierten Reports** mehr als 200 weitere Neuerungen. So besteht mit dem HTTPS-Proxy nun auch die Möglichkeit, Applikationen zu überwachen, die ansonsten durch dieses verschlüsselte Protokoll die Sicherheitsrichtlinien umgehen können. Unternehmen können darüber hinaus mit **WAN-Link-Balancing** die Vorteile mehrerer Internetanbindungen ausnutzen. Diese Funktion sorgt mit einer One-Click-Konfiguration für eine automatische Lastverteilung und Ausfallsicherheit aller Internetverbindungen sowie für deren regelbasierte Priorisierung. Durch diese Regeln können auch spezifische Typen von Internetverkehr wie etwa Webtraffic einzelnen Verbindungen zugewiesen werden. Astaro erweitert mit der neuen Version zudem die integrierte SSL-VPN-Technologie. Damit lassen sich Site-to-Site-Verbindungen herstellen, mit denen über eine einfache Konfiguration Tunnel zwischen den Astaro-Gateways möglich sind. Parallel zu diesem Release bietet der Hersteller das neue Appliance-Flaggschiff **Astaro Security Gateway 625** mit einem Firewall-Durchsatz bis 10 GBit/s an. Für rund 23.500 Euro ist die High-End-Lösung verfügbar. *(dr)*

Astaro: www.astaro.de/unsere_produkte/produktueberblick

E-Mailsicherheit in der Wolke

Nach der Übernahme von **Ironport** nutzt **Cisco** nun die Technologie des Security-Herstellers für ein eigenes, **gehostetes Angebot**. Bekannt ist Ironport durch seine **E-Mail- und Websecurity-Appliances**. Diese sorgen in Unternehmensnetzen für eine abgesicherte Kommunikation mit der Außenwelt. Nun bringt die neue Ironport-Mutter Cisco diese Dienste "in the cloud". Mit der Kombination aus **präventiven Reputationsfiltern** und anschließender **Inhaltsanalyse** gewährleistet das System Spamschutz, Data Loss Prevention (DLP), Virenschutz sowie E-Mail-Authentifizierung und bietet darüber hinaus umfassende Reporting-Tools. Im Gegensatz zu anderen Anbietern von Hosted E-Mailsecurity muss die Infrastruktur dabei nicht mit anderen Kunden geteilt werden. Dies garantiere höchste Verfügbarkeit bei maximalem Schutz sensibler Daten. Kunden behalten außerdem die Kontrolle über die extern gehosteten Appliances durch einen zusätzlichen **Management-Zugang**. So können sie jederzeit eigenhändig auf **Echtzeitreports** zugreifen oder Konfigurationsänderungen vornehmen, ohne dafür Wartezeiten für Service-Tickets in Kauf nehmen zu müssen. Ab sofort ist der Service auf dem Markt verfügbar. Für 5.000 User und drei Jahre Laufzeit kostet das Komplettangebot 12 US-Dollar pro Nutzer und Jahr. *(dr)*

Ironport: www.ironport.com/de/

Selbstbedienung am Helpdesk

Aagon Consulting will mit **Version 3.6** seiner Clientmanagement-Suite **ACMP** die Prozesse im Bereich **Helpdesk** optimieren. Eine neue Webschnittstelle des Helpdesks von ACMP 3.6 hilft laut Anbieter der IT-Abteilung dabei, Benutzeranfragen noch effizienter abzuwickeln. Denn Benutzer müssen ab sofort ihre Anfragen nicht mehr per Telefon aufgeben, sondern können sie selbst über das neue Webinterface im Helpdesk-System eintragen. Dadurch haben Anwender einerseits die Möglichkeit, auch außerhalb der offiziellen Helpdesk-Zeiten ihre Anliegen vorzubringen. Gleichzeitig können sie sich über ihre Webbrowser jederzeit über den aktuellen Bearbeitungsstand ihrer Anfragen informieren und ihrer Anfrage gegebenenfalls weitere Informationen hinzufügen. Zudem erhalten Endbenutzer über die Webschnittstelle Zugang zu einem freigegebenen Bereich der **Knowledge-Base** des Helpdesks, in dem die IT-Abteilung Lösungen für häufig auftretende Probleme hinterlegen kann – beispielsweise zur Beseitigung eines Papierstaus in einem Drucker. Vorteil für Administratoren: Sie haben durch die Selbstbedienung der Benutzer mehr Zeit, um sich um die Lösung der angefragten Probleme zu kümmern. Die **Clientmanagement-Suite** unterstützt in Version 3.6 nun zudem neben Windows Server 2008 auch SQL Server 2008 von Microsoft. Ab Juni soll die neue Version erhältlich sein. Der Preis pro Lizenz richtet sich nach der Gesamtzahl der Arbeitsstationen. Bei 25 bis 99 PCs kostet eine Lizenz 53,50 Euro. *(dr)*

Mit Version 3.6 verfügt die Clientmanagement-Suite ACMP über ein verbessertes Helpdesk-System

Aagon: www.aagon.de

Drei Neue bei Netgear

Netgear präsentiert drei neue **Layer-2-Switches** im Rahmen der **ProSafe FSM-Produktlinie**. Jeder der drei neuen Switches, der **FSM726E**, der **FSM7226RS** und der **FSM7250RS**, bietet sowohl einen unterschiedlichen Grad an Portdichte als auch unterschiedliche Funktionalitäten, um den Anforderungen von Unternehmen mit über 200 simultanen Nutzern zu entsprechen. Die Modelle FSM7226RS und FSM7250RS sind **Managed 24-Port** beziehungsweise **48-Port Switches** mit Autosensing-fähigen 10/100 Ports und zwei Fibre-Channel-fähigen GBit-Ethernet-Ports. Daneben sorgen zwei **Hochgeschwindigkeits-Stacking-Ports** auf der Rückseite der Switches jeweils mit 5 GBit/s Vollduplex für die kritische Bandbreite, die für die Switch-to-Switch Kommunikation notwendig ist. Ein **statisches Routing** soll die Kommunikation zwischen VLANs und Netzwerksegmenten ermöglichen. Beim Modell FSM726E handelt es sich um einen 24-Port Managed Switch, der sämtliche Funktionen der RS-Modelle bietet, außer der Möglichkeit des Stackings und des statischen Routings. An Sicherheitsfunktionen bieten die Geräte eine **IEEE 802.1x Port-basierte Authentifizierung** sowie **Access Control List** (ACL). Eine **SSLv3-Unterstützung** und **Secure Shell (SSH)** sorgen zudem für Sicherheit bei der Administration der Switches. Ab sofort sind die Geräte auf dem Markt und kosten je nach Modell zwischen 251 Euro (FSM726E) und 629 Euro (FSM7250RS). *(dr)*

Netgear: www.netgear.de/Unternehmen/Switches/Managed/

Die neuen Managed Switches von Netgear richten sich an KMUs

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

Citrix bietet künftig eine kostenlose Variante der **XenServer Enterprise-Virtualisierung** an. Bislang kostet die Virtualisierungslösung rund 900 US-Dollar. Allerdings müssen die Nutzer dabei auf Bestandteile wie das Workflow Studio oder Storage Link zur Verteilung von virtuellem Arbeitsspeicher verzichten. Auch Support will Citrix für den kostenfreien Server nicht bieten. Inbegriffen sind dagegen der Hypervisor für Windows- und Linux-Gastsysteme, ein unbegrenztes Multi-Servermanagement, die Live-Migration sowie die Ressourcenverwaltung. Verfügbar ist zu Redaktionsschluss dieser Ausgabe die Vorabversion der Gratissoftware. *(dr)*

www.citrix.com/freexenserver

ubitexx will mit seiner Mobile Device Management-Lösung **ubi-Suite** künftig neben Windows Mobile auch andere wichtige mobile Plattformen unterstützen. Die Suite erlaubt das Remote-Management von Smartphones. Firmengeräte lassen sich dabei "over the air" entsprechend der Unternehmensvorgaben mit einem Sicherheitssetup, sicherem E-Mail-Push und Zugriff auf persönliche Daten (PIM) ausstatten. Ab Sommer 2009 sollen auch Clients für iPhone und Symbian sowie ein Connector zu Blackberry zur Verfügung stehen. *(dr)*

www.ubitexx.com

HOB bietet die Remote-Desktop-Software **RD VPN** in Version 1.3 an. Ein PPP-Tunnel erlaubt bei der SSL-VPN-Zugangslösung den vollen Netzwerkzugriff, wodurch Anwendern die Funktionalitäten eines IPSec-VPNs zur Verfügung stehen, ohne dass diese hierfür spezielle Clients installieren müssen. Vielmehr reicht ein Java-fähiger Browser auf den Client-Rechnern aus. In Version 1.3 hat der Hersteller seine Software nun um weitere Funktionen ergänzt sowie das Handling vereinfacht. Zu haben ist die VPN-Lösung für 20.000 Euro bei 100 Usern. *(dr)*

www.hob.de

Western Digital stellt mit dem **ShareSpace** ein NAS-System vor, das mit vier Festplatten bestückt werden kann. Dabei fassen die Harddisks der Serie "Caviar Green" des Herstellers jeweils 2 TByte und sollen besonders stromsparend arbeiten. Das Topmodell der Serie erreicht damit bis zu 8 TByte Speicherkapazität, sofern alle Platten zusammengeschaltet werden. Andernfalls lässt sich das Gerät in den RAID-Modi 1 und 5 benutzen, was für einen Schutz vor Datenverlust sorgt. Für die Nutzereinrichtung unterstützt das Gerät auch Active Directory-Umgebungen. Für rund 1.800 Euro ist die Lösung erhältlich. *(dr)*

www.westerndigital.com/de/products/Products.asp?DriveID=584

Der IP-KVM-Switch KN4132 von Aten verfügt über eine aufgehübschte Optik

Fernwartung auf Knopfdruck

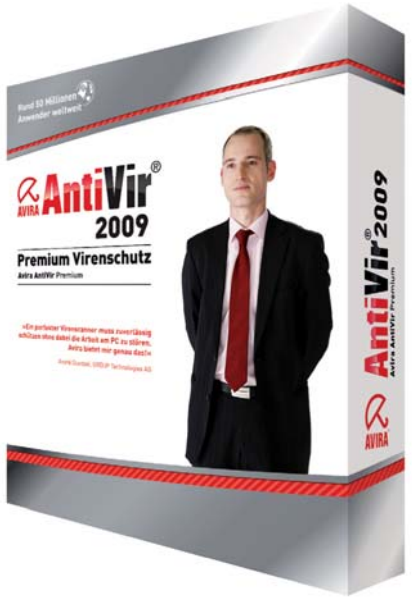
ATEN International erweitert sein Angebot für Unternehmen um drei neue **KVM Over the NET-Switches** der **ALTUSEN-Produktfamilie**. Die IP-basierten Cat 5 KVM-Geräte mit Remote-Management-Funktionalität ermöglichen in einer Kaskadenschaltung den sicheren Zugriff auf bis zu **256** beziehungsweise **512 lokale oder entfernte Server**. Die Variante KN4116 verfügt über 16 Ports und unterstützt einen lokalen sowie vier Remote-User. Die Modelle KN2132 und KN4132 dagegen bieten 32 Ports und erlauben jeweils einen lokalen sowie zwei beziehungsweise vier entfernte Anwender. Die neuen Switches ermöglichen dabei auch die **Steuerung der Stromversorgung** der Server aus der Ferne und **Out-of-band-Zugriff** auf Server bei heruntergefahrenem Netzwerk. Die Fernwartung erfolgt dabei über Web-Browser oder browserunabhängige Windows- oder Java-Applikationen, die eine direkte Verbindung zum KVM-Switch herstellen. Über die integrierte duale Netzwerkkarte (Dual Network Interface Card) lassen sich die Geräte redundant an das LAN anbinden und für einen dualen Betrieb konfigurieren. Fällt dabei die primäre LAN-Verbindung aus, übernimmt die sekundäre Karte automatisch und unterbrechungsfrei deren Funktion. Die KVM-Switches sind ab sofort erhältlich und kosten 3.695 Euro (KN2132), 4.995 Euro (KN4116) und 6.045 Euro (KN4132). *(dr)*

Aten: www.aten.com

Parallele Rechenleistung gegen Viren

Mit **Version 9** präsentiert **Avira** eine runderneuerte Fassung der Antiviren-Lösung **AntiVir**. Die Software ist in den Editionen "Personal", "Premium" und "Security Suite" erhältlich. In der neuen Version hat der Virenschutz nun eine **neue Oberfläche** erhalten und bietet eine laut Hersteller vereinfachte Benutzerführung. So nimmt nach der Installation ein Konfigurationsassistent den Benutzer an die Hand und hilft, schnell und einfach die Konfiguration anzupassen. Die Entwickler haben den Virenschutz so überarbeitet, dass der Anwender nicht nach jedem Fund zum weiteren Vorgehen befragt wird. Standardmäßig findet nun ein vollständiger Suchlauf statt, an dessen Ende der Anwender alle Schädlingsfunde in einer übersichtlichen Liste findet und von der aus er sie mit einem Mausklick von der Platte entfernen kann. Neben dieser sichtbaren Änderung hat Avira auch unter der Haube gearbeitet und den Scanner um bis zu **20 Prozent beschleunigt**. Dieser Geschwindigkeitsvorteil soll insbesondere Nutzern von **Multicore- und Multiprozessor-Systemen** zuteil werden. Administratoren können daneben Profile anlegen und Webseiten definieren, die unabhängig vom eingestellten Profil immer erlaubt oder stets verboten sind. Die neue Version ist ab sofort auf dem Markt. Eine Aktualisierung soll dabei auch über die automatischen Produktupdates möglich sein. In der Premium-Variante kostet die Einplatzlizenz inklusive einem Jahr Updates 19,95, wovon fünf Euro an die gemeinnützige Auerbach-Stiftung gehen, während Aviras Premium Security Suite 39,95 Euro kostet. *(dr)*

Avira: www.avira.de



Arbeitet nun schneller und übersichtlicher: AntiVir 9 von Avira

In eigener Sache

ShadowProtect-Software für 6.400 Euro zu gewinnen

In der April-Ausgabe verlost IT-Administrator für seine Leser zwei **IT-Editionen** von **Storage Craft ShadowProtect** im Wert von je **2.450 Euro**. Die Software ermöglicht es, von Windows-Servern zu einem exakt bestimmten Zeitpunkt **Abbilder** zu erstellen, ohne hierfür Software installieren oder das Zielsystem booten zu müssen. Damit eignet sich die Lösung etwa bei **Migrationen** oder vor geplanten **Anpassungen der Server**. Außerdem haben Sie die Chance, eine von zwei **Server-Editionen** im Wert von jeweils **629 Euro** sowie fünf **Desktop-Editionen** für je **56 Euro** zu gewinnen. Teilen Sie uns hiefür mit, welche Imaging-Tools Sie einsetzen und senden Sie Ihre Antwort zusammen mit Ihren Kontaktdaten an **redaktion@it-administrator.de** mit dem Betreff **ShadowProtect**. Einsendeschluss ist der 30. April 2009. *(dr)*

Storage Craft: www.storagecraft.eu/shadowprotect_it.html

1&1 WebHosting für Profis.

PCWELT 1. Platz MARKE DES JAHRES 08 Webhosting Imagestudie BA 2008

Mit mehr als 5 Millionen gehosteten Websites zählt 1&1 zu den größten Webhostern weltweit. Dafür gibt es viele gute Gründe: Höchste Datensicherheit, innovative Technik, eigene Hochleistungs-Rechenzentren mit umweltschonender Stromversorgung, kompetente Mitarbeiter, wertvolle Inklusive-Features, individueller Support und vieles mehr. Überzeugen Sie sich selbst! Denn unsere Top-Angebote gibt's jetzt zum halben Preis!

50 % RABATT

Angebot nur noch gültig bis 30.04.09!

DOMAINS

Ihre individuelle Internet-Adresse

Sichern Sie sich jetzt eine einprägsame Domain für Ihre Firma – wie z. B. www.meinfirmenname.biz. Sie können Ihren Wunschbegriff aus zahlreichen Domainendungen wählen.

.biz 0,99 €/Monat

Nur 0,99 €/Monat im 1. Jahr, danach supergünstige 1,99 €/Monat. Mindestvertragslaufzeit 12 Monate. Preise inklusive MwSt.

KEINE EINRICHTUNGS-GEBÜHR!

WEBHOSTING

Perfekte Leistung für Ihre Website

Zahlreiche Inklusivleistungen für Profis machen unsere WebHosting-Pakete so attraktiv. Wählen Sie aus vielen hochwertigen Komplett-Lösungen für jeden Anspruch.

1&1 HOMEPAGE BUSINESS

Mit dem 1&1 Homepage Business Paket bekommen Sie eine professionelle Lösung zum kleinen Preis.

6,99 €/Monat

Nutzen Sie 3 Inklusive-Domains, 2.000 MB Webspace, 5 MySQL-Datenbanken u.v.m.

Nur 6,99 €/Monat in den ersten 6 Monaten, danach supergünstige 14,99 €/Monat. Einmalige Einrichtungsgebühr 14,90 €. Mindestvertragslaufzeit 12 Monate. Preise inklusive MwSt.

VIRTUAL-SERVER

Server-Funktionalität zum kleinen Preis!

Die 1&1 Virtual-Server bieten vollen Root-Zugriff auf Ihr System und somit viele Vorteile eines Dedicated Servers – und das supergünstig!

1&1 VIRTUAL-SERVER XL

Ideal für große Foren, CMS, Wikis und Galerien. Nutzen Sie garantierte 512 MB Arbeitsspeicher,

9,99 €/Monat

2.000 GB Traffic sowie Inklusive-Features zur Programmierung. Plesk 9.0 ist bereits vorinstalliert.

Nur 9,99 €/Monat in den ersten 6 Monaten, danach supergünstige 19,99 €/Monat. Einmalige Einrichtungsgebühr 19,90 €. Mindestvertragslaufzeit 12 Monate. Preise inklusive MwSt.

MEMBER OF united internet

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

www.1und1.info

1&1

Neues Zuhause für Server

Mit den **PX Racks** stellt **Schäfer IT-Systems** die ersten Modelle einer neuen Generation von **Netzwerk- und Serverschränken** vor. Die Racks sind mit bis zu 400 Kilogramm belastbar. Sie verfügen über fest in die Rahmenkonstruktion integrierte Sockel und zwischen den Rahmen liegende Türen. Die geschlossenen Seitenteile und die perforierten Türen können wahlweise an allen vier Seiten montiert werden, letztere zudem mit wechselnden Anschlägen. Dadurch sind die Racks sehr vielseitig, zum Beispiel auch in Ecken, einsetzbar und gewährleisten dennoch eine uneingeschränkte Zugänglichkeit. Optional können die Racks auch mit außen aufliegenden Türen aus dem SP Rack-Programm des Herstellers ausgestattet werden. Die Seitenwände sind mit **Vorreibern und Schlössern** ausgestattet, um sie einfacher montieren zu können und eine sichere Befestigung zu gewährleisten. Die Dachmodule verfügen zudem über Ausbrüche für die **Lüftermontage** sowie über **Bürstenleisten** für die Einführung von Kabeln. Als Bodenmodule können bei Bedarf die im SP Rack-Programm erhältlichen Modelle eingesetzt werden. Die neuen PX Racks, die Schäfers PE Rack-Programm im Laufe dieses Jahres ablösen werden, bietet der Hersteller in acht verschiedenen Abmessungen, mit 25 und 43 Höheneinheiten (HE), 800 und 1000 Millimetern Tiefe und 600 und 800 Millimetern Breite, an. Das Modell mit den Standardabmessungen 800 x 2000 x 800 Millimeter soll dann bereits ab 350 Euro erhältlich sein. *(dr)*

Die neuen PX Racks von Schäfer tragen bis zu 400 kg

Schäfer IT-Systems: www.schaefer-it-systems.de

Schutz vor Datenabfluss dank Sniffer

Die **Kaspersky-Schwester InfoWatch** ist mit ihren **Data-Loss-Prevention-Produkten** nun auch auf dem deutschen Markt präsent. Dabei bietet das Unternehmen mit dem **Traffic Monitor 3.2** unter anderem die neueste Generation seines Security-Werkzeugs an. Die Software ermöglicht, ausgehende Mail-, Web- und Instant Messaging-Daten auf sensitive Informationen zu prüfen. Hierfür arbeitet das Tool entweder als **Sniffer** oder als **transparenter Proxy**. So lässt sich Netztraffic des Unternehmens abfangen und nachträglich analysieren. Der Sniffer erhält die Daten, erstellt dabei eine Kopie des Datenverkehrs und reicht diese an einen externen Speicher weiter. Somit wirkt sich die Schutzlösung nicht negativ auf die Performance des Unternehmensnetzwerks aus. Daneben soll die Software **Device Monitor** als **Portblocker** verhindern, dass Mitarbeiter vertrauliche Daten über externe Speichermedien wie USB-Sticks aus dem Unternehmen schleusen. Erhältlich sind die Produkte aus Russland ab sofort. Der Traffic Monitor kostet für 250 User 22.500 Euro, während der Device Monitor für 11.250 Euro zu haben ist. *(dr)*

InfoWatch: www.infowatch.ru/de/

Migration von Linux auf Mac

Apple stellt die Migrationssoftware **Linux2Mac** vor, die es erlaubt, Linux-Rechner automatisiert in Mac-Computer **umzuwandeln**. Das Tool richtet sich damit an künftige Mac-User, die jedoch bereits ein voll eingerichtetes Linux-System nutzen. Dabei kommt der Apple-Software die Tatsache zugute, dass der Kernel in Mac OS X dem **Linux-Kernel** ähnelt. Unterstützt werden bislang Distributionen von **Suse, RedHat und Debian**. Nach dem Systemstart über eine **Boot-CD** übernimmt das Tool alle relevanten Systemeinstellungen sowie die persönlichen Dateien der User. Sollten sich Nicht-Mac-fähige **Applikationen** auf dem Rechner befinden, sucht Linux2Mac automatisch nach passenden Alternativen im Netz und schlägt diese dem Anwender vor. Anschließend wandelt die Software die Festplattenpartitionen um und tauscht dabei das zugrundeliegende Betriebssystem aus. Nach einem Neustart steht den Nutzern dann ein voll funktionsfähiger, Intel-basierter Mac-Rechner zur Verfügung. Sogar die zuvor angelegten Icons, das Startmenü sowie das Desktop-Hintergrundbild finden sich nach der Migration wieder, sofern zuvor die Linux-Desktops **KDE** oder **Gnome** genutzt wurden. Offen ließ Apple die Frage, ob auch eine Windows-Version des Tools geplant ist. Am 1. April 2018 soll Linux2Mac auf den Markt kommen. *(dr)*

Linux2Mac: http://de.wikipedia.org/wiki/Aprilscherz

1&1 Root-Server für Profi-Sparer.

DEDICATED SERVER

Ein eigener Root-Server zum unschlagbar günstigen Spar-Preis!

Voller Root-Zugriff unter Linux, inklusive Plesk 9.0, der idealen Lösung für die Verwaltung der eigenen Domains, Mail-Postfächer und Anwendungen.

1&1 ROOT-SERVER S64

49,– €/Monat

Mindestvertragslaufzeit 24 Monate. Preise inkl. MwSt.

KEINE EINRICHTUNGS-GEBÜHR!

AMD Athlon™ X2 64

DAUERHAFT SUPERGÜNSTIG!

1&1 Root-Server S64:

- AMD Athlon™ X2 3800+ Dual-Core Prozessor
- 2,0 GHz
- 1.024 MB Arbeitsspeicher
- 2 x 160 GB Festplatte
- Software RAID 1
- 1 Domain inklusive (.at, .biz, .com, .de, .eu, .info, .name, .net, .org)
- 1&1 Firewall
- 1&1 Recovery-Tool
- 160 GB FTP-Backup
- Plesk 9.0 vorinstalliert

Weitere günstige Server-Angebote finden Sie im Internet.

RECS Quality Standard

Übrigens: Als erster deutscher Webhoster bezieht 1&1 ausschließlich Strom aus erneuerbaren Quellen und spart so bis zu 30.000 Tonnen CO_2 pro Jahr!

MEMBER OF united internet

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

www.1und1.info

1&1

IT-Defense, 11. bis 13. Februar 2009, Potsdam

Mit Sicherheit unsicher

von Daniel Richey

Das Publikum war so bunt gemischt wie die Redner auf der siebten IT-Defense in Potsdam. So fanden sich in den Reihen der rund 200 Teilnehmer unter anderem IT-Verantwortliche aus kleineren und mittelständischen Unternehmen, Sicherheitsbeauftragte von Service Providern, Spezialisten staatlicher Behörden sowie Programmierer und Hacker. Sie alle einte das Thema der Vortragsveranstaltung: die IT-Sicherheit. IT-Administrator war für Sie vor Ort.

Hinter dem Rednerpult konnte der Veranstalter der IT-Defense, der IT-Sicherheitsdienstleister Cirosec, hochkarätige Redner versammeln. Andrew Cushman, unter anderem verantwortlich für die monatlichen Patches bei Microsoft, gab beispielsweise einen Einblick in die Arbeitsweise des Microsoft Security Response Center und zeichnete die Sicherheitstrends der Zukunft auf.

Andrew Cushman führte die Teilnehmer in die Arbeit des Security Response Center ein

Sicherheit bei Microsoft

Dass er einen der besten Jobs der Welt habe, daran ließ Andrew Cushman als Chef des Microsoft-Sicherheitsteams keinen Zweifel. Dabei sollte es nach seinen eigenen Worten eigentlich eher Pech sein, in Redmond für das Thema IT-Sicherheit verantwortlich zu sein. Nur zu oft wird der Software-Hersteller für seine scheinbar fehlende Sicherheit gescholten. Doch immerhin gibt es bei Microsoft, im Gegensatz zu anderen Herstellern, ein zentrales Team für Sicherheitsrichtlinien, an dem kein Produkt vorbeikommt und das universalgültige Vorgaben machen kann. Seit zehn Jahren will das Response Center so für mehr Sicherheit sorgen.

Dass das Unternehmen nicht alleine gegen unzählige Löcher und immer organisiertere Online-Kriminelle ankommt, hat man in Redmond längst erkannt. Und so bezeichnete auch Cushman die Gefahren als so schwerwiegend, dass ein Hersteller alleine nur auf verlorenem Posten kämpfen könne. Eine Sicherheitspartnerschaft müsse also her. Angesichts der Tatsache, dass es mehr Schwachstellen denn je in Software gibt und diese immer schneller und professioneller ausgenutzt würden, kein überraschender Appell.

So stellt das "Active Protection Program" monatliche Schwachstellen-Informationen für kommerzielle Anbieter von Sicherheitssoftware bereit. Damit sollen die Hersteller einen Vorsprung vor den Hackern bekommen, die natürlich ebenfalls die veröffentlichen Patches analysieren und ihre Exploits darauf schreiben. Insgesamt sei die Entscheidung Microsoft nicht leicht gefallen, bestehe schließlich ein Risiko, dass die Informationen in die falschen Hände fallen könnten. Doch die Vorteile überwiegen laut Cushman. Die Voraussetzungen für eine Teilnahme an dem Programm: Ein unterzeichnetes NDA-Abkommen, der Partner muss Sicherheitslösungen für Microsoft-Produkte herstellen und dabei mehr als 10.000 User bedienen. Schließlich darf der Partner im Wesentlichen keine Produkte verkaufen, die für Angriffe auf Microsoft-Software dienen.

Dem Sicherheitsteam bei Microsoft sei dabei durchaus bewusst, dass es nie alle Schwachstellen finden könne. Daher sollen zunehmend grundlegende Sicherheitsmechanismen vor Exploits schützen - etwa in Form des bereits von Windows XP und diversen Prozessoren bekannten Puffer-Überlaufschutzes. Ein anderer, grundlegender Ansatz sei es außerdem, die Kosten für illegale Aktivitäten zu erhöhen und Angreifern sogar legitime Arbeits- und Geschäftsmöglichkeiten zu geben. Wie dies genau geschehen soll, führte Cushman jedoch nicht aus.

iSCSI – neue Technik, alte Fehler

In die technischen Details stieg Himanshu Dwivedi, Mitbegründer der IT-Sicherheitsfirma iSEC in Kalifornien, beim Thema iSCSI ein. Das Protokoll erlaubt es, Festplatten über das Netzwerk wie lokale Laufwerke bereitzustellen. Doch es scheint so, als hätte die Industrie nicht aus den Sicherheitsfehlern der Vergangenheit gelernt und so wartet auch iSCSI mit so einigen Fallstricken auf. Das Hauptproblem: Die Identifizierung findet alleine anhand des Clientnamens statt. Sollte ein Angreifer nicht durch bloßes Raten auf diesen Anmeldenamen kommen, genügt ein Mitsniffen im lokalen Netzwerk. Grundsätzlich fließt die iSCSI-Kommunikation nämlich unverschlüsselt durch das LAN. Spezielle Tools sind übrigens nicht dafür notwendig, dem eigenen iSCSI-Client einen anderen Namen zu verpassen - dies geschieht einfach über die GUI der entsprechenden Applikation und stellt ein sogar ausdrücklich erwünschtes Feature dar.

Eine weiterführende Authentifizierung ist, so Dwivedi, üblicherweise deaktiviert. Und sollte sie doch einmal abgefragt werden, biete das CHAP-Protokoll mit MD5 keinen besonders verlässlichen Schutz. Zum einen ist das Hash-Verfahren bereits durch seine etwas zu kurz geratene Schlüssellänge in die Kritik geraten und gilt als nicht mehr zeitgemäß. Andererseits würden laut Dwivedi besonders für Storage verantwortliche Administratoren in der Regel eher schwache Passwörter verwenden, die sich so leicht brute-forcen ließen. Für mehr Sicherheit könnten hingegen IPSec, Integritätschecks sowie Kerberos sorgen.

Vertrauenswürdige Rechner

Es ist ein Baustein, der zwar in zahlreichen Mainboards sitzt, aber dennoch eher wenig Beachtung findet: Das "Trusted Platform Module", kurz TPM. Der kleine kryptografische Chip ist Teil des Trusted Computing und arbeitet mit einem Public-Private-Key-Verfahren. Dr. Christoph Wegener, Inhaber von wecon.it-consulting, gab den interessierten Zuhörern einen Einblick in den Aufbau und die Funktionsweise dieser vermeintlich sicheren Architektur.

Ein Anwendungsfall für TPM stellt das sichere Booten von Rechnern dar. So lässt sich die Plattform beim Bootprozess nicht manipulieren. Bei einem "Trusted Boot" beziehungsweise "Secure Boot" wird allerdings nur geprüft, ob das System noch die zuvor überprüften und genehmigten Soft- und Hardware-Komponenten besitzt - sollte dies nicht der Fall sein, schreibt es der Chip in sein Log und führt gegebenenfalls weitere Aktionen aus. Dieser Standard ist laut Wegener jedoch nach wie vor nicht implementiert. Auch stelle sich die Frage, wer bei Update-Prozessen etwa zum Patch-Day die neuen Werte vermisst und diesen vor allem vertraut.

Ein weiteres Anwendungsbeispiel ist Schutz einer Root-CA mit TPM. Schließlich soll niemand den Zertifizierungsserver stehlen können und dann den privaten Schlüssel extrahieren dürfen. Eine Besonderheit des TPM-Chips ist nämlich, dass dieser quasi Schlüssel nochmals verschlüsseln kann und damit an die Hardware-Plattform bindet. So wird der Root CA-Key im TPM generiert und mit dessen "Storage Root Key" nochmals verschlüsselt. Allerdings ist dieser Verschlüsselungsprozess relativ langsam, weshalb er sich nicht zum direkten Sichern von größeren Datenmengen eignet.

Denkbar ist dieses Szenario auch mit AES-Schlüsseln. Dieser, sprich eine 256-Bit-Zufallszahl, werden im TPM erzeugt. Dann wird eine Datei mit openSSL verschlüsselt und mit dem TPM ein RSA-Objekt erzeugt. Der AES-Schlüssel wird dann mit dem RSA-Objekt geschützt, das RSA-Objekt wiederum mit dem SRK (Storage Root Key). Damit ist die Verschlüsselung an die Plattform gebunden, da das TPM benötigt wird. Doch hat laut Wegener auch das TPM-Verfahren einige Schwachstellen. Zum einen bestehe die Gefahr, dass der Chip seine Funktion einstellt und damit die gesicherten Daten nicht mehr wiederherstellbar sind. Würde nun der AES-Key zur Sicherheit auf einem separaten System gespeichert, führe dies die gesamte Prozedur ad absurdum. Auch setzen oft die Hardware-Hersteller den vertraulichen internen Schlüssel und nicht die Nutzer selbst. Damit könnten die Anbieter Nachschlüssel besitzen.

Prinzipiell sei es möglich, mit Zugang zur Hardware alle Sicherheitsfunktionen außer Kraft zu setzen. Auch TPM lasse sich eventuell so austricksen. Ein Problem stellt laut Wegener zudem die unzureichende Kryptographie dar. So verwendet die Plattform lediglich 2.048 Bit-Schlüsel und nutzt SHA-1. TPM sei zudem nicht flashbar, daher auch nicht aktualisierbar und auch Migrations- und Backupmechanismen fehlten bislang. Grundsätzlich biete TPM daher interessante Ansätze und der Standard müsse weiter vorangebracht werden. Offene Fragen gelte es allerdings zu klären. Besonders aus Unternehmenssicht sei das Schlüsselmanagement ein bedeutendes Thema.

Fazit

Auch 2009 lockte die IT-Defense Zuhörer aus allen Teilen Deutschlands mit fachkundigen und hochkarätigen Referenten. Dass die IT-Sicherheit ein weites Feld ist, bewiesen etwa auch Vorträge zum RDFID-Hacking oder dem Border Gateway Protocol. Den Besuchern hat es sicher nicht geschadet, Security-Themen auch einmal außerhalb der eigenen Verantwortung zu betrachten und so über den eigenen Tellerrand zu blicken.

Im Test: Kerio MailServer 6.6

Es geht auch einfach

von Sandro Lucifora

Als One-Click-Lösung – installieren, konfigurieren, fertig – bietet Kerio in der sechsten Generation den E-Mail- und Groupware-Server "Kerio MailServer 6.6" an. In der aktuellen Version wurde der Server um ansehnliche Team-Managment-Funktionen und die Anbindung an die mobile Welt erweitert. Ob die Exchange-Alternative hält, was der Hersteller verspricht, fanden wir in einem Praxistest heraus. Besonders die einfache Installation überzeugt.

Quasi unbemerkt von der Windows- und Linux-Welt hat sich unter Apple der Kerio MailServer bis zur Version 6.6 entwickelt und ist mittlerweile auch unter Windows und Linux im Einsatz. Dabei stellt die Software geringste Anforderungen an die Hardware. Die klassische Zielgruppe des MailServer sind Firmen mit bis zu 150 Usern. Bis zu 1.000 Anwender sind maximal möglich, doch ist das wohl eher die Ausnahme. Unter Windows ist der Betrieb eines Active Directory dabei keine Pflicht, wird von uns jedoch für die gute Integration in die Netzwerk-Welt des Unternehmens sehr empfohlen. Die Groupware-Lösung arbeitet auch losgelöst von zentralen User-Verwaltungen, was die Konfiguration jedoch unnötig aufwändig macht – die Entscheidung liegt bei Ihnen.

Im Test konzentrierten wir uns auf die Windows-Variante und installierten die Software unter Windows 2003 Server. Auf einem separaten System lieferte ein Small Business Server das Active Directory und stellte die Basis für die Migration der Exchange-Daten zum Kerio MailServer dar. An dieser Stelle muss noch erwähnt werden, dass Kerio auch mit dem Apple Open Directory zusammenarbeitet. Da der Hersteller auf ein eigenes Frontend verzichtet, diente uns als Client Microsoft Outlook 2003. Dass Kerio auf bestehende Client-Lösungen zurückgreift, ist grundsätzlich zu begrüßen, da der Anwender weiter mit seiner gewohnten Umgebung arbeiten kann. Dabei kommt jede Software in Frage, die IMAP-Postfächer unterstützt – jedoch steht nur mit Outlook der volle Groupware-Funktionsumfang wie Kalender und Aufgaben zur Verfügung.

Ein Klick und los

Der Hersteller verspricht, dass die Installation schnell und leicht vonstattengeht und das System in kürzester Zeit einsatzbereit ist. Während der Installation auf unserem Server wurden zur Grundeinrichtung die Hauptdomain für den E-Mail-Verkehr sowie die Anmeldedaten für

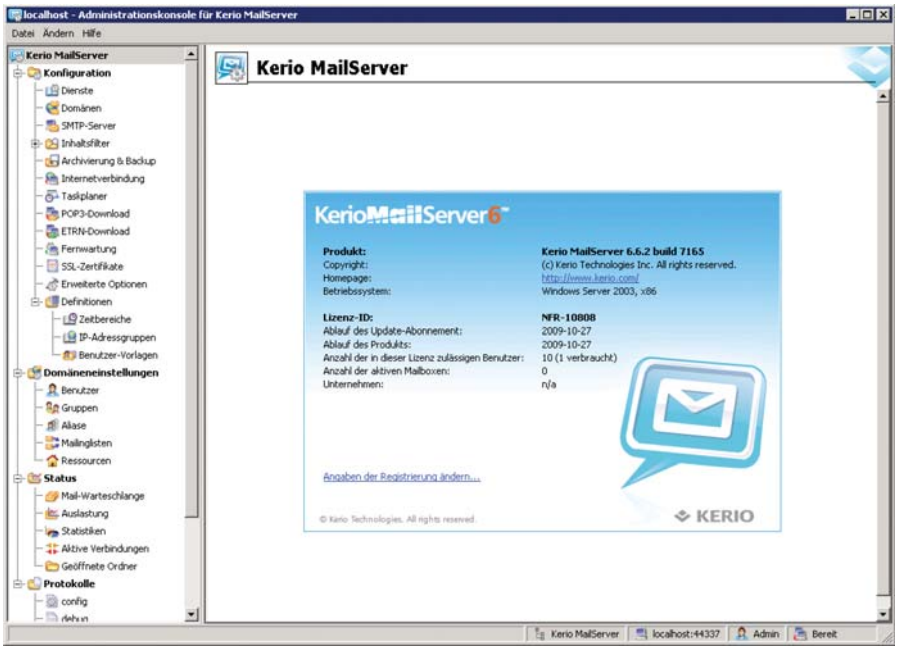


Bild 1: Klar strukturiert: Die Oberfläche zeigt sich aufgeräumt und übersichtlich

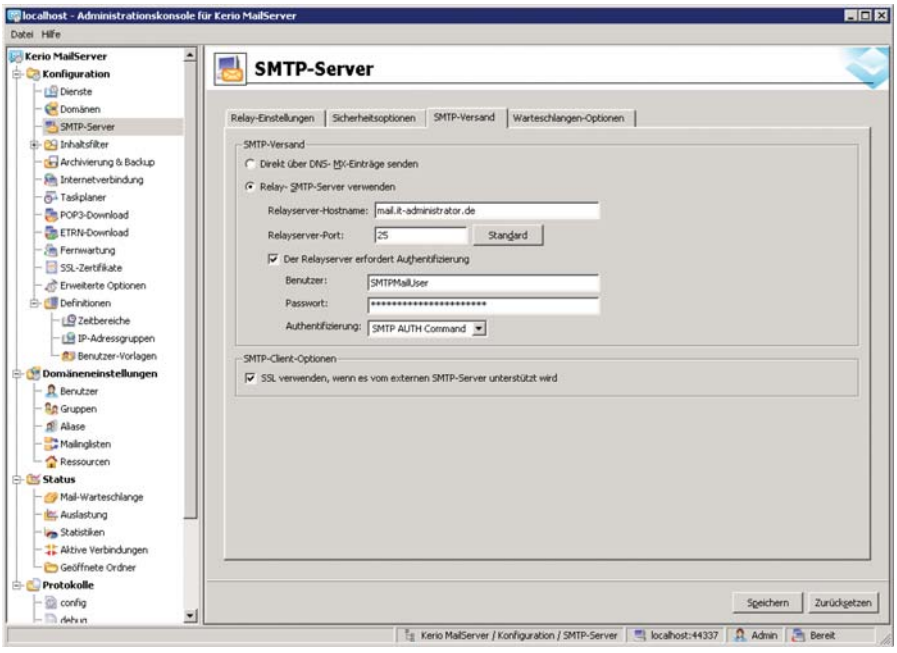


Bild 2: Das Einrichten des Relay-SMTP-Servers ist schnell erledigt

den Administrator abgefragt. Leider haben wir keinen Weg gefunden, den Eintrag der Domain im Nachhinein zu ändern. Schlecht, wenn sich im Laufe der Zeit die Domäne ändert. Es empfiehlt sich, das Datenverzeichnis möglichst auf einer separaten Partition abzulegen. Da der MailServer ohne Datenbank auskommt, werden alle Daten auf Dateiebene in einzelnen Dateien gespeichert.

Bis hierhin können wir schon mal das Versprechen der einfachen Installation bestätigen. Nach der Installation folgt das Einrichten über die mitgelieferte Administrations-Konsole. Ein Vorteil dabei ist, dass die Konsole remote auf den Server zugreifen und so auch auf dem Arbeitsplatz des Administrators installiert sein kann.

Konfiguration schnell erledigt

Nachdem der MailServer seine Dienste gestartet hat, gilt es das System einzurichten. Direkt fiel uns in der Liste der Dienste auf, dass der HTTP-Dienst nicht gestartet wurde. Die Ursache war schnell gefunden: Auf unserem Server lief der IIS – und zwei Dienste können schlichtweg nicht auf demselben Port verbunden werden. Da wir den IIS nicht beenden wollten, galt es den Port 80 des Kerio-WebServer zu ändern. Das erfolgte recht einfach über die Bearbeitung des Kerio-HTTP-Dienstes. Wir stellten hier Port 8080 ein, der dann beim Aufruf des WebMail-Clients, auf den wir später noch zu sprechen kommen, mit angegeben werden musste.

Ist die externe IP-Adresse des Kerio MailServers nicht als MX-Record unter der benutzten Domain hinterlegt, sollten Sie den SMTP-Versand über einen externen Relay-Server konfigurieren. Das dient der Sicherheit, damit Ihre E-Mails zukünftig nicht von Spam-Filtern geblockt werden. Diese prüfen mittlerweile sehr oft, ob die IP-Adresse des sendenden SMTP-Servers auch der Adresse entspricht, die im DNS der Domain als solche eingetragen ist. Stimmen die Werte nicht überein, geht ein Spam-Filter von einer unerlaubten Verwendung der Absender-Domain aus. Die Konfiguration des Relay-Servers findet über den Menüpunkt "Konfiguration / SMTP-Server / SMTP-Versand" statt.

Über die Relay-Einstellungen im selben Menü lässt sich auch konfigurieren, ob der Kerio MailServer als Relay-Server für andere berechtigte User dienen soll und wie sich diese für den Mailversand authentifizieren müssen. Einige Sicherheitsoptionen empfehlen wir direkt von Anfang an einzurichten. Dazu gehört die Beschränkung der maximalen Anzahl von Nachrichten pro Stunde von einer IP-Adresse. Dies stellt sicher, dass der MailServer nicht für einen unerlaubten Massenversand missbraucht wird. Die maximale Anzahl unbekannter Empfänger schützt den Server vor einer Harvest-Attacke. Darunter ist zu verstehen, dass Spammer an jeden auch nur erdenklichen Empfänger einer Domain E-Mails versenden, in der Hoffung dabei auch existierende E-Mailadressen zu erreichen. Das Blockieren der Absender-Domains, die nicht über einen DNS aufgelöst werden, schützt vor dem Empfang von fiktiven Absendern. Die integrierten Inhaltsfilter für Spam, Antivirus – sofern in der Lizenz enthalten – und die der Mailanhänge lassen sich im Laufe

Systemanforderungen

Server

Windows 2003 (SP1, 32 Bit)
Windows XP (SP2 oder SP1, 32 Bit)
WIndows 2000 (SP4)

Red Hat Linux
Red Hat Enterprise Linux 3 / 4
Fedora Core 4 (32 Bit)
Fedora Core 5 (32 Bit)
SUSE Linux 10.0 und 10.1 (32 Bit)

Mac OS X 10.3 Panther
Mac OS X 10.4 Tiger

Groupware-Clients

Outlook Connector arbeitet nur mit den folgenden Microsoft Outlook-Clients zusammen:

Microsoft Outlook 2003 (SP2), Outlook XP (SP3) und Outlook 2000 (SP3)

Microsoft Entourage benötigt keine zusätzliche Software auf dem Client. Die folgenden Versionen von Entourage werden unterstützt:

Microsoft Entourage X
Microsoft Entourage 2004 SP2 (11.2.3)

Mobile Endgeräte

Windows Mobile 2003 SE, 2003, 2002 und 5.0 Pocket PC, Pocket PC Phone Edition
Palm Treo 750v, 700p/w, 650

der Zeit verfeinern. Die Grundeinstellungen sind für den Anfang gut gewählt und müssen nicht verändert werden. Auf die Grundkonfiguration folgt die Einrichtung der User.

Benutzerverwaltung – Vorteil Active Directory

Bei der Einrichtung des Servers lässt sich Zeit sparen, sofern er in einer Active Directory-Umgebung (AD)zum Einsatz kommt. Das wird spätestens bei der Einrichtung der Benutzer deutlich. Insgesamt gibt es drei Wege, die zu einem Userstamm führen: Der MailServer wird direkt an die AD-Domäne angebunden. Der Vorteil liegt darin, dass die User nur noch an einer Stelle zu verwalten sind. Alternativ werden nur die Benutzer aus dem AD importiert. Das ist sinnvoll, wenn nicht alle AD-User eine Mailbox benötigen. Schließlich werden die Benutzer einzeln angelegt und im Mailserver verwaltet. Für eine Active Directory-Integration ist es zusätzlich notwendig, auf dem AD-Server die Kerio Active Directory Extensions zu installieren. Nur durch diese kann der MailServer auf die AD-Authentifizierung zugreifen.

Nach dem Import oder der Anbindung an die Domäne gilt es, noch mindestens eine Nachjustierung vorzunehmen: Die E-Mailadresse. Kerio MailServer bildet aus der Domain und dem Login-Namen des Active Directory automatisch die E-Mailadresse. In unserem Fall war diese jedoch nicht mit der öffentlichen Mailadresse gleichzusetzen. Daher mussten wir in die Konfiguration für E-Mails gehen und die externe Adresse als weiteren Eintrag hinzufügen. Weiterhin lassen sich der maximale Speicherplatz festlegen und bei Bedarf Weiterleitungen einrichten.

E-Mailgruppen mit Einschränkungen

Der Empfang von Nachrichten an allgemeine E-Mailadressen wie "info" oder "verkauf" läuft über E-Mailgruppen ab. Jeder Gruppe können beliebig viele eigene E-Mailaliase und User zugeordnet werden. An diese User werden dann die eingehenden E-Mails verteilt. Ein großes Manko der Funktion: Jede Gruppe entspricht einem zu lizenzierenden Benutzer, obwohl es sich hierbei um nichts anderes als eine Weiterleitung an Postfächer handelt. Zudem antworten die Benutzer dann mit ihrer persönlichen E-Mailadresse und nicht mit dem Gruppenabsender. Die Antwortmail liegt dann im Postausgang des Benutzers. Der Sinn und Zweck eines Gruppenpostfachs wurde hier nicht bis zum Ende umgesetzt.

Mailinglisten und Ressourcen

Ein weiteres Goodie des Servers sind die Mailinglisten. Diese lassen sich wie üblich nutzen und auch per NNTP abfragen. Neben der Konfiguration, wie und ob eine aktive Anmeldung der User erlaubt ist und die Festlegung der Moderatoren, können sowohl lokal eingerichtete Benutzer als auch externe E-Mailadressen manuell oder über eine CSV-Datei als Mitglieder hinzugefügt werden.

Ein neues Feature in Version 6.6 ist die Verwaltung von Ressourcen. Dabei handelt es sich etwa um Räume, Geräte wie Beamer oder Notebooks oder auch Fahrzeuge. Neben der Ressourcen-Bezeichnung und dem Typ lässt sich festlegen, wer die Ressource einplanen darf und wer sie verwaltet. Wer Termine über Webmail bucht, kann zusätzlich als Ort auch eine Ressource mit dem Typ "Raum" aus einer vordefinierten Liste auswählen. Insgesamt eine gute Funktion – lediglich der Ressourcen-Typ "Fahrzeug" fehlte uns hier.

Zugriff über Standard-Clients

Nach der wirklich einfachen Einrichtung des Servers müssen die Clients der User auf den MailServer zugreifen. Im Test nutzten wir dazu Outlook 2003, um den vollen Groupware-Funktionsumfang zu testen. Damit Outlook die Verbindung herstellen konnte, mussten wir auf dem Client erst den Kerio Outlook Connector installieren. Dabei wurden wir direkt mit der Fehlermeldung begrüßt, wonach Outlook 2003 SP3 oder Outlook 2007 Voraussetzung ist. Das ist deshalb erwähnenswert, da nicht jeder Administrator Office beziehungsweise Outlook 2003 auf SP3 updaten will. Denn dieses Service Pack bringt einige neue – auch bei Microsoft bekannte – Fehler im Mailclient mit sich. Nach dem Outlook-Update und der Installation des Outlook Connectors galt es, ein neues Profil für den Zugriff auf den Kerio MailServer anzulegen.

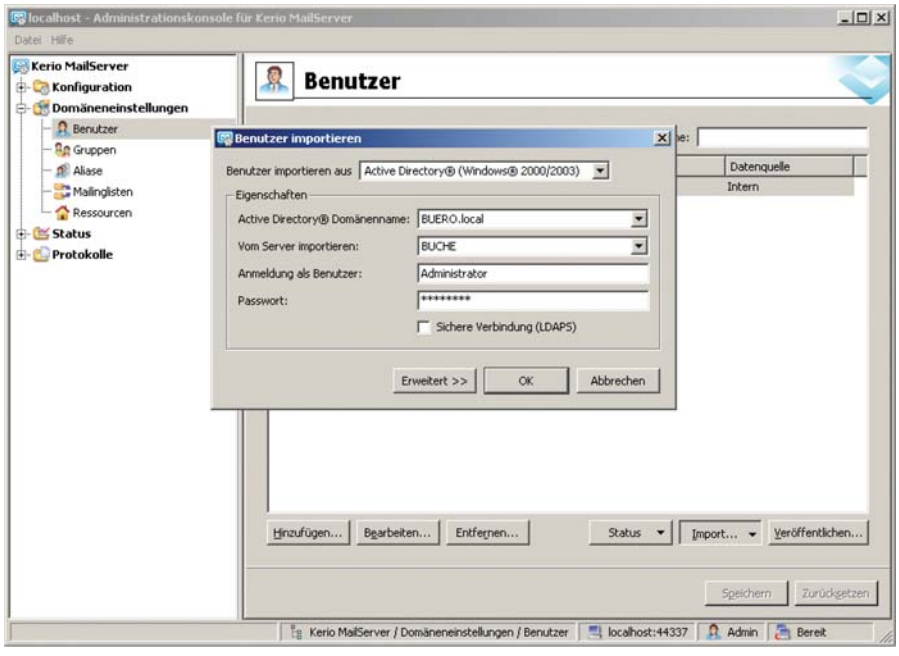


Bild 3: Aus dem Active Directory lassen sich Userdaten bequem importieren


Noch nie war es einfacher, zu virtualisieren:
Kosten zu sparen.
Flexibler zu sein.
Mehr zu erreichen.
Nutzen Sie die Chancen der Virtualisierung. Jetzt.
Mit Microsoft Virtualisierung müssen Sie dafür nicht einmal an Ihr Erspartes. Denn im Betriebssystem Windows Server® 2008 ist der Hypervisor fester Bestandteil und muss nicht erst separat erworben werden. Erfahren Sie mehr über Virtualisierungsmöglichkeiten auf microsoft.de/virtualisierung
Microsoft | Virtualisierung
© Microsoft Corporation 2009. Alle Rechte vorbehalten.

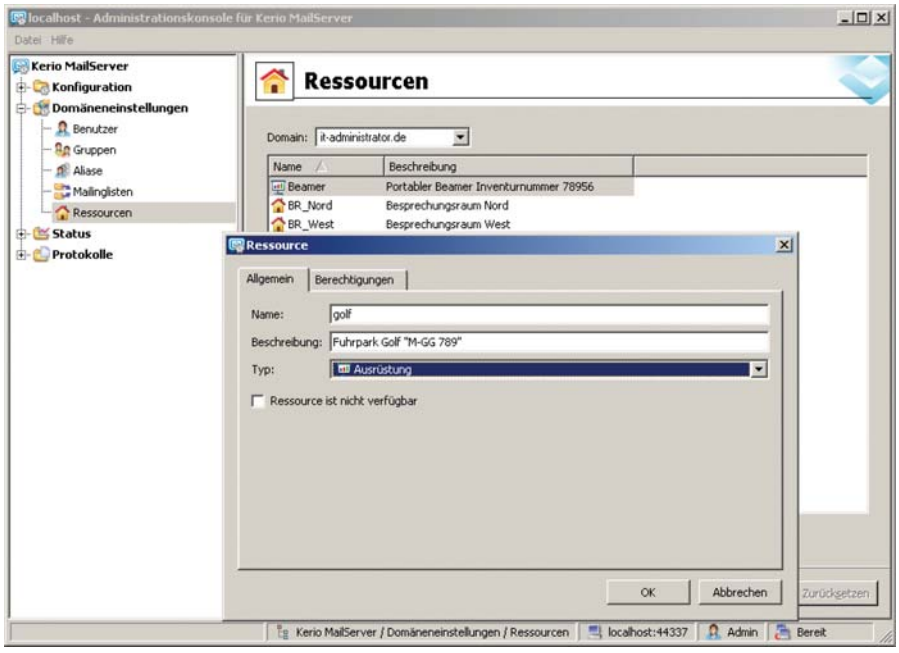


Bild 4: Das Anlegen einer neuen Ressource geht schnell von der Hand und kann ohne viel Aufwand vorgenommen werden

Dem Kerio MailServer richteten wir als MAPI-Server ein neues Profil in Outlook ein. Hierzu riefen wir über die Systemsteuerung von Windows den entsprechenden Eintrag auf und wählten bei der Einrichtung "Zusätzliche Servertypen" aus. Im folgenden Dialog erschien der Kerio Mail-Connector. Da wir die User über das Active Directory bezogen hatten, haben wir hier zudem die sichere Passwortauthentifizierung aktiviert. Anschließend meldete sich der Connector mit dem Benutzer des aktuellen Windows-Logins an (Single Sign On). Bei manuell angelegten oder importierten Usern mussten wir den Kontonamen und das Passwort zusätzlich eingeben.

Nach dem Start von Outlook verband sich der Connector mit dem MailServer und stellte uns alle Daten zur Verfügung. Durch den Einsatz eines separaten Profils in Outlook lässt sich die Umstellung von Exchange zu Outlook sanft durchführen und die User haben die Möglichkeit, Daten von beiden Systemen manuell abzugleichen.

Um die Ressourcen in Outlook einsehen zu können, ist es wichtig, auf dem Kerio MailServer das SSL-Zertifikat zu installieren und zu aktivieren, da der Kerio Outlook Connector über Port 443 die Frei/Gebucht-Stati abfragt.

Verschlüsselte Ressourcen-Abfrage

Mobilität

Neben dem Online- und Offline-Zugriff mit Outlook stehen mobile Zugriffe über Webmail zur Verfügung. Auf den Webmailer griffen wir mit der Server-Domain und dem angepassten Port 8080 zu – wir hatten ihn zu Beginn umgestellt. Aus Sicherheitsgründen ist der HTTPS-Zugang für einen Zugriff von extern zu bevorzugen.

Auch Nutzer eines PDA unter Windows Mobile kommen auf ihre Kosten. Mobile Outlook wird dabei so eingerichtet, als ob der Zugriff auf einen Exchange-Server via Outlook Web Access (OWA) erfolgt. Da wir kein öffentlich bestätigtes SSL-Zertifikat im Test nutzten, mussten wir das durch den Kerio-Server eingerichtete Sicherheits-Testat auf dem PDA importieren. Auch Outlook kann über den Outlook Connector via Web auf den MailServer zugreifen. Hierbei ist es jedoch notwendig, als Server nicht die interne Bezeichnung, sondern eine externe Domain – zum Beispiel via DynDNS – oder die feste IP-Adresse anzugeben. Neu ist zudem, dass Apples iPhone zu den mobilen Clients für den MailServer gehört. Daneben unterstützt die Groupware auch Blackberry-Smartphones sowie mobile Geräte unter Palm OS, Symbian (Nokia, Sony-Ericsson) – was wir nicht testeten, jedoch an dieser Stelle erwähnt sein soll.

Zeitaufwändige Exchange-Migration

Wer bereits einen Small Business oder Exchange Server einsetzt, hat zumeist großes Interesse daran, die bestehenden Da-

Produkt
Mailserver mit Active Directory-Anbindung für kleine und mittelständische Unternehmen.

Hersteller
Kerio Technologies
www.kerio.de

Preis
Kerio MailServer für zehn Benutzer 399 Euro, mit Virenschutz von McAfee für zehn Benutzer 479 Euro. Weitere Lizenzvarianten nach Preisstaffel.

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

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

Handhabung	9
Konfiguration	8
Laufender Administrationsaufwand	9
Client-Anbindung	9
Mobiler Zugriff	10

Dieses Produkt eignet sich

optimal für kleinere und mittlere Unternehmen mit bis zu 150 Anwendern und einer Active Directory-Struktur.

gut für kleinere Unternehmen mit wenigen Anwendern ohne zentrale Benutzerverwaltung, etwa über ein Active Directory.

nicht für Unternehmen mit mehr als 1.000 Usern auf dem Mailserver.

Kerio MailServer 6.6

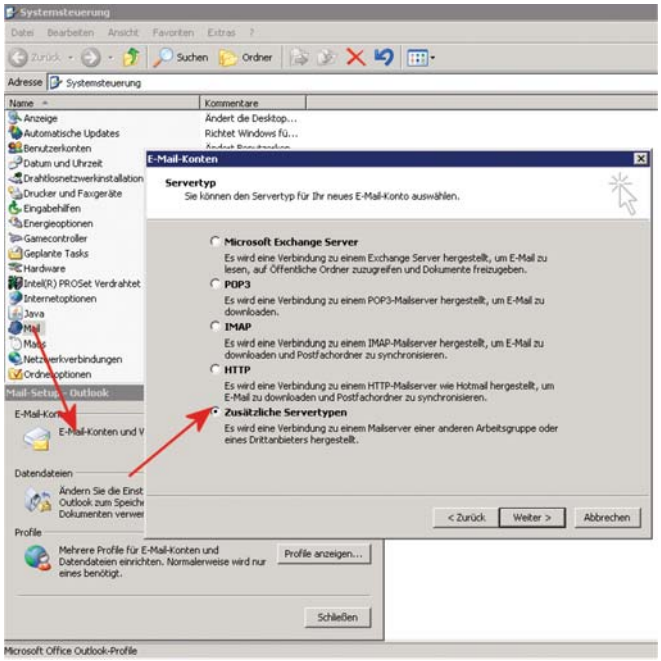


Bild 5: Die Anbindung an den Kerio MailServer erfolgt als MAPI-Server über den Kerio Outlook Connector

ten zu übernehmen. Dazu liefert Kerio das Exchange Migrations Tool mit. Es ermöglicht, die Benutzerdaten, öffentliche Ordner, Nachrichten, Kontakte und Kalender von einem Exchange-Server ab 5.5. bis zur aktuellen Version 2007 zu migrieren. Dabei ist vor allem zu berücksichtigen, dass die Datenübernahme einige Zeit benötigt. Im Test haben wir fünf Benutzer, einige öffentliche Ordner und rund 200 Kontakte migriert. Das Ergebnis konnte sich sehen lassen: Neben den Userdaten und den Nachrichten wurden auch gesetzte Rechte übernommen. Die benötigte Zeit von gut sechs Stunden will hingegen eingeplant sein. Denn während der Migration empfiehlt es sich, dass keiner mehr auf den "alten" Exchange-Server zugreift, um so die Inkonsistenz von Daten zu verhindern.

Fazit

Die Aussage "installieren, konfigurieren, gut ist" können wir bei der Windows-Version des Kerio MailServer bestätigen. Die Einrichtung geht fix und die Implementierung ins System ist schnell gemacht. Einige Funktionen, die zunächst erfolgversprechend schienen, wie die Gruppenmails, erwiesen sich im Test später als wenig praktikabel. Die Daten auf Dateiebene abzulegen ist dagegen Ansichtssache. Die Flexibilität für den User bei der Wahl des Clients, die mobile Anbindung und die Ausstattung sind Aspekte, die klar für das System sprechen. Auch die schnelle Zugriffszeit, vor allem über die mobilen Clients, sticht positiv heraus. Dennoch empfehlen wir die Einrichtung durch einen erfahrenen Server-Administrator durchführen zu lassen. Kleinere Konfigurationen wie das Einrichten neuer Benutzer, Ressourcen oder Mailinglisten lassen sich dann ohne weiteres von einem erfahrenen Mitarbeiter vornehmen. *(dr)*

Kostenlos für IT-Administrator-Abonnenten

iTANet

Workshop in Berlin

Storage-Lösungen für virtualisierte Server am 28. Mai 2009

Die Agenda:

> Anforderungen an SAN-Lösungen im Virtualisierungsumfeld

> iSCSI: Herstellerungabhängiges SAN-Protokoll
iSCSI - Konzepte, Implementation, Optimierung und Sicherheit

> Speicher-Anforderungen der Desktop- und Applikations-Virtualisierung

Ihre Dozenten sind Thomas Weyergraf und Nico Lüdemann

Termin: 28.05.2009
Ort: Fast Lane Institute for Knowledge Transfer, Oranienburger Straße 66, 10117 Berlin
Uhrzeit: 13.00 bis ca. 17.30 Uhr

Teilnahmegebühren:
Für ITANet-Mitglieder beziehungsweise IT-Administrator-Abonnenten kostenlos.

Anmeldeschluss: 18.05.2009

ITANet Schirmherrschaft: REALTECH

Mehr Infos und Anmeldeformulare unter
http://www.it-administrator.de/usergroup/termine/

Im Test: eGroupware 1.6.001

Gruppendynamik

von Thomas Drilling

Unter den inzwischen zahlreichen Open Source Lösungen für Groupware und Collaboration nimmt das vollständig auf PHP basierende eGroupware eine Sonderstellung ein. Zwar folgt auch dieses Produkt primär dem Ziel, organisatorisches Arbeiten im Team mit gemeinsamen Adressbüchern und Kalendern zu verbessern, leistet aber dank seines modularen Aufbaus wesentlich mehr und eignet sich sogar als ausgewachsenes ERP-System. Im Test stellte die freie Lösung ihre ungewöhnliche Funktionsvielfalt unter Beweis.

Dank des modularen Aufbaus ist eGroupware [1] heute weit mehr als eine Goupware-Lösung im klassischen Sinne – die aktuelle stabile Version 1.6.001 bietet einen beachtlichen Funktionsumfang. Außer den für Collaboration obligatorischen Modulen für E-Mail, Adressbuch, Kalender und Aufgabenverwaltung bietet die Lösung schon von Haus aus zahlreiche weitere Anwendungen von der zentralen Dateiablage bis zur Projektverwaltung in Form von Modulen, die sich relativ einfach nachrüsten lassen.

Fertige Pakete

Die Basis für eGroupware bildet eine typische LAMP- oder WAMP-Umgebung, also Webserver mit PHP-Unterstützung und eine Datenbank, wie etwa MySQL. WAMP- oder LAMP-Umgebungen mit Apache, PHP und MySQL haben sich für solche Zwecke bewährt und mit einer Easy-to-Install-Lösung wie dem XAMPP-Paket von Apachefriends [2] steht mit wenig Aufwand ein Applikationsserver zur Verfügung, der sämtliche Voraussetzungen erfüllt (Apache, MySQL und PHP). Die Komponenten sind hierbei bereits aufeinander abgestimmt und das Paket bringt sogar das PHP-basierte MySQL-Konfigurationswerkzeug "phpMyAdmin" mit. Die Installation des XAMPP-Paketes auf einem Linux-Server erspart außerdem eine Menge Konfigurationsarbeit, sofern auf der Plattform nicht bereits eine andere Apache-Instanz läuft. Linux-Nutzer können die benötigten Pakete alternativ auch mit dem Paketmanager der Distribution installieren, sofern Apache oder PHP nicht ohnehin bereits laufen. IT-Verantwortliche, welche die Pakete einzeln installieren, müssen darauf achten, dass der Apache vor der Installation von PHP und MySQL bereits mit PHP-Unterstützung läuft. Auch für Windows-Server stehen einfach zu handhabende XAMPP-Pakete bereit.

Mailserver einrichten

Für einen Groupware-Server ist ein funktionierender Mailserver unerlässlich. eGroupware bringt keinen Mailserver mit, sodass dieser aufgesetzt werden muss. Neben Mail Transfer Agent (MTA) und Mail Delivery Agent (MDA) ist ein IMAP-Server erforderlich. Unter Linux haben sich dazu Open Source-Lösungen, wie der MTA "Postfix" und der IMAP-Server "Cyrus" bewährt und etabliert. Es gibt aber gerade unter Linux reichlich Auswahl in dieser Hinsicht und auch der MTA "Exim" oder der "Courier-Mailserver" (MTA, MDA und IMPA-Server in Einem) sind im Web umfangreich dokumentiert.

Für unser Testsystem entschieden wir uns für das Gespann Cyrus-IMAP und Postfix. Anleitungen [3] hierfür finden sich zahlreich im Internet. Die Konfiguration von Postfix und Cyrus für das gewünschte Mailserver-Szenario lässt sich alternativ auch mit einer grafischen Oberfläche wie Webmin [4] mit überschaubarem Aufwand erledigen. Für Windows-Nutzer empfiehlt sich der einfach zu handhabende Out-of-the-Box Mailserver von Kerio [5]. Der Kerio-Mailserver lässt sich dank einer hervorragenden grafischen Administrationsoberfläche komfortabel und schnell konfigurieren (siehe Test ab Seite 14).

Im Test konfigurierten wir unseren Linux Mailserver mit Postfix und Cyrus IMAP so, dass er E-Mails für die einzurichtende Mail-Domain via fetchmail vom IMAP-Server des externen Mail-Providers abholt und in die IMAP-Postfächer des Cyrus-Servers verteilt. Ausgehende Nachrichten verschickt der Mailserver über den SMTP-Smarthost des Providers.

Es empfiehlt sich übrigens, zur Remote-Administration auch gleich SSH mit zu installieren beziehungsweise den Dienst zu aktivieren. Auf einem Ubuntu-Server steht dazu ein grafischer Menüeintrag zur Verfügung.

eGroupware installieren

Nachdem sämtliche XAMPP-Komponenten eingerichtet und der Mailserver konfiguriert war, begannen wir mit der Installation. Ubuntu-Nutzer können die Version 1.4.004 von eGroupware inklusive einer großen Anzahl von Modulen einfach und ganz bequem via Synaptic aus der Universe-Paketquelle installieren. Ubuntu konfiguriert während der Instal-

Systemanforderungen

Die Hardwareanforderungen richten sich selbstverständlich nach dem geplanten Einsatzzweck sowie der Anzahl der Benutzer – für unsere Testinstallation genügte bereits ein virtueller Server mit 512 MByte RAM. eGroupware ist auf Server- und Client-Seite betriebssystemunabhängig.

lation auch gleich den eGoupware-Administrator (Headerverwaltungsbenutzer).

Um die aktuellste eGroupware-Version 1.6.001 unter Unbuntu zu installieren sind die Originalpakete
- *eGroupware-1.6.001.tar.bz2*
- *eGroupware-egw-pear-1.6.001.tar.bz2* und
- *eGroupware-icalsrv-1.6.001.tar.bz2*

von Sourceforge [6] notwendig. Diese sind in das htdocs-Verzeichnis, beispielsweise unter */usr/share/egroupware,* zu entpacken. Die eigentliche Installation erfolgt, wie bei PHP-Anwendungen üblich, im Webbrowser durch Aufruf der URL des Installationsskriptes *http://{IP-Adresse/egroupware}*. Als Sprache benötigt die Installation "Deutsch" und ein Installationstest zeigt schnell, ob alle weiteren Voraussetzungen erfüllt sind. Sind sämtliche Einstellungen mit einem grünen Häkchen versehen – was bei XAMPP mit Ausnahme der odbc-Option der Fall war, folgt das Anlegen der Datei *header.inc.php* für die grundlegenden Einstellungen wie etwa Installationspfad, Datenbanktyp et cetera.

Nun erhielt der Webserver noch Schreibrechte im Installationsverzeichnis von eGroupware. Über die Schaltfläche "Herunterladen" liess sich die Datei *header.inc.php* zunächst lokal speichern und anschließend via *scp* oder *rcopy* in das Verzeichnis */usr/share/egroupware* auf dem Server übertragen. Die weitere Installation erfolgte bequem im Webbrowser, wobei sich die Default-Werte meist übernehmen lassen. Lediglich bei "Benutzer Headerverwaltung" im Feld "Passwort Headerverwaltung" war die Angabe eines Passworts notwendig.

Datenbank konfigurieren

Nun wendeten wir uns im Dialog "Setup-/Konfigurationsadmin-Login" dem Aufsetzen der notwendigen Datenbank zu. Zunächst legten wir den Zeichensatz – etwa "utf-8" – fest und erstellten dann eine Datenbank. Das XAMPP-Paket vergibt per Default kein Passwort für den Benutzer root der MySQL-Datenbank, daher genügte an dieser Stelle ein Klick auf "Datenbank erzeugen". In unserem Setup funktionierte alles, was uns der Installer mit "Ihre Datenbank arbeitet, aber Sie haben keine Anwendungen installiert!" bestätigte.

Es folgte ein Klick auf "Installieren Alle Anwendungen". Während der Installation zeigte der Installer keine weiteren Statusmeldungen an. Im Anschluss ist ein Klick auf "Installation erneut überprüfen" erforderlich, der dazu führen muss, dass "Schritt 1 - Einfache Verwaltung der Anwendungen" mit einem grünen Haken markiert ist.

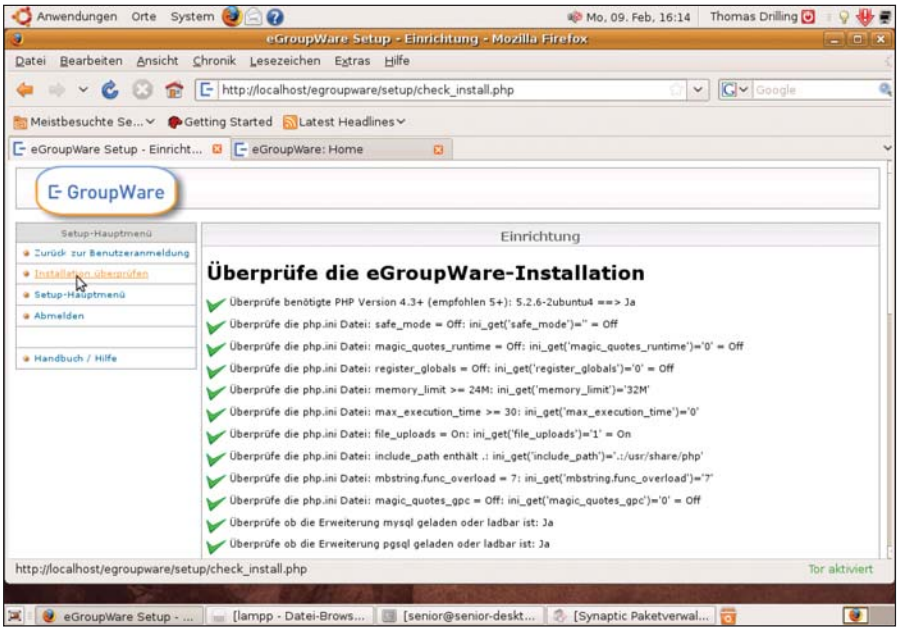


Bild 1: eGroupware überprüft im PHP-Installationsskript selbstständig, ob die Installationsvoraussetzungen erfüllt sind und gibt entsprechende Hinweise

Konfiguration anpassen

Nach der Installation des Basis-Systems stellten wir unter "Schritt 2 – Konfiguration / Gegenwärtige Konfiguration überarbeiten" zunächst im Bereich "Pfadinformationen" die Pfade für temporäre Dateien und für die entsprechenden Verzeichnisse für die spätere Verwaltung des Groupware-Systems ein. So benötigten wir etwa für das Backup ein so genanntes "Datensicherungsverzeichnis". Dabei müssen sämtliche Pfade außerhalb des Documentroot des Webservers liegen.

Abgesehen vom ersten Verzeichnis */tmp* benötigte der Webserver Schreibrechte auf die angegebenen Verzeichnisse, die diesbezüglichen Vorschläge des Installers lassen sich aber problemlos übernehmen. Zu bedenken ist allerdings, dass diese Pfade mit Ausnahme von */tmp* auf dem eGroupware-Server von Hand anzulegen und mit den benötigten Schreibrechten für den Webserver zu versehen sind.

In der folgenden Sektion "Host Informationen" waren keine Änderungen notwendig, denn das Feld "Hostname des Computers" versieht der Installer bereits mit der IP-Adresse des Groupware-Servers (sofern die Installation nicht wie im Beispiel auf "localhost" erfolgt). Nun vervollständigten wir lediglich noch die Einstellungen in der Sektion "Standard Mailserver Einstellungen" gemäß dem Mailserver-Szenario. Im letzten Schritt vergaben wir im Hauptmenü "Schritt 3" über "Administrator Konto / Administrator-Konto anlegen" Benutzername, E-Mail-Adresse und ein Passwort.

eGroupware administrieren

Die Applikation für den eGoupware-Administrator ist die "Admin Anwendung", die unter der eGroupware-URL *http://{ip-adresse}/egroupware* nach An-

meldung als Benutzer "admin" über die Portalseite des Administrators zu erreichen ist. Der erste Link "Konfiguration der Anwendung" ermöglicht es, eGroupware im Erscheinungsbild anzupassen. Das reicht vom Logo über die Verfügbarkeit von Anwendungen bis hin zu Timeouts und Sicherheitseinstellungen.

Wir legten zunächst einige Benutzer über die Schaltfläche "Hinzufügen" in der Sektion "Admin / Benutzerkonten" an. Neben den eigentlichen Benutzerdaten legten wir hier für jeden einzelnen Benutzer auch fest, welche eGroupware-Anwendungen ihm zur Verfügung stehen. Soll der neue Benutzer auch mit dem E-Mail-Subsystem von eGroupware arbeiten und seine Mails in eGroupware verwalten dürfen, ist parallel ein System-Account sowie ein Account auf dem IMAP-Server erforderlich. Läuft der eGroupware-Server nicht auf einer lokal zugänglichen Maschine, ist die Konfiguration auch über SSH möglich.

Zum Anlegen des IMAP-Benutzers für Cyrus-IMAP dient das Kommando *cyradm*. Dazu meldeten wir uns als Cyrus-Administrator (User: Cyrus) am IMAP-Server an und legten im Cyrus-Kommandomodus die Benutzer an:

```
cyradm –user cyrus localhost
IMAP Password:
localhost>cm user.tdrilling
localhost>quit
```

eGroupware im täglichen Einsatz

Bereits mit der beschriebenen Standard-Installation bringt eGroupware weit mehr Module [7] mit als vergleichbare Lösungen. Darunter finden sich Kalender, Adressbuch, der Mail-Client "FelaMiMail", das Modul "InfoLog" und die Dateiverwaltung. Außerdem fungiert eGroupware selbst dank ihrer offenen Entwicklungsschnittstelle als Fundament für weitere Third-Party-Produkte. Neben den offiziellen, auf der eGroupware-Projektseite genannten Anwendungen sind auf Sourceforge noch weitere, vorwiegend geschäftliche eGroupware-Anwendungen zu finden, darunter beispielhaft ein Modul zum Einbinden der Open Source-Telefonanlage Asterisk.

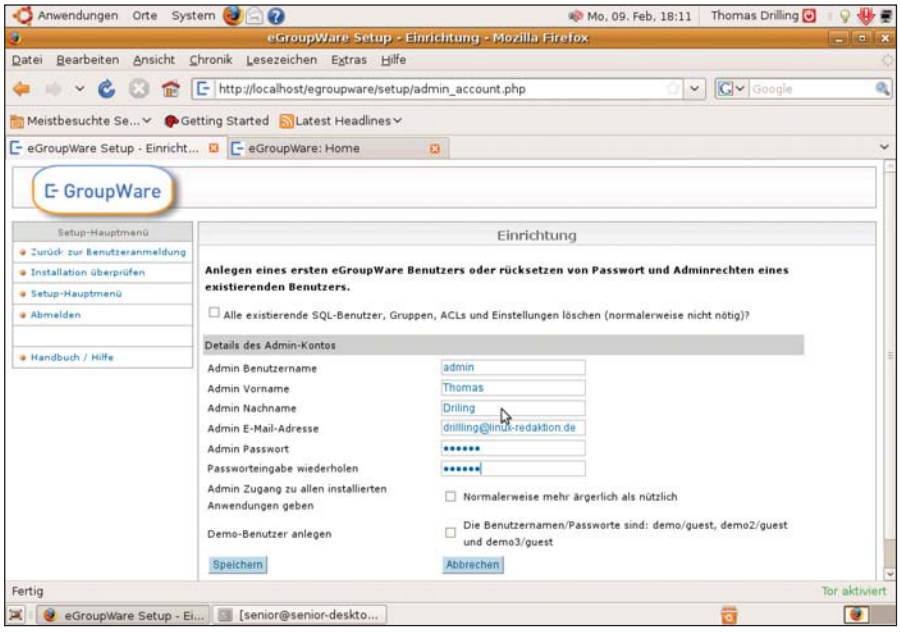


Bild 2: Nur der Administrator kann weitere Benutzer anlegen und Einstellungen an den installierten Applikationen vornehmen

Das Kalendermodul von eGroupware

Die Kern-Applikation von eGroupware ist der Kalender zum Verwalten der Termine von Einzelpersonen und Gruppen. Der Kalender zeigt per Default in der Bildschirmmitte die Tagesansicht und links davon die Monatsübersicht sowie diverse Import- und Exportfilter. Ein neuer Termin lässt sich einfach über "Hinzufügen" im Kalender-Menü oder direkt über eine Uhrzeit in der Tagesansicht erstellen. eGroupware erfragt nun gewohnte Termindetails wie Datum, Uhrzeit, Dauer, Ort und einige weitere Informationen.

Zu den Besonderheiten von eGroupware gehört die Verknüpfung von Informationen (etwa Termine) aus den unterschiedlichen Modulen. Mit dem Link "Kalender Einstellungen" lassen sich individuelle Anpassungen am Kalendermodul vornehmen, etwa "E-Mail Updates" einschalten, um Team-Mitglieder automatisch über Terminänderungen zu informieren. Weiterhin ist es IT-Verantwortlichen möglich, Nicht-Team-Mitglieder die Belegtzeiten via iCal einsehen zu lassen (die Einstellung erfolgt über *https://{IP des eGroupware-Servers}/egroupware/calendar/freebusy.php?user={benutzername}*). Rechts von der Tagesansicht bietet die Kalenderansicht Zugriff auf die Aufgabenverwaltung, die ihrerseits auf Informationen des Moduls "InfoLog" zugreift.

Adressbuch

Das Adressbuch ist in einer Groupware-Lösung das Schlüsselelement für perfekte Teamarbeit und bildet die Basis jeder Art von Planungsaktivität. Auch eGroupware

Mit der Option der Freigabe ganzer IMAP-Ordner für Team-Mitglieder verfügt eGroupware über eine faszinierende und einfache Möglichkeit zur Verwaltung von Arbeitsgruppen und Dokumenten auf einem IMAP-Server. Dabei lassen sich individuelle Berechtigungen für jeden Ordner festlegen. Die Konfiguration der Ordnerverwaltung bedarf des Starts des Webmailers "FelaMiMail" und erfolgt dort in der Ordner-Verwaltung. Das Feld "Unterordner anlegen" belegen Anwender mit einen passenden Namen. Klicken Sie dann auf "Erzeugen". Der neue Ordner erscheint dann links in der Baumstruktur des IMAP-Ordners. Ein Klick auf den Ordner und den Register-Reiter "ACL" öffnet ein Popup-Fenster, um den Namen des Benutzers der Freigabe festzulegen.

Ordnerverwaltung im IMAP

QualityHosting

Läuft auch, wenn Sie sich mal nicht um alles kümmern können.

Hosted Exchange 2007

Jetzt 60 Tage kostenlos testen & Einrichtungsgebühr sparen!*

*60 Tage Rücktrittsrecht & kostenfrei sowie keine Einrichtungsgebühr bei 24 Monaten Vertragslaufzeit (monatlich 11,89 €) und Eingabe des Aktionscodes: »**Exchange**«.

Hosted Exchange 2007: Systemadministration mit Weitblick!

Mitarbeiter optimal vernetzen!
Stets synchronisierte E-Mail-Accounts, Kalender, Kontakte und Projektdaten! Jederzeitiger Direktkontakt mit Ihren Mitarbeitern, Kunden und Partnern via Desktop, Notebook, PDA oder Smartphone auch von unterwegs.

Features, die begeistern:
- **2000 MB Speicherplatz**
- **Outlook 2007-Lizenz**
- **Outlook Web Access 2007**
- **Push-Mail-Dienst**
- **tägliche Datensicherung**
- **99,9% Verfügbarkeit u.v.m.**

Professioneller Schutz ohne Extra-Budgets und Manpower!
Genießen Sie professionelle E-Mail-und Sicherheitssysteme. Und das bei null Investitionskosten. Sofort einsatzbereit. 24/7-Support.

Als erster deutscher Anbieter, der das Hosting von Exchange 2007 in einer speziell entwickelten Microsoft-Umgebung realisiert hat, steht QualityHosting seit nunmehr 10 Jahren kompromisslos für Qualität und individuelle Lösungen.

Anspruch. Leistung. Sicherheit.

www.qualityhosting.de

kennt neben dem globalen Adressbuch ein "persönliches" Adressbuch, mit dessen Hilfe eGroupware-Nutzer Kontakte vor dem Zugriff der anderen Gruppenmitglieder verbergen. Das eGroupware-Adressbuch besitzt einerseits einen recht komfortablen Eingabedialog, bietet aber selbstverständlich auch eine CSV-Importschnittstelle, was besonders bei einer Migration mit vorhandenen Adressbüchern sehr nützlich ist; denn die meisten E-Mail-Clients können ihre Adressbücher im CSV-Format exportieren. Daneben lassen sich eGroupware-Adressbücher selbstverständlich auch in einer CSV-Datei exportieren. Auch die Möglichkeit, Platzhalter für eGroupware-Adressbucheinträge in Dokumentvorlagen zu verwenden, die eGroupware dann per Mausklick automatisch einfügt, ist ein wertvolles Feature.

Aufgabenverwaltung mit InfoLog

Das InfoLog-Modul von eGroupware leistet aber noch wesentlich mehr als die reine Aufgabenverwaltung (die Entwickler titulieren InfoLog gerne als "einfaches CRM-System"). So kennt InfoLog beispielsweise unterschiedliche Aufgabentypen wie "Anruf", "Notiz" und "E-Mail" und ist außerdem in der Lage, Aufgaben an andere Team-Mitglieder zu delegieren.

Zusätzlich können Anwender InfoLog-Einträge mit Daten aus Adressbuch, Kalender, Projektmanager und sogar mit externen Dateien verknüpfen. Sobald wir eine InfoLog-Aktivität mit einer externen Datei verknüpften, speicherte eGroupware diese im eigenen virtuellen Dateisystem (VFS).

Eine weitere Besonderheit von InfoLog ist dessen Fähigkeit zum Anlegen von Untereinträgen, was im Test auch direkt aus dem Kalender, Adressbuch oder Projektmanager heraus gelang. So legten wir einen InfoLog-Eintrag aus dem Adressbuch heraus an, indem wir den gewünschten Datensatz wählten und eGroupware den aktuellen Adressdatensatz automatisch in die Verknüpfung übernahm. Administratoren haben übrigens jederzeit die Möglichkeit, die bereits vorhandenen InfoLog-Felder im Admin-Menü unter "Benutzerdefinierte Felder, Typen und Status" um selbst definierte Felder zu erweitern.

Komfortable Dateiverwaltung für die Anwender

Der in eGroupware eingebaute Dateimanager ermöglicht Anwendern das Verwalten ihrer Dateien direkt auf dem eGroupware-Server oder via WebDAV auf dem Web-Server der eGroupware-Maschine. So können Teams problemlos mit einem gemeinsamen Vorrat an Dateien arbeiten. Außerdem unterstützt eGroupware ACLs zum Setzen von Zugriffsberechtigungen nur auf Gruppen-Ebene. Eine solche Gruppe lässt sich in der Gruppenverwaltung im Admin-Modul erstellen.

Problemlos fügten wir einer neuen Gruppe explizit diejenigen Benutzer hinzu, die auf diese Gruppe (Freigabe) zugreifen dürfen und erlaubten diesen Benutzern, die gemeinsamen Dateien über eGroupware zu verwalten (über "Verfügbar/ACL" unter "Dateiverwaltung"). Hilfreich ist dabei, dass sich bei vielen Modulen direkt neben dem Verfügbar-Häkchen ein kleines Notizblock-Symbol findet, über das wir explizit die ACLs für die Gruppe und die einzelnen Mitglieder vergaben.

Webmail-Client

eGroupware verfügt weiterhin über einen eingebauten Webmail-Client mit der kryptischen Bezeichnung "FelaMiMail", der zwingend einen IMAP-Server voraussetzt. Daher legten wir im Zuge der eGroupware-Installation gesteigerten Wert auf die vorherige Konfiguration des Cyrus-IMAP-Servers (und auch das Setup von eGroupware prüft, ob ein IMAP-Server vorhanden ist). Sofern Anwender dessen korrekte Konfiguration bei der Installation nicht auslassen, steht der Webmailer jedem neuen eGroupware-Benutzer zur Verfügung.

Der Webmail-Client beherrscht neben dem Verfassen von Nachrichten alle wichtigen Funktionen, wie das Sortieren und Markieren von Nachrichten und besitzt eine Suchfunktion. Eine Besonderheit ist die Möglichkeit, den Ordner des IMAP-Kontos im Rahmen der individuell einstellbaren Berechtigungen auch für andere Nutzer einer Gruppe freizugeben. So ist es mit dem Webmailer möglich, Dokumente für Arbeitsgruppen auf einem IMAP-Server zu verwalten.

Full-Clients

eGroupware ist in erster Linie für das Arbeiten im Browser gedacht und optimiert. Zum Abfragen des IMAP-Servers lässt

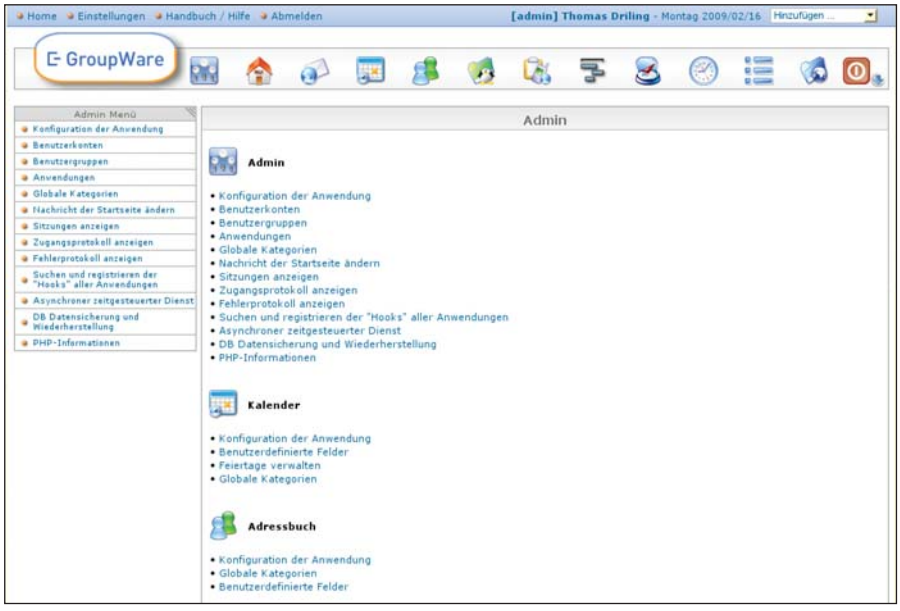


Bild 3: Als Administrator lässt sich eGroupware im Modul "Einstellungen" weiter konfigurieren

Jetzt ist alles drin – sogar der Storage Manager.

intel Xeon® inside™
Kraftvoll. Effizient.

UMDENKEN BEIM THEMA VEREINFACHTE DATENSICHERUNG:

HP All-in-One Storage Manager Software. Jetzt kostenlos im Paket mit HP ProLiant Storage Servern.

Behalten Sie die Kontrolle über Ihre Daten – mit HP All-in-One Storage Manager Software (ASM). Jetzt ohne Aufpreis bei den meisten HP ProLiant Storage Servern. Gemeinsam genutzten Speicher einrichten, migrieren, verwalten und schützen, NAS-Umgebungen im Handumdrehen konfigurieren, schnelle Änderungen über die intuitive Schnittstelle vornehmen: Intelligente Speicherlösungen sind wirtschaftlicher als die reine Aufstockung der Kapazität.

Technologien für Ihren Geschäftserfolg.

0 % Zinsen – 100 % Leistung!
Jetzt neueste Server- und Storage-Technologie von HP günstig leasen. Gültig bis 30. 05. 2009.*
www.hp.com/de/null-prozent-leasing

HP ProLiant DL380 G5 Storage Server
- Mit Intel® Xeon® Prozessor
- In verschiedenen Konfigurationen und mit vielen Erweiterungsoptionen erhältlich
- Skalierbares Hochleistungssystem für Arbeitsgruppen und Unternehmensumgebungen

ab € 4.580,– inkl. MwSt.

Auf www.hp.com/go/simplestorage erfahren Sie, wie Sie Ihre Daten mit dem HP StorageWorks All-in-One Storage Manager ganz einfach in den Griff bekommen.

© 2009 Hewlett-Packard Development Company, L.P. Intel, das Intel Logo, Xeon und Xeon Inside sind Marken der Intel Corporation in den USA und anderen Ländern. * Es handelt sich um ein freibleibendes Finanzierungsangebot der De Lage Landen Technology Finance GmbH, Hansaallee 249, Düsseldorf (DLL). Das Angebot richtet sich ausschließlich an Unternehmer. 0% Leasingrate bedeutet, dass die Summe der Leasingraten innerhalb der Mindestlaufzeit dem Anschaffungswert des finanzierten Objekts entspricht. Weitere aufgrund des Vertrags zu leistende Zahlungen (z. B. Bearbeitungsgebühr) bleiben von diesem Angebot unberührt. Es gilt ein Mindest-Investitionsvolumen in Höhe von EUR 10.000 (zzgl. MwSt.). Die Mindestlaufzeit des Leasingvertrags beläuft sich auf 30 Monate. Voraussetzung für den Abschluss eines Leasingvertrags ist eine positive Bonitätsprüfung durch DLL. DLL behält sich das Recht vor, diese Aktion jederzeit zu ändern oder zu beenden.

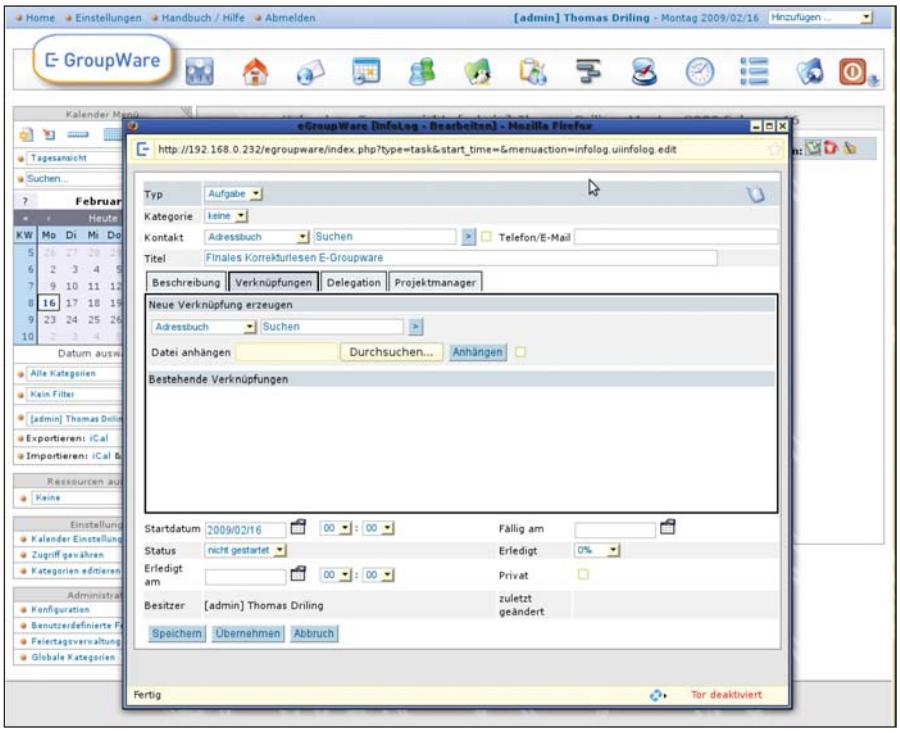


Bild 4: Informationen aus beinahe allen Modulen lassen sich miteinander verknüpfen

sich selbstverständlich jeder beliebige Mailclient, wie Outlook oder Thunderbird, verwenden. Zusätzlich unterstützt eGroupware hinsichtlich der Kommunikation zwischen ihrem Applikationsserver und nativen Clients neben IMAP und LDAP auch die offenen Standards GroupDAV, SyncML und XML-RPC. Unter [8] findet sich eine hervorragende Übersicht, ob und in welcher Weise die einzelnen Haupt-Module von eGroupware mit den gebräuchlichen Full-Clients Outlook, Kontact, Evolution und Thunderbird kommunizieren.

Für die Anbindung von Outlook über IMAP hinaus benötigten wir zusätzliche Hilfsprogramme, weil eGroupware keine MAPI-Unterstützung bietet, wie etwa der auf Seite 51 in dieser Ausgabe beschriebene Zarafa-Server. Da der eGroupware-Server das XMLRPC-Protokoll unterstützt, bietet sich die Installation des Sync-Tools "eGWOSync" [9] an. Das Tools setzt Microsofts .NET-Framework voraus, welches wir aber komfortabel aus dem Programm heraus installierten.

Beim ersten Start von eGWOSync fragte das Programm im "First time guide" den Hostnamen und die Login-Daten des eGroupware-Servers ab und führte einen Login-Test durch. Nachdem alles funktionierte, konfigurierten wir eGWOSync problemlos. Zu beachten ist lediglich, dass wir dazu zuvor im eGroupware-Setup den xmlrpc-Service im Admin-Menü in der Sektion "Sicherheit" unter "Konfiguration aktiviert hatten. Nach erfolgtem Login residierte eGWOSync in der Windows-Taskleiste und wir nahmen über deren Kontextmenü die Einstellungen von eGWOSync vor. Stellte das Tool bei der Synchronisation einen möglichen Datenkonflikt fest, fragte es nach, bevor es Daten überschrieb oder löschte. Die zur Synchronisation erforderlichen Kommandos stehen ebenfalls direkt im Kontextmenü des Systray-Icons von eGWOSync zur Verfügung.

eGroupware auf Rootservern

eGroupware ist angesichts seines Funktionsumfangs geradezu prädestiniert für den Einsatz auf einem Root-Server. Mit Hilfe des Online-Tools "eGWPush" [10] gelingt die Installation von eGroupware auf einem Rootserver im Handumdrehen. Bei "eGWPush" müssen lediglich die Daten für den FTP-Zugang und das Zielverzeichnis erfasst werden, sowie die gewünschte Version wählen. Das Werkzeug überträgt die Installation so direkt auf den Rootserver.

Produkt
Modular erweiterbare Groupware- und Kollaborations-Lösung auf Basis von PHP-Apache-MySQL.

Hersteller
Open-Source-Projekt
www.egroupware.org

Preis
kostenlos

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

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

Funktionsumfang	10
Installation und Bedienung	5
Konfigurierbarkeit	9
Schnittstellen / Erweiterbarkeit	10
Stabilität	9

Dieses Produkt eignet sich

optimal für Unternehmen aller Unternehmensgrößen, die eine flexible und plattformunabhängige Kollaborations-Lösung benötigen, die weit mehr kann, als Adressbücher und Kalender verwalten.

teilweise für Unternehmen, die vorrangig eine Groupware-Lösunge mit gemischten Clients suchen. Die Unterstützung für Outlook ist teilweise gegeben, aber keine MAPI-Funktionalität. Der Browser-Client bietet keine AJAX-Unterstützung. Das Produkt eignet sich teilweise auch als CRM-System.

nicht für Unternehmen oder Kleinstanwender, die eine leicht installierbare und einfach wartbare Groupware-Lösung als Ersatz für MS Exchange suchen und die ausschließlich Outlook-Clients verwenden.

eGroupware 1.6.001

Fazit

Ein Blick auf die über die Standardfunktionen "Mail", "Adressbuch", "Kalender" und "Aufgaben" (InfoLog) vorliegenden Möglichkeiten von eGroupware zeigt, dass die

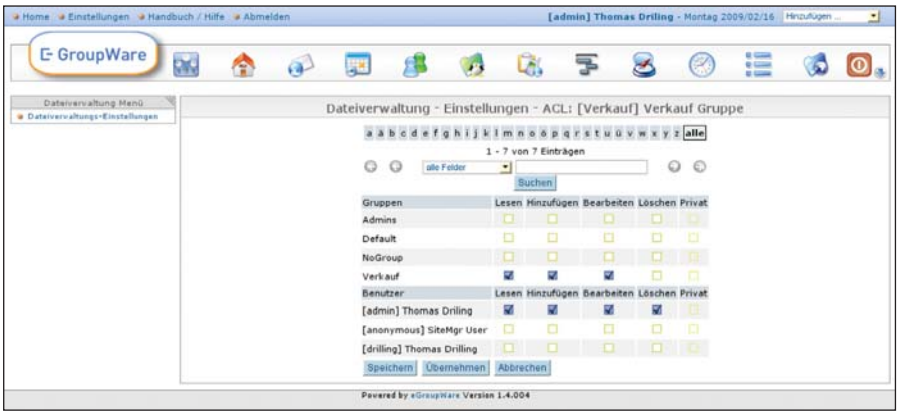


Bild 5: Zum Setzen der ACLs dient das kleine Notizblock-Symbol in der Verfügbarkeitsliste

Lösung weit mehr als eine Groupware-Lösung auf PHP- und MySQL-Basis ist. Bereits die Standard-Installation bringt die Module "Projektmanager", "Ressourcen", "Stundenzettel", "WIKI" und ein Verfolgungssystem mit. Ein besonderes Merkmal besteht neben der ausgeklügelten ACL-Verwaltung darin, dass sich Informationen und Daten aus beinahe allen Modulen miteinander verknüpfen lassen.

Besonders der Funktionsumfang des Infolog-Modules ermöglicht Funktions- und Arbeitsabläufe eines ausgewachsenen CRM-Systems; ebenfalls gefallen kann die Freigabe von IMAP-Ordnern. Darüber hinaus lässt sich das System mit zahlreichen hauseigenen Modulen, Zusatztools und Third-Party-Produkten erweitern und dank der offenen Schnittstellen und Standardprotokolle LDAP, GroupDAV oder XMLRPC flexibel in die bestehende Infrastruktur integrieren, wobei sich auch Fat-Clients wie Kontact, Evolution oder Thunderbird über die reine IMAP-Funktionalität hinaus nutzen lassen. Für die Anbindung von Outlook existiert zwar eine funktionierende Sync-Lösung, diese reicht allerdings im Komfort nicht an eine MAPI-Implementation wie etwa in Zarafa heran.

eGroupware ist ein offenes, anpassbares System, das beinahe jeden denkbaren Einsatzzweck moderner Teamarbeit abdeckt. Allein der gigantische Funktionsumfang machen Installation und Handhabung im Webinterface zwar aufwändig, aber alles in allem noch beherrschbar. Das Webinterface kommt im Look&Feel nicht an Zarafa heran und lässt gegenüber diesem ausgefeilte AJAX-Funktionalität vermissen, ist aber trotzdem leidlich gut bedienbar und bietet einen unerreichten Funktionsumfang bis hin zu einem vollwertigen CRM- oder ERP-System. Die große internationale Entwicklergemeinde garantiert zudem nicht nur schnelle Hilfe in allen Lebenslagen, sondern auch eine zukunftsträchtige und stetige Weiterentwicklung. *(jp)*

Links

[1] eGroupware Download
www.egroupware.org

[2] XAMPP-Paket von Apachefriends
www.apachefriends.org/de/xampp.html

[3] Cyrus-IMAP und Postfix
http://wiki.hetzner.de/index.php/DebianMailserver

[4] Webmin
www.webmin.com

[5] Kerio 60-Tage-Testversion
www.kerio.de/kms_download.html

[6] eGroupware 1.6.001 unter Unbuntu
http://sourceforge.net/project/showfiles.php?group_id=78745

[7] Module für eGroupware
www.egroupware.org/applications

[8] IMAP-Clients
www.egroupware.org/sync

[9] MSHnstaller-PaketeGWOSync
http://prdownloads.sourceforge.net/egroupware/eGWOSyncSetup_0.4.0.msi?download

[10] eGWPush
http://egwpush.proserver1.at/

Mail-SeCure™
98,5% SPAM Erkennungsrate

100% Virenschutz

Mail Encryption Solution™
Mail ist bis zu ihrer Öffnung vollständig gesichert

PineApp™ - die "RUNDE" Lösung für IHRE IT-Sicherheit aus einer Hand

Archive-SeCure™
E-Mails werden in standardisiertem Format gespeichert (d.h. RFC822), komprimiert und verschlüsselt.

Surf-SeCure™
Proactives Real-Time Web and VoIP Filtering

SeCure SoHo™
All-in-one Sicherheitslösung

www.datakom-distribution.de

PineApp
Our Innovation - Your SeCurity

Einkaufsführer: Sichere E-Mailumgebungen

Geschützte Kommunikation

von Chris Meidinger

Unternehmen stellen unterschiedliche Anforderungen an ihre Kommunikationsinfrastrukturen. Immer mehr Firmen rüsten dabei auf und investieren in Insellösungen, die sicher sein und zugleich die Produktivität der Mitarbeiter fördern sollen. Doch steigt so auch die Komplexität der Systeme. Das Ergebnis: Höhere Ausgaben für Pflege und Wartung, unnötige Hindernisse im laufenden Betrieb und eine größere Fehlerquote. IT-Administrator zeigt auf, worauf es in kleinen, mittleren und großen Umgebungen ankommt.

Um die Anforderungen an E-Mailumgebungen sinnvoll betrachten zu können, teilen wir die Infrastruktur in drei logische Komponenten auf. Die erste stellt dabei der "Security-Layer" dar. Hier finden bei der Annahme einer E-Mail zunächst Spamabwehr, Virenprüfung und weitere Inhaltskontrollen statt. Danach wird die Mail an den "Policy-Layer" weitergegeben. In diesem Layer befindet sich die eigentliche Intelligenz der E-Mailinfrastruktur: Entscheidungen zum Routing, LDAP-basierte Policies, Compliance-Prüfungen und sonstige regelbasierende Anforderungen werden hier ausgeführt. Der Policy-Layer gibt die Nachricht anschließend an den "Internal-Layer" weiter. Dort befinden sich die klassischen Groupware-Systeme, die E-Mails vorhalten und den Anwendern zur Verfügung stellen. In kleineren Unternehmen können diese äußeren Layer (Security und Policy) oftmals zu einer Einheit zusammengefasst werden. Große Unternehmen hingegen haben oftmals gänzlich separate Arbeitsgruppen für die Bewältigung der anstehenden Aufgaben in den Security- und Policy-Layer. In weiteren Verlauf unseres Einkaufsführers gehen wir auf die Infrastrukturkomponenten der Security- und Policy-Layer im Detail ein.

Appliances wie die "Sentrion MP 301" von Sendmail beinhalten einen MTA und bieten E-Mailsicherheit

Security Layer

Es gibt zwei primäre Ansätze im Security-Layer: das Insourcing und das Outsourcing. Dienste wie Postini von Google, Message Labs von Symantec oder eXpurgate von eleven nehmen Firmen den Betrieb des eigenen E-Mailgateways ab. Die damit verbundenen Administrierungsaufgaben entfallen damit für die eigene IT-Abteilung. Je nach Wunsch werden nur gefilterte, gescannte, archivierte und verifizierte E-Mails an die eigenen internen Systeme weitergeleitet. Für kleinere Firmen können solche Angebote wirtschaftlich durchaus verlockend und auch sinnvoll sein. Der meist überlastete Administrator muss sich bei dieser Lösung nicht mehr mit komplexen Themen wie der Pflege von Blacklists, der Abwehr von Directory-Harvesting Attacken, der Sicherung vor Open-Relays und ähnlichen Dinge befassen. Zugleich verliert das Unternehmen aber die Kontrolle über die eigene Kommunikation. Mittelständische bis große Unternehmen bevorzugen daher oftmals den Betrieb einer eigenen E-Mail-Infrastruktur. Unabhängig davon, ob diese Aktivitäten in Eigenleistung oder als Dienstleistung erbracht werden, sind die wesentlichen Merkmale des Security-Layers die Gleichen. Die nachfolgenden Informationen sollen bei der Bewertung eines möglichen Dienstleisters als Leitfaden für das Gespräch mit dem Anbieter dienen.

Annahme verweigert

Möglichst viele Kontrollen im Security-Layer sollten noch während der Annahme einer E-Mail ausgeführt werden. Ist dies gegeben, kann die Kommunikation im Zweifelsfall sofort abgebrochen werden, bevor ein "250 Message accepted for Delivery" ausgegeben wird. Stattdessen erhält der Absender einen 550er-Fehler - die Verweigerung der Annahme. Somit entfällt bei False-Positives die Wartezeit und Verwirrung beim User sowie die Anrufe beim Helpdesk, die typischerweise damit verbunden sind. Aufgrund dieser Nicht-Annahme wird die unerwünschte E-Mail weder auf die Festplatte des Gateways geschrieben noch läuft sie Gefahr, in einem Archivsystem zu landen.

Das erste Kommando in klassischer SMTP-Kommunikation nach der HELO-Begrüßung (im erweiterten SMTP der EHLO) ist der "mail from:"-Befehl. Ein modernes Mailgateway stellt bereits hier sicher, dass kein unauthentisierter Absender E-Mails von angeblich internen Adressen ins Unternehmen einschleust. Sollte ein Spammer dies versuchen, sollte die E-Mail mit einem 550er-Fehler verweigert werden. Mobile Mitarbeiter müssen jedoch oft E-Mails von externen Standorten über das Firmennetz versenden, sowohl vom Laptop als auch vom Handy oder Smartphone. In Großunternehmen findet dies typischerweise über ein VPN statt, kleine und mittelständische Unternehmen können den Versand direkt am Gateway erlauben. Hierzu ist es notwendig, dass der MTA den User direkt gegen das Corporate-Directory authentifizieren kann. Im Gegensatz zur Situation vor zehn Jahren haben inzwischen selbst die kleinsten Unternehmen einen Small Business Server, um die eigenen Userdaten pflegen und verwalten zu können. Ein moderner MTA sollte sich problemlos an das Directory anmelden können, um die Daten des Users zu verifizieren.

Im SMTP-Dialog wird nach Angabe des Absenders der Empfänger mit "rcpt to:" mitgeteilt. Hier sollte ein MTA auch direkt prüfen können, ob es diesen Empfänger tatsächlich im Unternehmen gibt. Ist der Empfänger nicht vorhanden, kann die E-Mail sofort mit "550 User unknown" abgelehnt werden. Diese Ablehnung bringt erneut die Vorteile der Sofortbenachrichtigung des Absenders. Klassische Mailrelays kannten oftmals nur die internen Domänen und nicht die einzelnen User. Moderne Systeme können per LDAP abfragen, ob ein User vorhanden ist und haben damit ohne zusätzlichen Pflegeaufwand eine stets aktuelle Übersicht der vorhandenen Adressen. In kleinen Unternehmen ohne umfassende Sicherheitsinfrastruktur kann es sinnvoll sein, dem Relay einen direkten Zugriff auf interne Verzeichnisdienste wie Microsoft Active Directory oder openLDAP zu gestatten. Mittlere bis größere Unternehmen dagegen sollten aus Sicherheitsgründen diesen direkten Zugriff nicht gestatten. Dazu ist es wichtig, eine Replik der LDAP-Daten in der DMZ bereitzustellen. Solche Repliken sind oftmals bereits für die Verwendung durch andere sicherheitskritische Systeme vorhanden, die sich ebenfalls anmelden müssen. Steht keine Replik zur Verfügung, kann sie auch direkt am Gateway ohne bedeutsamen Performanceverlust bereitgestellt werden. In einem größeren Unternehmen, das einige Nachrichten pro Sekunde empfängt, ist die Performance einer der entscheidenden Faktoren. Hier empfiehlt es sich, eine Replikationsstruktur aufzubauen, in der Verzeichnisdaten von der Administrations-Konsole aus dem internen Netz direkt zu den Gateways gepusht werden; auf jedem MTA wird eine eigene Replik vorgehalten. Der Mail-Daemon kann mittels der Unix-Domain-Sockets die unzähligen Lookups viel schneller und effizienter als über Inet-Sockets im Netzwerk durchführen.

Skalierbare Filterung

Ein guter MTA sollte in der Lage sein, während aller Sender/Empfänger-Kontrollen Traffic-Statistiken zu führen. Es passiert im Normallfall jedoch selten, dass ein sendendes System eine E-Mail an fünf oder zehn "bad recipients" (nicht-vorhandene Empfänger) zuzustellen versucht; wie es für Directory-Harvesting-Angriffe typisch ist. Darunter versteht man den Versuch, gültige Adressen zu erhalten, um an diese später unerwünschte Nachrichten zu senden. Sollte dabei ein gewisser Schwellwert überschritten werden, muss ein MTA in der Lage sein, die laufende Verbindung zu kappen und weitere, aus der gleichen Quelle kommende Verbindungsversuche zu blocken. Besonders in großen Umgebungen ist es wichtig, dass der Mail-Daemon entweder auf der eigenen Host-Firewall entsprechende Drop-Einträge vornimmt oder besser gleich auf der Unternehmens-Firewall. Diese Einträge sollten stets temporärer Natur sein, um bei einer konzentriert angelegten Spam-Attacke, wie von einem Botnet, keinen Totalausfall des E-Mailverkehrs herbeizuführen.

Verlassen Sie sich
nicht aufs
Bluffen!

Bei Systemausfällen
hilft Ihnen
kein Pokerface weiter!

PRTG – Ihr Ass im Ärmel

bewahrt Sie vor bösen
Überraschungen
in Ihrem Netzwerk.

PRTG Network Monitor
überwacht
Verfügbarkeit • Bandbreite • Auslastung

network Computing
Referenz

PAESSLER
www.paessler.com

Getestet in NWC 10/08

Die klassischen Spam- und Virus-Filter sind bezüglich der Rechenleistung vergleichsweise teuer. Folglich sollten solche Scans erst erfolgen, wenn alle oben beschriebenen Stufen erfolgreich passiert worden sind. In spezifischen Fällen kann auf Content-Scans ganz verzichtet werden, da immer mehr Unternehmensdaten zwischen Systemen automatisiert per E-Mail ausgetauscht werden. Das Ausschließen dieser Machine-to-Machine-Kommunikation von der Inhaltsprüfung spart Rechenzeit. Bei der Wahl des MTAs sollten Sie zudem darauf achten, dass dieser über die Möglichkeit verfügt, Content-Filter verschiedener Anbieter parallel einzusetzen, die Filter aber gleichzeitig leicht austauschbar sind. Das ermöglicht deutlich höhere Erkennungsraten als mit nur einem einzelnen Anbieter. Auch bietet es sich an, die Inhaltsfilter nur als Plug-Ins zu betreiben, um für Änderungen in der Zukunft flexibel zu bleiben.

Trotz bester Content-Filter haben viele Unternehmen Policies über zulässige Dateitypen definiert. So dürfen in vielen Organisationen grundsätzlich keine ausführbaren Dateien per E-Mail ausgetauscht werden, obwohl sie am Gateway meist nicht als schadhaft erkannt werden. Es gibt zum Dateiaustausch geeignetere Methoden als E-Mail, wie FTP und SCP. Ein guter MTA sollte dabei in der Lage sein, nicht nur nach simplen Dateierweiterungen zu arbeiten, sondern auch den echten MIME-Type selber zu ermitteln. Jeder Administrator hat sicher schon erlebt, wie Dateien in .txt umbenannt oder mit Doppelendungen wie .txt.vbs versehen werden, um sie unerkannt an Content-Filtern vorbeizuleiten. Um dieser Gefahr zu begegnen, sollte ein gutes Mailrelay den eigentlichen Dateityp von E-Mailanhängen ermitteln können. Es sollte sich auch nicht auf den MIME-Header verlassen, sondern die Datei verarbeiten und eigenständig den Typ ermitteln.

Zertifizierte Absender

Im Kampf gegen Spam, insbesondere gegen Phishing, setzen sich derzeit neue Standards zur Sender-Authentifizierung durch. Mit diesen kann überprüft werden, ob eine E-Mail, die angeblich vom Absender "kunden.service@meinebank.de" kommt, auch wirklich von dem Kundenservice dieser Bank stammt. Um diese Entscheidung treffen zu können, gibt es zwei Varianten, basierend entweder auf dem von der Nachricht zurückgelegten Weg (Path-Based) wie SPF oder auf der Kryptographie, wie bei DKIM.

Bei der Path-Based Verifizierung, namentlich SPF oder auch SenderID, werden spezielle DNS-Einträge zur jeweiligen Domäne geprüft, um festzustellen, ob ein bestimmter Host E-Mail für die fragliche Domäne verschicken darf. Diese Systeme sind aber nicht besonders robust, die Nachrichten werden außerdem nicht signiert. Für mittlere bis größere Unternehmen ist die Verwaltung von SPF zudem zeit- und ressourcenaufwändig. So wird möglicherweise ein beauftragter Mailing- oder Newsletterversand von Empfängersystemen zurückgewiesen. Aufwändiges Debugging ergibt dann meist, dass vergessen wurde, die SPF-Einträge für diesen Auftrag einzupflegen. Solche Fehleranalyse nimmt einige Zeit in Anspruch und wird oft abteilungsübergreifend.

In dieser Hinsicht erweist sich das kryptographische System DKIM als leistungsstärker und toleranter. DKIM verwendet kryptographische Signaturen für den Message-Body, aber auch für bestimmte Header-Felder. Somit kann durch im DNS bereitgestellte Key-Daten eindeutig sichergestellt werden, dass eine Nachricht tatsächlich vom angegebenen Absender stammt. Die digitale Signatur beweist zudem, dass die Nachricht unterwegs nicht verändert wurde. Erst seit 2007 im RFC4871 verankert, ist der junge Standard noch nicht sehr stark verbreitet. Jedoch setzen ihn bekannte Provider wie GMail, Yahoo! und MobileMe sowie bekannte Unternehmen der Finanzbranche bereits produktiv ein. Da solche Technologien zunehmende Verbreitung finden, ist es besonders wichtig, dass zeitgemäße E-Mail-Infrastrukturen damit umgehen können.

Quarantänehaltung

Viren lassen sich meist eindeutig identifizieren, bei Spam dagegen gibt es oft noch einige Nachrichten, bei denen nur der Verdacht besteht. Meistens weisen diese Nachrichten aber genügend "saubere" Eigenschaften auf, um die Erkennungssysteme zu verunsichern. Aus eben diesem Grund sollte ein gutes Mailgateway unbedingt über eine eigene Quarantäne verfügen, der Anwender sollte dabei in regelmäßigen Abständen eine Kurzfassung über die in der Quarantäne befindlichen Nachrichten erhalten. Diese Benachrichtigung soll am besten mit einem direkten Link versehen werden, damit sich der User im Web-Interface der Quarantäne anmelden kann. Dort darf er seine Nachrichten entweder freigeben oder löschen. Die Erfahrung zeigt, dass eine Integration der Quarantäne ans Groupware-System überflüssig ist, die Nutzer kommen mit Web-Interfaces meist besser zurecht. Eine Integration kann dabei sogar geradewegs zur Kostenfalle mutieren, da das Storage am Groupware-System typischerweise wesentlich teurer ist als der am Gateway. Zusätzlich landet Spam eventuell sogar in Backups und wird damit dauerhaft archiviert.

Policy Layer

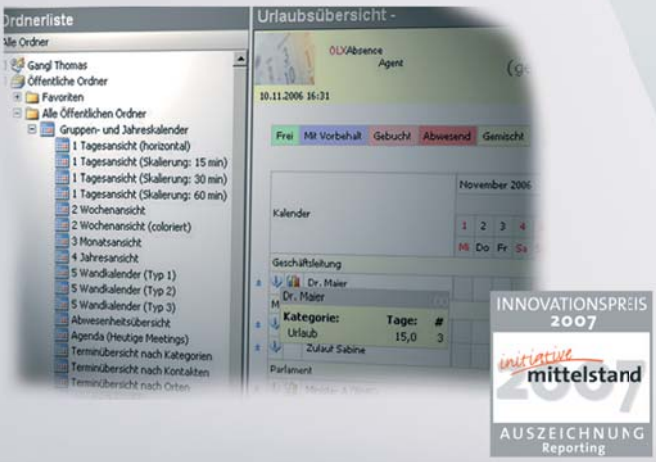
Der Policy-Layer nimmt E-Mails sowohl vom Security-Layer als auch vom Groupware-System entgegen. In einem kleineren Unternehmen kann der Policy-Layer recht kompakt ausfallen, bei Großkonzernen sind die Anforderungen weit umfangreicher, da hier bereits wichtige Routing-Entscheidungen getroffen werden. Weitere Vorgänge, wie zum Beispiel Policy-Verarbeitung und Verschlüsselung werden bei einer modernen, ausgereiften Infrastruktur ebenfalls hier vorgenommen.

Verzeichnisdienst für Groß und Klein

Schon bei kleineren Unternehmen kann es schnell dazukommen, Routing-Entscheidungen auf Basis von im LDAP bereitgestellten Daten treffen zu müssen. Dies ist beispielsweise der Fall, wenn ein zweiter Standort aufgebaut wird. In Großkonzernen ist LDAP-Routing sogar un-

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

Gruppenkalender
Terminmanagement



INNOVATIONSPREIS 2007 initiative mittelstand AUSZEICHNUNG Reporting

Mobiler Zugriff
auch für Öffentliche Ordner

INNOVATIONSPREIS 2007 initiative mittelstand AUSZEICHNUNG Mobile Business

Unternehmensweite
Signaturen & Disclaimer

Individualentwicklung
Vertrauen in Erfahrung

www.gangl.de

Ihr Partner für praxisorientierte Outlook© und Exchange© Lösungen!

Ihre Ansprüche sind unser Ansporn!

✉ info@gangl.de ☎ +49 7173 9290 53

abdingbar. Anhand dieser Daten wird bei jeder eingehenden E-Mail geprüft, auf welchem Groupware-Server in welchem Rechenzentrum das Userkonto vorhanden ist, um eine direkte Zustellung zu ermöglichen. Beim ausgehenden Mailverkehr kann die LDAP Integration ebenfalls relevant sein. Beispielsweise können bei einer einheitlichen E-Maildomäne wie company.com Fußzeilen beziehungsweise Disclaimer je nach absendendem Mitarbeiter länderspezifisch und in seiner Landessprache hinzugefügt werden.

Im Falle einer Firmenübernahme können auch in sauber konzipierten und homogen umgesetzten Umgebungen heterogene Systeme unvorhergesehen hinzukommen. Es ist dann Aufgabe der IT-Abteilung, die Unternehmensnetze schnellstmöglich zusammenzuschließen und die User des neuen Unternehmens auf die bestehenden Systeme zu übernehmen. Meistens lassen sich diese Aufgaben nur durch eine Integration der Mailsysteme schnell umsetzen. Im Messaging-Bereich muss dabei der vollständige E-Mailverkehr zwischen den beiden Netzwerken möglich sein. Microsoft Exchange zum Beispiel kann dabei nur durch komplexe Eingriffe eine E-Maildomäne mit einem weiteren System teilen. In der Praxis werden daher Adressen oftmals am Gateway umgesetzt, um nach außen die Einheitlichkeit zu gewährleisten, während interne Integrationsarbeiten noch durchgeführt werden. Für ein kleines oder mittleres Unternehmen reicht dabei ein simpler Wechsel von firma.de auf neuenname.com oft aus. In großen Unternehmen ist fast immer eine komplexe Umsetzung auf Basis von LDAP-Daten mit verhältnismäßig hohem Zeitaufwand notwendig. Ein moderner MTA ist aber in der Lage, die Umsetzung dieser Anforderungen deutlich zu vereinfachen.

Schutz gegen Datenschwund

Der Schutz gegen Datenverlust, auch DLP (Data Loss Protection) genannt, wird für Firmen unabhängig von ihrer Größe immer wichtiger. Denn selbst die kleinsten Firmen können zu einer Vielzahl gesetzlicher Standards verpflichtet werden. Gesetze, wie zum Beispiel SOX/Euro-SOX oder HIPAA, greifen immer öfter auch für im Ausland ansässige Unternehmensfilialen und Lieferanten. Im medizinischen Bereich gelten dabei besondere Regelungen im Umgang mit Patientendaten, im Finanzbereich sind es Konto- und Zahlungsinformationen. Unternehmen müssen unter anderem sicherstellen, dass ihre Mitarbeiter, gerade auch beim Versand per E-Mail, geschützte Daten aus dem eigenen Netzwerk nicht unkontrolliert verschicken können.

Um dieser Anforderung gerecht zu werden, muss der Inhalt ausgehender E-Mails tiefergehend geprüft werden. Ein MTA sollte dabei zumindest in der Lage sein, die Produkte dritter DLP-Hersteller per Milter-Interface zu integrieren, um diese Regelungen umzusetzen und auffällige E-Mail umzuleiten. Selbst bei einem kleinen Unternehmen kann die langfristige Wettbewerbsfähigkeit beeinflusst werden, da mancher Kundenkreis ausgeschlossen wird. In einem größeren Unternehmen ist die Kontrollautonomie dabei besonders wichtig, um eigene Richtlinien mit entsprechendem Reporting umzusetzen. Die Policy-Engine eines modernen MTAs sollte zudem den Nachrichtenverkehr auf bekannte Zeichenfolgen wie Kreditkarten- und Kontonummern oder Patienten-Kennungen kontrollieren können, um im Problemfall richtlinienkonform einzugreifen.

Virenschutz und Verschlüsselung

Ausgehende E-Mail wird - außer bei Internet-Providern - nur selten auf Spam-Inhalte überprüft. Im Gegensatz dazu müssen ausgehende E-Mails unbedingt auf Viren geprüft werden. Einige der Schädlinge versenden sich selbstständig an Kontakte im lokalen Adressbuch und müssen daher bereits am MTA geblockt werden. Wenn eingehende E-Mail auf Viren geprüft wird, ist die zur Prüfung benötigte Funktionalität in der Regel vorhanden. Beim Entwurf der Architektur ist es wichtig zu berücksichtigen, dass das Mailrelay ausreichende Konfigurationsmöglichkeiten bietet, um auch ausgehende E-Mail auf Viren zu kontrollieren. Nachdem eine E-Mail zum Versand freigegeben wurde, möchte der Absender auch davon ausgehen können, dass die E-Mail sicher übermittelt wird. In manchen Fällen allerdings, wie bei Rechtsanwälten beziehungsweise der Rechtsabteilung einer Firma, ist die Sicherheit geschäftskritisch.

Ein guter MTA sollte nicht nur Verschlüsselung an sich beherrschen, sondern muss auch den Verschlüsselungsstandard vernünftig und richtlinienkonform sicherstellen. Unternehmen konfigurieren ihre Mailgateways idealerweise so, dass etwa E-Mails von der Buchhaltung zum Finanzdienstleister oder von der Chef-Etage zu wichtigen technologischen Partnern automatisiert verschlüsselt werden. Sollte die Verschlüsselung dabei fehlschlagen, wird der Versand auch abgebrochen. Allgemeine E-Mail sollte trotzdem unverschlüsselt verschickt werden dürfen, auch wenn die Verschlüsselung fehlschlägt oder der empfangende MTA kein TLS unterstützt.

Jede Firma hat verschiedene Anforderungen an Reporting- und Monitoring-Funktionen, die sich mit der Zeit auch ändern können. Hier sind Flexibilität, Konfigurierbarkeit und Integrationsfähigkeit die wichtigsten Eigenschaften. Ein SNMP-Interface, das neben Daten vom Betriebssystem auch Statistiken des MTAs selbst be-

Sendmail-MTA

Der Sendmail Mail Transfer Agent ist die am meisten genutzte E-Mailtechnologie im Internet. Seit 1982 vertrauen weltweit Tausende von Unternehmen sowohl auf die Open Source-Lösung als auch auf die kommerziellen Technologien von Sendmail für komplexes, regelbasierendes E-Mailhandling und Routing. Über die Hälfte des weltweiten täglichen Mailaufkommens laufen über Sendmail MTAs. Auf den meisten UNIX-Derivaten gehört der Sendmail MTA zum Lieferumfang. Neben Sendmail sind auf freien Betriebssystemen Alternativen schnell gewachsen: Wietse Venemas Postfix, DJBs Qmail und Philip Hales Exim sind die bekanntesten. Im proprietären Bereich bilden Microsofts Exchange, IBMs Lotus Domino, die Collaboration Suite von Oracle und HPs OpenMail – inzwischen quelloffen unter dem Namen Scalix verfügbar – die allerseits bekannten Größen.

iladministrator

Live-Workshops 2009

Jetzt Plätze sichern und anmelden!

1 München

Exchange 2007

ITANet-Workshop (kostenlos für Abonnenten)
am 05. Februar 2009, 13.00-17.30 Uhr
Dozent: Thomas Joos
Workshop-Partner: IronPort
Anmeldeschluss: 28. Januar 2009

2 Frankfurt/Eschborn

Netzwerksicherheit

ITANet-Workshop (kostenlos für Abonnenten)
am 01. April 2009, 13.00-17.30 Uhr
Dozent: wird noch bekannt gegeben
Workshop-Partner: Realtech
Anmeldeschluss: 23. März 2009

anschließend, am 02. und 03. April 2009:

Data Center Security

Intensivseminar in Kooperation mit Fast Lane
Preis: Euro 1.190,- zzgl. 19% MwSt.
Sonderpreis für IT-Administrator-Abonnenten: Euro 1.071,- zzgl. 19% MwSt.
Anmeldeschluss: 13. März 2009

3 Berlin

Storage-Lösungen für virtualisierte Server

ITANet-Workshop (kostenlos für Abonnenten)
am 28. Mai 2009, 13.00-17.30 Uhr
Dozent: wird noch bekannt gegeben
Workshop-Partner: wird noch bekannt gegeben
Anmeldeschluss: 18. Mai 2009

jetzt anmelden

am darauffolgenden Tag, dem 29. Mai 2009:

Storage-Virtualisierung

Intensivseminar in Kooperation mit Fast Lane
Preis: Euro 700,- zzgl. 19% MwSt.
Sonderpreis für IT-Administrator-Abonnenten: Euro 630,- zzgl. 19% MwSt.
Anmeldeschluss: 08. Mai 2009

4 Heidelberg

Hochverfügbarkeit von Diensten und Applikationen

ITANet-Workshop (kostenlos für Abonnenten)
am 16. Juli 2009, 13.00-17.30 Uhr
Dozent: wird noch bekannt gegeben
Workshop-Partner: Realtech
Anmeldeschluss: 06. Juli 2009

5 Hamburg

E-Mail-Management

ITANet-Workshop (kostenlos für Abonnenten)
am 30. September 2009, 13.00-17.30 Uhr
Dozent: wird noch bekannt gegeben
Workshop-Partner: Gingcom
Anmeldeschluss: 21. September 2009

anschließend, am 01. und 02. Oktober 2009:

SPAM

Intensivseminar in Kooperation mit Fast Lane
Preis: Euro 1.090.- zzgl. 19% MwSt.
Sonderpreis für IT-Administrator-Abonnenten: Euro 981,- zzgl. 19% MwSt.
Anmeldeschluss: 11. September 2009

6 Böblingen

Virtualisierte Infrastrukturen

ITANet-Workshop (kostenlos für Abonnenten)
am 29. Oktober 2009, 13.00-17.30 Uhr
Dozent: wird noch bekannt gegeben
Workshop-Partner: Kroll Ontrack
Anmeldeschluss: 19. Oktober 2009

7 München

Open Source im Mittelstand

ITANet-Workshop (kostenlos für Abonnenten)
am 24. November 2009, 13.00-17.30 Uhr
Dozent: wird noch bekannt gegeben
Workshop-Partner: GeNUA

anschließend, vom 25. bis 27. November 2009:

IT-Security-Workshop

Intensivseminar in Kooperation mit GeNUA
Preis: Euro 1.395,- zzgl. 19% MwSt.
Sonderpreis für IT-Administrator-Abonnenten: Euro 1.245,- zzgl. 19% MwSt.

IT-Administrator Trainings-Partner: GeNUA

IT-Administrator Trainings-Partner: fast lane

ITANet

Die System und Netzwerk User Group

ITANet Schirmherrschaft: REALTECH

Mehr Infos und Anmeldeformulare zu den Veranstaltungen unter

http://www.it-administrator.de/usergroup/termine/

oder per E-Mail an info@itanet.de

reitstellt, gewährleistet diese Funktionen, über ein SMNP kann das Mailgateway direkt in ein beliebiges NMS integriert werden. Das Reporting muss der MTA selbst bereitstellen. Hier sollte besonderes darauf geachtet werden, dass die Reporting-Mechanismen auch End-to-End arbeiten, damit der Weg einer einzelnen E-Mail durch die Messaging-Infrastruktur komplett nachverfolgt werden kann.

Administrierbarkeit

Wenn alle Funktionen analysiert worden sind und alle technischen Anforderungskataloge abgehakt wurden, muss neben den rein fachlichen Ansprüchen noch die Administrationsweise bedacht werden. Für ein kleines Unternehmen ist es sehr wichtig, dass der Administrator auch das Management der Mailgateways selber beherrscht. Ein Dienstleistungsunternehmen kann die Ersteinrichtung übernehmen, aber im täglichen Betrieb sollte sich der Administrator sicher fühlen. Hierzu empfiehlt sich meist ein Web-Interface. Selbst wenn der Admin sämtliche Konfiguration auf der Kommandozeile vornehmen kann, muss eine mögliche Vertretung oder Ersatz ebenfalls mit den Systemen zurechtkommen, falls der Mitarbeiter das Unternehmen verlässt oder sich im Urlaub befindet.

Ein größeres Unternehmen dagegen kennt meistens seine fachlichen Kompetenzen; ist genügend UNIX/Linux-Know-how im Unternehmen vorhanden, bieten sich auch komplex zu administrierende Systeme an. Jedoch geht es bei Großunternehmen meist nicht um kleinere Rechner, sondern um mehrere Maschinen und komplexere Ausfallkonzepte. In größeren Architekturen kommen dabei oft noch Probleme in der Konfigurationssynchronität vor. In der Praxis werden viele Änderungen von einem System zum anderen bei manueller Administration nicht gespiegelt. Dadurch mutiert jeder MTA zu einem undurchsichtigen System und erschwert das Troubleshooting im Problemfall. In diesem Punkt müssen große Unternehmen neben der Konfigurationsweise auch schwer auf die Verteilung der Konfiguration und besonders auf die Cluster-Administration achten. Bessere Systeme können mehrere Gateways über eine Administrations-Konsole verwalten. Es ist wichtig, darauf zu achten, dass die Konsole in der Lage ist, Systemdaten wie etwa IP-Adressen von der Applikationskonfiguration zu trennen und gesondert zu den MTAs zu publizieren.

Fazit

Die schnelle Entwicklung der Kommunikation zwingt kleine Unternehmen zunehmend dazu, in Bezug auf E-Mails wie große Unternehmen zu denken und handeln. Fällt das Mailsystem aus, fällt die komplette Firma aus. Andere Teilsysteme können für den Komplettausfall der Kommunikation nicht einspringen. Um diese wachsende Anforderung zu meistern, setzen Firmen zunehmend auf bewährte Technologien und entwickeln mehrstufige Strategien. *(dr)*

Chris Meidinger ist Messaging Solutions Architect bei Sendmail.

Anforderungen an E-Mailsicherheitslösungen

Merkmal	Kleine Unternehmen	Mittlere Unternehmen	Große Unternehmen
Inhaltsprüfung während der SMTP-Kommunikation	sehr wichtig	sehr wichtig	sehr wichtig
Anti-Spoofing	sehr wichtig	sehr wichtig	sehr wichtig
Authentifizierung gegen interne Verzeichnisse	wichtig	sehr wichtig	weniger wichtig
Relay Domain Check	sehr wichtig	wichtig	weniger wichtig
Recipient Validation per LDAP	weniger wichtig	wichtig	sehr wichtig
LDAP-Directory Replik auf dem MTA	weniger wichtig	wichtig	sehr wichtig
Erkennung von typischem Spam-Verhalten	sehr wichtig	sehr wichtig	sehr wichtig
Schutz gegen DoS durch Firewall-Einträge	wichtig	sehr wichtig	sehr wichtig
Whitelisting von bestimmter E-Mail	wichtig	sehr wichtig	sehr wichtig
Content-Filter als Plug-In	sehr wichtig	sehr wichtig	sehr wichtig
Lokale Erkennung von Dateitypen	wichtig	wichtig	sehr wichtig
Sender-Verification: SPF / DKIM	sehr wichtig	sehr wichtig	sehr wichtig
Eigene Quarantäne	wichtig	sehr wichtig	sehr wichtig
Directory-basierendes, intelligentes Routing	wichtig	sehr wichtig	sehr wichtig
Komplexes Routing zwischen heterogenen Umgebungen	weniger wichtig	wichtig	sehr wichtig
Policy-Kontrollen auf ausgehende E-Mail	weniger wichtig	wichtig	sehr wichtig
Ausgehende Virenprüfung	sehr wichtig	sehr wichtig	sehr wichtig
Policy-basierte Verschlüsselung	weniger wichtig	wichtig	sehr wichtig
Flexibles Reportingsystem	weniger wichtig	sehr wichtig	wichtig
Zentrales Managementsystem	weniger wichtig	wichtig	sehr wichtig

E-Mailumgebungen im Eigenbau

Der Pinguin als Postmaster

von Thomas Hümmler

Mit Fetchmail und Procmail richten Sie Ihre eigene Linux-Mailumgebung ein

Unter Linux werden komplexe Aufgaben in viele kleinere unterteilt. Das gilt vor allem für das Thema E-Mail. Es gibt Programme zum Lesen, zum Transportieren und Abholen, zum Sammeln von Mailadressen oder auch zum automatischen Weiterleiten. Sind diese passend konfiguriert, wird E-Mail zum reinen Vergnügen. In diesem Workshop zeigen wir Ihnen Schritt für Schritt den Aufbau einer E-Mailumgebung unter Linux.

Mit Fetchmail holen Sie E-Mails für beliebig viele Benutzer bei beliebig vielen Providern ab. Dabei spielt es keine Rolle, ob auf der anderen Seite ein POP-, IMAP- (Version 2 bis 4) oder ein ETRN-Server steht – Fetchmail unterstützt alle gängigen Protokolle und leitet sie an einen so genannten MDA (Mail D Agent = Mailverteiler) wie Procmail weiter. Unter Debian installieren Sie Fetchmail mit dem Befehl

```
apt-get install fetchmail
```

Dabei wird das "fetchmail"-Skript im Verzeichnis "/etc/init.d" erzeugt. Damit dieses Skript als Daemon startet, sind zwei Voraussetzungen erforderlich: die Konfigurationsdatei */etc/fetchmailrc* muss vorhanden sein und in der Datei */etc/default/fetchmail* muss die Zeile *START_DAEMON=yes* stehen. Zu Beginn existiert die Datei */etc/fetchmailrc* noch nicht. Sie können sie aber leicht mit Hilfe der Beispielkonfiguration unter */usr/share/doc/fetchmail/examples/fetchmailrc.example* einrichten (siehe Kasten "Fetchmails Beispieldatei"). Kopieren Sie diese Datei als Root mit dem Befehl

```
cp /usr/share/doc/fetchmail/exam-
  ples/fetchmailrc.example
  /etc/fetchmailrc
```

in das Verzeichnis */etc* und öffnen Sie sie in einem Editor. Löschen Sie in der Zeile "#set daemon 300" das Kommentarzeichen und geben Sie ein Intervall in Sekunden an, in dem Fetchmail Nachrichten abrufen soll. Ändern Sie die Vorgabe von "300" (fünf Minuten) auf "3600", wenn Fetchmail einmal stündlich Mails abholen soll.

Mails vom Server holen

Nun geben Sie anhand unseres Beispiels unter "Server Section" ganz unten in der Beispieldatei die Postfächer und lokalen Benutzer an. Dazu dienen die folgenden Schlüsselwörter:

- "poll": Gibt den Server an, von dem Post geholt werden soll.
- "proto" oder "protocol": Gültige Werte für das zu verwendende Protokoll sind "AUTO" oder die manuelle Festlegung auf "POP2", "POP3", "APOP", "RPOP", "KPOP", "SDPS", "IMAP" (die Version sucht Fetchmail selbst heraus), "ETRN" oder "ODMR".
- "timeout": Zeit in Sekunden, wie lange Fetchmail versucht, sich mit einem Server zu verbinden (Standard: 300 Sekunden). Diese Angabe ist nicht unbedingt erforderlich; geht bei der Verbindung etwas schief, wird nicht weiter angewählt, sondern erst nach Ablauf des Daemon-Intervalls ein neuer Versuch unternommen.
- "user" oder "username": Der Benutzername auf dem Mailserver.
- "pass" oder "password": Das Passwort für den Mailserver.
- "is {BENUTZERNAME} here": {BENUTZERNAME} steht für den lokalen Benutzernamen.

Falls Fetchmail einen Fehler wie "fetchmail: Command not supported." in der Log-Datei meldet, können Sie das getrost ignorieren. Das liegt daran, dass das POP3-Protokoll seit RFC 1725 vom November 1994 den Befehl *LAST* zum Melden der letzten Nachricht nicht mehr unterstützt. Fetchmail hält sich hier nicht an die Standards und schickt den LAST-Befehl weiterhin an POP3-Server, die daraufhin einen Fehler melden, der zur erwähnten Fehlermeldung führt.

Fehler: Command not supported

Für einen einzigen Mail-Account, etwa bei T-Online, sieht der Eintrag etwa so aus:

```
poll pop.t-online.de
protocol pop3
timeout 120
username "AAAAAAAAAA-
  AATTTTTTTTT#0001"
password "{Passwort}"
is {Benutzername} here
```

Die Zeile mit dem Benutzernamen setzt sich bei T-Online zusammen aus der zwölfstelligen Anschlusskennung (A), der T-Online-Nummer (T), einem Doppelkreuz (#) und der Mitbenutzernummer (meist "0001"). Das Passwort setzen Sie ebenso wie den Benutzernamen in Anführungszeichen.

Fetchmail für mehrere Benutzer

Wollen Sie Fetchmail für mehrere Benutzer einrichten, kopieren Sie das Beispiel und fügen es darunter mit den weiteren Werten für "poll", "protocol", "username", "password" und Benutzernamen ein. Existieren bei einem Provider mehrere E-Mail-konten, können Sie die Server-Optionen vorweg zusammenfassen:

```
defaults "pop.onlinehome.de"
protocol pop3
timeout 120
```

Das Schlüsselwort "defaults" statt "poll" besagt, dass für alle folgenden E-Mail-Konten der gleiche Server gilt (ein Einzelner kann trotzdem immer wieder mit "poll" dazwischen geschoben werden). Erst danach folgen die Einträge mit den Benutzeroptionen:

```
username "{BENUTZER-1}"
password "{PASSWORT-1}"
is {BENUTZER-1} here

username "{BENUTZER-2}"
password "{PASSWORT-2}"
is {BENUTZER-2} here

username "{BENUTZER-3}"
password "{PASSWORT-3}"
is {BENUTZER-3} here
```

Weitere Beispiele für Server-Anweisungen stehen in der sehr ausführlichen, allerdings englischsprachigen Man-Page "fetchmailrc". Wichtig: Als Besitzer der Datei tragen Sie den Benutzer "fetchmail" ein:

```
chown fetchmail /etc/fetchmailrc
```

Außerdem sollten Sie die Datei anschließend mit dem Befehl *chmod 600 /etc/fetchmailrc* nur für den Benutzer fetchmail beziehungsweise für Root einsehbar machen. Sonst kann jeder mit Zugang zum Rechner die Benutzernamen und Passwörter herausfinden. Starten Sie danach mit

```
/etc/init.d/fetchmail restart
```

den Daemon. Sofern Sie keine andere Log-Datei angegeben haben, können Sie in der Datei */var/log/syslog* die Aktivitäten Fetchmails beobachten. Sollte Fetchmail nicht starten, enthält die Datei */etc/fetchmailrc* vermutlich einen oder mehrere Syntaxfehler. In dem Fall sollten Sie als Root den Befehl

```
/etc/init.d/fetchmail debug-run
```

ausführen, um die Ursache zu ermitteln. Allerdings können Sie mit der Option "debug-run" keine Fehler entdecken, die nur im Daemon-Modus vorkommen.

Procmail einrichten

Nachdem Fetchmail die Nachrichten abgeholt und den Benutzern ins Postfach kopiert hat, können Sie dort Procmail [1] zwischenschalten und diesem Pro-

```
# /etc/fetchmailrc for system-wide daemon mode
# This file must be chmod 0600, owner fetchmail
# The default for this option is 300, which polls the server every 5
# minutes.
#
#set daemon 300
# By default, the system-wide fetchmail will output logging messages to
# syslog; uncomment the line below to disable this. This might be useful
# if you are logging to another file using the 'logfile' option.
#
# set no syslog
# Avoid loss on 4xx errors. On the other hand, 5xx errors get more
# dangerous.
#
set no bouncemail
# The following defaults are used when connecting to any server, and can
# be overridden in the server description below.
#
# Set antispam to -1, since it is far safer to use that together with no
# bouncemail.
#
defaults:
antispam -1
batchlimit 100

# Example server section.
#
#poll foo.bar.org with protocol pop3
# user baka there is localbaka here smtphost smtp.foo.bar.org;
```

Fetchmail Beispieldatei

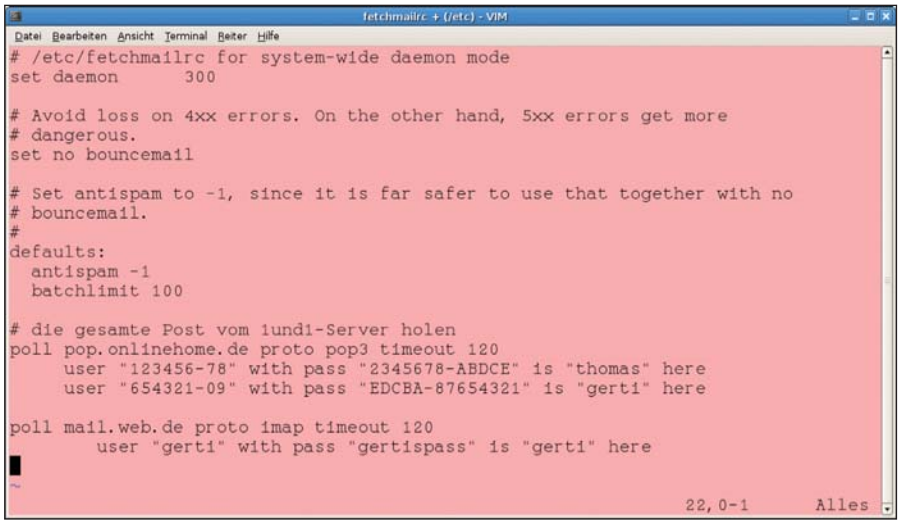


Bild 1: Mit Fetchmail sammeln Sie die Mails von einem oder auch mehreren Providern für einen oder mehrere Benutzer Ihres Systems ein

gramm die E-Mails zur weiteren Bearbeitung überlassen. Procmail ist unter Linux der Spezialist zum Filtern, Verschieben, Löschen, Weiterleiten und Beantworten von Mails. Das Werkzeug kann aber noch mehr: einen Mailserver erstellen, Mailing-Listen verwalten, Mails vor dem Lesen bearbeiten oder bestimmte Programme bei der Ankunft von Mails starten. Mit dem ebenfalls im Procmail-Paket enthaltenen Programm Formail erzeugen Sie unter anderem Auto-Replys, teilen Listen-Digests wieder in die originalen Nachrichten auf oder manipulieren Kopfzeilen.

Läuft ein Mailserver mit Exim oder Sendmail, funktioniert auch Procmail bereits und Sie müssen es nur noch konfigurieren. Möchten Sie Procmail systemweit einrichten, nutzen Sie die Datei */etc/procmailrc*. Diese läuft eventuell mit Root-Rechten und muss entsprechend vorsichtig gehandhabt werden. Es bietet sich jedoch eher an, eine rc-Datei mit Benutzerrechten in den jeweiligen Home-Verzeichnissen anzulegen:

```
touch ~/.procmailrc
```

Anschließend schreiben Sie nur noch die Procmail-Anweisungen ("Rezepte" genannt) in diese versteckte Datei. Es gibt zwei Arten Rezepte: E-Mail-auslieferndе und nicht-auslieferndе. Trifft ein auslieferndes Rezept zu, betrachtet Procmail die Mail als zugestellt und beendet die rc-Datei, nachdem die Befehlszeile des jeweiligen Rezepts ausgeführt wurde. Trifft ein nicht-auslieferndes Rezept zu, wird die rc-Datei nach Ausführen der Befehlszeile weiter abgearbeitet. Rezepte beginnen mit einem Doppelpunkt (:) und haben das folgende Format:

```
:0 [flags] [ : [locallockfile] ]
```

Dabei sind entweder keine oder mehrere Bedingungen möglich (eine pro Zeile) und das Rezept muss in einer Befehlszeile stehen. Es gibt mehrere Flags, die auch kombiniert werden können:

- "H": untersucht den Header einer Mail (das ist die Voreinstellung)
- "B": untersucht den Body einer Mail
- "D": unterscheidet zwischen Groß- und Kleinschreibung (standardmäßig keine Unterscheidung)
- "A": Rezept wird nicht ausgeführt, bis die Bedingungen im letzten vorhergehenden Rezept ohne "A"- oder "a"-Flag ebenfalls zutreffen (dient zum Verbinden von Aktionen, die von einer gemeinsamen Bedingung abhängen)
- "a": Hat die gleiche Bedeutung wie das "A"-Flag, zusätzlich muss das vorhergehende Rezept erfolgreich beendet sein
- "E": Rezept wird nur ausgeführt, wenn das vorhergehende Rezept nicht ausgeführt wurde (damit können Sie "else-if"-Bedingungen ausführen)
- "e": Rezept wird nur ausgeführt, wenn die Befehlszeile des vorhergehenden Rezepts einen Fehler erzeugt hat
- "h": leitet den Header in eine Pipe, eine Datei oder an ein Mail-Ziel (Voreinstellung)
- "b": leitet den Body in eine Pipe, eine Datei oder an ein Mail-Ziel (Voreinstellung)
- "f": betrachtet die Pipe als Filter
- "c": erzeugt eine Kopie der Mail
- "w": wartet, bis Filter oder Programm beendet ist und prüft den Exit-Code; war der Filter erfolglos, wird der Text nicht gefiltert
- "W": wie das "w"-Flag, unterdrückt aber alle Programmfehlermeldungen
- "i": ignoriert alle Schreibfehler in diesem Rezept (etwa wegen einer zu früh geschlossenen Pipe)
- "r": Raw-Modus; versucht nicht, die Mail mit einer Leerzeile abzuschließen, sondern schreibt das, was kommt

Sie können auch eine Lock-Datei angeben. Diese sperrt für normalerweise acht Sekunden die weitere Ausführung, damit es nicht zu Kollisionen zwischen den bearbeitenden Programmen kommt und Mails eventuell zerstört würden.

Bedingungen starten mit einem Stern (*); alles, was danach folgt, wird intern wei-

www.realtech.de/bpm

Was brauchen Sie mehr?

... als ein Business Process Management, das IT-Daten mit Informationen aus ERP-Systemen verknüpft und bedarfsgerecht aufbereitete Kennzahlen für Ihr Management und Ihre IT-Administration bereitstellt.

Erfahren Sie mehr unter:
www.realtech.de/bpm

REALTECH

REALTECH AG
Tel.: +49.6227.837.651
bpm@realtech.de · www.realtech.de/bpm

terverarbeitet, außer führende und angehängte Leerzeichen. Mehrere Bedingungen müssen alle zutreffen; geben Sie keine Bedingung an, gilt die Bedingung als erfüllt und die Befehlszeile wird ausgeführt. Es gibt außerdem ein paar spezielle Bedingungen, die direkt auf den Stern folgen:

- "!": invertiert die Bedingung
- "$": berechnet den Rest der Bedingung gemäß den Ersetzungsregeln in doppelten Anführungszeichen des "sh(1)"-Befehls, entfernt führende Leerräume und analysiert erneut.
- "?": nutzt den Exit-Code des hier spezifizierten Programms.
- "<": prüft, ob die Mail kürzer ist als die angegebene Zahl (dezimal) an Byte.
- ">": prüft, ob die Mail länger ist als die angegebene Zahl (dezimal) an Byte.
- "Variablenname ??": prüft den Rest der Bedingung gegen den Wert der Umgebungsvariable; ist der Variablenname "B", "H", "HB" oder "BH", ändert dieses lediglich den Standardsuchbereich des Rezepts.
- "\": vor eine Sonderbedingung gesetzt, wird diese als normales Zeichen interpretiert (Quoten).

Die Befehlszeile schließlich kann mit einem der folgenden Zeichen beginnen:

- "!": leitet alles an die angegebene Mail-Adresse weiter.
- "|": startet das angegebene Programm. Steht vor dem Pipe-Symbol eine Variable der Art "VARIABLE=", wird die Standardausgabe des Programms in der Umgebungsvariablen gespeichert. Das Pipe-Symbol allein ohne ein Programm leitet die Mail an die Standardausgabe.
- "{": folgt auf die geschweifte Klammer mindestens ein Leerzeichen, Tabulator oder eine Zeilenschaltung, markiert das den Anfang eines verschachtelten Blocks. Alles bis zur nächsten schließenden Klammer hängt von den Bedingungen dieses Rezepts ab. Tiefere Verschachtelungen sind erlaubt. Ist das Ende eines Blocks erreicht, wird normal weitergearbeitet. In einem Block betreffen die "H"- und "B"-Flags nur die Bedingungen, die zum Block führen; die "h"- und "b"-Flags haben dagegen überhaupt keine Auswirkungen.

Alles andere wird als Mailbox-Name betrachtet – entweder ein Mailverzeichnis oder eine Maildatei. Handelt es sich um eine Datei, wird die E-Mail an diese angehängt. Ein paar Beispiele für Procmail-Rezepte finden Sie im nachfolgenden Abschnitt. Weitere Beispiele stehen unter Debian im Verzeichnis */usr/share/doc/procmail/examples/* zur Verfügung.

Procmail-Rezepte

Nachfolgend zeigen wir Ihnen einige Beispiele zur Procmail-Nutzung auf. Um E-Mails der deutschen Debian-User-Liste an die Mailbox "in-l-debian-user" anzuhängen, geben Sie die folgenden Zeilen ein:

```
:0:
* ^X-Mailing-List:.*debian-user-
  german
in-l-debian-user
```

Mails der Procmail-Users-Liste hängen Sie mit den folgenden Zeilen an die Mailbox "in-l-procmail" an:

```
:0:
* ^List-Id:.*procmail.lists
in-l-procmail
```

Die Listenkennungen löschen Sie mit

```
:0 fhw
* ^Subject:[ \t]*(Re:
  )?(=\?((iso|ISO)-8859-1(5)?|wind-
  ows-1252)\?Q\?)?(Re(\[2\])?
  (:|=3A)?( |_|=20))?(\[|=5B)\
(announce|debian|(de-)?users(_de)?)\
(\]|=5D)([ _]|=20)?
| perl -pe 's/(\[|=5B)(announce|
  debian|(de-)?users(_de)?)(\]|=5D)
  ([ _]|=20)?//g'
```

"AW: ", "RE: ", "Re:" und ähnliche in "Re: " ändern:

```
:0 fhw
* ^Subject:[ \t]*(=\?(ISO-8859-
  1(5)?|Windows-1252)\?Q\?)?
  (RE|Re:\s*Re|Re\[2\]|AW|AW\.|Aw|An
  tw|Antwort|Betr.|
  Betreff|WG)(:|=3A)
| perl -pe
  's/((RE|Re(\[2\])?|AW|AW\.|Aw|Antw
  |Antwort|Betr.|Betreff|WG)(:|=3A)
  ( |_)?\s*)+/Re: /g'
```

Pressemitteilungen, -meldungen und -informationen im Subject an die Mailbox "in-pressemitteilungen" anhängen:

```
0:
* ^Subject:.*(P|p)resse(mit|mel|
  inf|[ ]*-[ ]*Inf)
in-pressemitteilungen
```

Mails für thomas@thomas.net an den Benutzer thomas weiterleiten:

```
:0c
* ^TO_thomas@thomas.net
! thomas
```

Die Sommerzeitregel ändert die Zeit auf Sommerzeit:

```
:0 fhw
* ^FROM:.*Heribert Schnurzegal
* ^Date:.*0100$
| perl -pe 's/0100/0200/i'
```

Ist Ihr Mailserver nicht direkt mit dem Internet verbunden und Spamassassin folglich nicht auf SMTP-Ebene im Einsatz, überlassen Sie Procmail das Aussortieren von Spam. Die folgenden Zeilen prüfen Mails und verschieben Spam-Mitteilungen mit 15 Spam-Punkten in den Ordner "SPAM-wahrscheinlich", andere in den Mail-Ordner "SPAM-vermutlich":

```
:0fw: spamc.lock
* < 256000
| spamc
:0:
* ^X-Spam-Level:
  \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
SPAM-wahrscheinlich
:0:
* ^X-Spam-Status: Yes
SPAM-vermutlich
```

E-Mails weiterleiten

Mit Hilfe von Procmail können Sie auch Mails weiterleiten. Das Rezept

```
:0c
* ^TO_thomas@thomas.net
! thomas
```

etwa sorgt dafür, dass E-Mails an die Adresse "thomas@thomas.net" an den Benutzer namens thomas weitergeleitet werden. Das geht aber auch einfacher – mit der Datei *.forward* im Home-Verzeichnis. Diese existiert zunächst nicht. Falls Sie sich entschließen, sie als Benutzer mit

```
touch ~/.forward
```

in Ihrem Home-Verzeichnis anzulegen, können Sie Anweisungen hineinschreiben, wie mit ankommenden Mails verfahren werden soll. Steht in der Datei nichts oder existiert sie überhaupt nicht, passiert einfach nichts. Im einfachsten Fall schreiben Sie in die Datei eine E-Mail-Adresse, an die alle Nachrichten weitergeleitet werden. Der Eintrag

```
thomas@irgendwo.unterwegs.de
```

schickt alle ankommenden Mails an diese Adresse weiter. Arbeiten Sie im Büro mit Linux und will sich in der Zeit Ihrer Abwesenheit eine Kollegin oder ein Kollege um Ihre Post kümmern, tragen Sie einfach den Benutzernamen in die .forward-Datei ein: *\kollegin*. Auf den Rückstrich können Sie auch verzichten. Schreiben Sie ihn aber an den Anfang der Zeile, werden Mails direkt in die Mail-Spool-Datei des anderen Benutzers geschrieben, ohne weitere Umleitungen zu beachten. Insofern bietet es sich an, den Eintrag als letzten in die .forward-Datei zu schreiben. Auf keinen Fall sollten Sie aber einen Vorwärtsstrich ("/kollege") nutzen. Dann versucht Linux nämlich, ankommende Mails mit einfachen Benutzerrechten in der Datei "kollegin" im Wurzelverzeichnis abzulegen. Das funktioniert auf einem Unix-System natürlich nicht und hat zur Folge, dass der Absender eine Nachricht erhält, dass seine Mail nicht zugestellt werden konnte.

Die Einträge in der .forward-Datei können Sie beliebig kombinieren. Jede ankommende Mail wird an alle eingetragenen Adressen und Benutzer weitergeleitet. Möchten Sie Mails zum Beispiel an eine externe Adresse ebenso weiterleiten wie an die Kollegin und auch selbst noch eine Kopie behalten, dann schreiben Sie drei Einträge in die Datei:

```
thomas@irgendwo.unterwegs.de
\kollegin
\thomas
```

So werden ankommende Nachrichten an Ihre externe Adresse, an die Kollegin und in Ihr eigenes Postfach weitergeleitet (tragen Sie statt "thomas" Ihren Benutzernamen ein). Sollte die Kollegin ebenfalls in Urlaub gehen, erzeugt sie eine eigene .forward-Datei in ihrem Home-Verzeichnis und trägt dort einen weiteren Mitarbeiter ein, der dann die Mails der Kollegin und Ihre Mails erhält. Sind Sie dann wieder im Büro, löschen Sie den Benutzernamen der Kollegin aus Ihrer .forward-Datei und Ihre Mails werden nicht mehr an andere Mitarbeiter weitergeleitet. Vermeiden Sie jedoch beim Weiterleiten die Bildung von Schleifen. Mails, die an eine andere Adresse weitergeleitet werden, dürfen von dort nicht wieder an die ursprüngliche Adresse zurückgeschickt oder weitergeleitet werden.

Gerade in einen Netzwerk mit mehreren Benutzern sollten Sie zudem darauf achten, dass nur Sie als Eigentümer Schreibrechte in der Datei haben (Modus 644). Falls nicht, könnten sich andere Ihrer Mails bemächtigen, indem Sie die Einträge ändern. Normalerweise wird die Datei mit diesen Dateirechten angelegt, mit einem *ls -l ~/.forward* können Sie sich aber noch von den korrekten Dateirechten überzeugen.

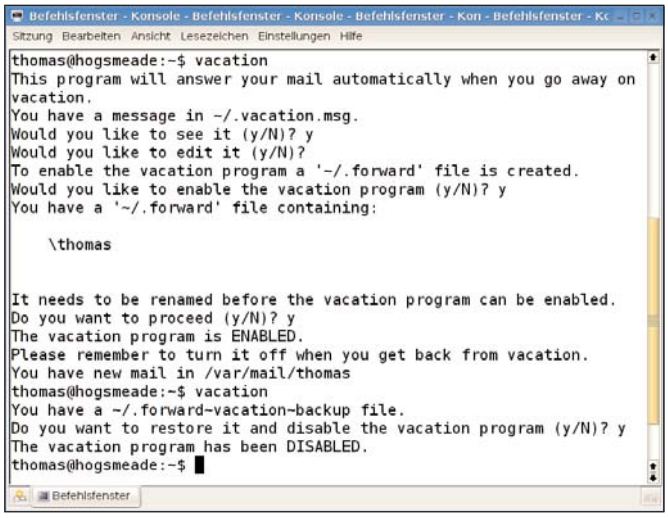


Bild 2: Die Abwesenheitsmeldung mit vacation erzeugen Sie mit dem Programmaufruf auf einer Textkonsole

Out-of-Office-Meldungen mit Vacation

Anstelle einer Mailadresse können Sie in der .forward-Datei auch ein Programm eintragen, an das die Mails als Standard-Input weitergereicht werden sollen. In dem Fall schreiben Sie das Pipe-Symbol (|) vor den Programmnamen, etwa so:

```
"|/usr/bin/vacation"
```

Die Anführungszeichen sind eigentlich erst dann erforderlich, wenn Sie dem Programm weitere Argumente und Parameter übergeben.

Das Programm vacation sendet Anderen auf ihre Mails eine Antwort, wenn Sie gerade nicht da sind. Das Tool wurde ebenso wie der Mailserver sendmail von Eric Allman entwickelt, der als Vater der modernen Internet-E-Mail gilt. Im Gegensatz zu einfachen Out-of-Office-Meldungen, wie sie etwa Outlook erzeugt, können Sie das 1983 entwickelte vacation sehr individuell anpassen. Unter OpenSuse Linux installieren Sie es im YaST-Kontrollzentrum, in Debian

und Kubuntu mit dem Befehl *apt-get install vacation*. Nur fünf Dateien stecken im Debian-Paket vacation – drei Textdateien mit Hinweisen zu Urheberrechten und Programmänderungen, eine Man-Page sowie die eigentliche Programmdatei vacation. In OpenSuse sind im vacation-Paket außerdem das Programm vaclook (das vacation mit dem Parameter "-l" startet) mit dazugehöriger Man-Page sowie die Man-Page zu forward zum Weiterleiten von Mails enthalten. Mit vaclook können Sie die Datei *.vacation.db* im Home-Verzeichnis ansehen. Diese enthält die Adressen, denen eine Abwesenheitsmitteilung geschickt wurde mit Zeit und Datum der Meldung.

Die Abwesenheitsheitsmeldung ist schnell erstellt. Starten Sie vacation ohne Parameter in einer Textkonsole, können Sie automatisch eine Mitteilung erzeugen und die entsprechenden Einträge in die .forward-Datei schreiben. Eine vorhandene .forward-Datei wird gesichert, sie heißt anschließend ".forward~vacation~backup". Beim nächsten Start von vacation – nach dem Urlaub – wird diese Backup-Datei wieder zurückgeschrieben und die Abwesenheitsmeldungen wieder ausgeschaltet. Die von vacation erzeugte neue .forward-Datei enthält nur die Zeile

```
thomas, "|/usr/bin/vacation thomas"
```

mit Ihrem Benutzernamen und dem vacation-Programmaufruf, dem als Parameter der Benutzername übergeben wird. Diese Zeile müssen Sie anpassen, wenn der Benutzername nicht auch Teil Ihrer E-Mail-Adresse ist – ansonsten reagiert vacation nur auf interne Mails. Um dem Programm einen Bestandteil Ihrer E-Mail-Adresse mitzuteilen, benutzen Sie den Parameter "-a Alias". Dann könnte die .forward-Zeile beispielsweise so aussehen:

```
thomas, "|/usr/bin/vacation -a
  huemmler thomas"
```

Nun erhalten alle Mails eine Antwort, die "thomas" oder "huemmler" als Bestandteil im "To"- oder "Cc"-Header enthalten. Sollen noch andere Weiterleitungen berücksichtigt werden, müssen Sie die .forward-Datei wie oben beschrieben noch weiter anpassen.

Die Mitteilung, die jeweils an die Mail-Absender geschickt wird, steht in der versteckten Datei .vacation.msg und hat zunächst folgenden Inhalt:

```
Subject: away from my mail
I will not be reading my mail for a
  while.
Your mail concerning "$SUBJECT"
will be read when I return.
```

In einem Editor passen Sie die Datei schnell an. Die Zeichenfolge "$SUBJECT" wird in der Mitteilung durch den Betreff ersetzt. Andere Platzhalter akzeptiert das Programm nicht. Allerdings können Sie weitere Header-Zeilen einfügen, etwa so (achten Sie darauf, dass zwischen den Header-Zeilen und dem Text in der Datei *.vacation.msg* eine Leerzeile steht):

```
From: mir@meinefirma.de (ich selbst)
Subject: Ihre Mail von gerade eben
  ...
Precedence: bulk

... mit dem Betreff "$SUBJECT" ist
  in meinen Postfach angekommen. Da
  ich bis einschließlich Ostermontag
  nicht im Büro bin, werde ich Ihre
  Mitteilung erst danach lesen. Wenn
  Sie so lange nicht warten können,
  wenden Sie sich an meine Kollegin
  (kollegin@meinefirma.de).
```

Den Empfänger der Mitteilung übernimmt vacation aus der Header-Zeile, die mit "Return-Path" oder mit "From" beginnt. Sind beide Header-Zeilen vorhanden, wird die "Return-Path"-Adresse benutzt. Keine Rückmeldung gibt es auf Mails, bei denen "Precedence: bulk", "Precedence: junk" oder "Precedence: list" im Mail-Header steht. Ebenfalls nicht beantwortet werden Nachrichten von "???-REQUEST", "Postmaster", "UUCP", "MAILER" oder "MAILER-DAEMON" – unabhängig von der Schreibweise. Wer alles eine Antwort bekommen hat, steht nach dem Urlaub in der versteckten Datei *.vacation.db* im Home-Verzeichnis.

Kleiner Bruder als Adressensammler

Ein Tool, auf das vor allem Benutzer des Mailprogramms Mutt [2] nicht verzichten sollten, ist die Little Brother's Database von Roland Rosenfeld [3]. Dieses Programm sammelt mit Hilfe von Prcomail aus allen ankommenden Mails die Absender und schreibt sie in eine Datei. Dazu müssen Sie lediglich die zwei Zeilen

```
:0hc
| lbdb-fetchaddr
```

in die Datei *~/.procmail* schreiben. Anschließend wird die Little Brother's Database in Mutt mit dem "query_command" als Abfrage-Datenbank festgelegt:

```
set query_command="lbdbq %s"
```

Suchen Sie nun eine E-Mailadresse, geben Sie einfach "m" für eine neue Mail ein, schreiben ein Fragment des Namens und drücken "Strg+T". Damit wird in der Datenbank nach der Zeichenfolge gesucht und alle Namen, die diese enthalten, angezeigt. Mit den Cursor-Tasten wählen Sie die Gesuchte und mit "Eingabe" übernehmen Sie diese. *(dr)*

Links

[1] Procmail
www.procmail.org

[2] Mailprogramm Mutt
www.mutt.org

[3] Brother's Database von Roland Rosenfeld
www.spinnaker.de/lbdb

Active Directory mit Tools exportieren, dokumentieren und durchsuchen

Wer sucht, der findet

von Nils Kaczenski

Mit den richtigen Werkzeugen lässt sich das Active Directory einfach dokumentieren und durchforsten

Ein guter Admin dokumentiert – wenn auch meistens nur widerwillig. Gut, wenn es für Teilbereiche des Netzwerks einfache Werkzeuge gibt, die den Netzwerkverwalter bei dieser Arbeit unterstützen: Wer seine Windows-Domäne unter Active Directory dokumentieren oder gezielt darin suchen möchte, findet gleich eine ganze Auswahl an kostenlosen Tools. Mit ihnen erledigt sich die lästige Pflicht im Handumdrehen.

Beginnen möchten wir unseren Workshop mit einem sehr nützlichen Tool, das sich seit Windows 2000 auf jedem Server findet: "CSV Directory Exchange" oder einfach *csvde.exe*. Um es von einem Client aus zu nutzen, kopieren Sie es dorthin; erst Vista bringt es selbst mit. Mit dem Werkzeug exportieren und importieren Sie Daten aus beziehungsweise in das Active Directory (AD). Allerdings eignet sich der Import nur für einfache Objekte wie Kontakte, da *csvde.exe* keine Kennwörter setzen kann. Auch kann es vorhandene Objekte nicht verändern, sondern nur neue erzeugen.

Export der AD-Informationen

Zum Exportieren ist CSV Directory Exchange aber sehr hilfreich, weil es mit dem Betriebssystem installiert wird. Es erzeugt einen Textauszug des AD im CSV-Format (Comma-separated Values), also als Text-Tabelle. Eine solche Datei können Sie etwa mit Excel bequem öffnen. Den Export definieren Sie mit LDAP-Fragmenten. Alle Benutzer der OU "EDV" geben Sie zum Beispiel mit folgendem Befehl in die Datei *EDV-Benutzer.txt* aus:

```
csvde -f EDV-Benutzer -r "(&(object-
  Class=user)(objectCategory=per-
  son))" -d "OU=EDV,DC=domain,DC=de"
```

Dabei exportiert *csvde.exe* alle Felder, die es im Active Directory findet. Geben Sie den Schalter "-n" an, so unterdrückt das Programm alle Binärwerte, die nur für die AD-Replikation relevant sind. Interessieren Sie sich nur für bestimmte Werte, können Sie die nötigen Attribute mit "-l" angeben. Das folgende Beispiel gibt die wichtigsten Felder für alle Computer aus, wenn Daten über Service Packs gefragt sind:

```
csvde -m -f Computer.txt -r
  "(&(objectClass=user)(object
  Category=computer))" -l name,
  adsPath,operatingsystem,operating-
  systemversion,operatingsystemser-
  vicepack
```

In deutschsprachigen Umgebungen werden Sie oft auf Daten treffen, die Umlaute enthalten. Solche Werte gibt das Tool dann unleserlich codiert aus. Um dem abzuhelfen, nutzen Sie den Schalter "-u", der in manchen CSVDE-Versionen nicht dokumentiert ist:

```
csvde -u -f Kontakte.txt -r "(&(ob-
  jectClass=contact))" -l displayNa-
  me,sn,givenName
```

Auch Daten aus dem Schema oder aus der Konfiguration-Partition des AD gibt das Werkzeug aus. Nutzen Sie den Schalter "-d", um eine andere Suchbasis als die Standard-Domäne anzusprechen. Die folgende Zeile gibt einen Überblick über das im Forest gültige Schema:

```
csvde -f Schema.txt -d
  "CN=Schema,CN=Configuration,DC=
  domain,DC=de" -r "(|(objectClass=
  attributeSchema)(objectClass=class
  Schema))" -l name,mayContain,must-
  Contain,objectClass, subClassOf,
  attributeID,isSingleValued,lDAP-
  DisplayName"
```

Auf diese Weise machen Sie auch Schema-Erweiterungen ausfindig: Vergleichen Sie die Ausgabe eines solchen Kommandos von Ihrem System mit der Ausgabe eines Referenzsystems. Schema-Objekte, die in dem Referenzsystem fehlen, müssen von nachträglichen Erweiterungen stammen. Einige Hilfsmittel dazu liefert der Web-Artikel unter [1].

AdFind: Umfassende Active Directory-Suche

Ein sehr flexibles Werkzeug zur Suche von Daten im Active Directory hat der amerikanische MVP Joe Richards geschrieben. Es heißt AdFind und findet sich kostenlos unter [2]. AdFind ist ein Kommandozeilentool mit einer Vielzahl von Schaltern, durch die es leider auf den ers-

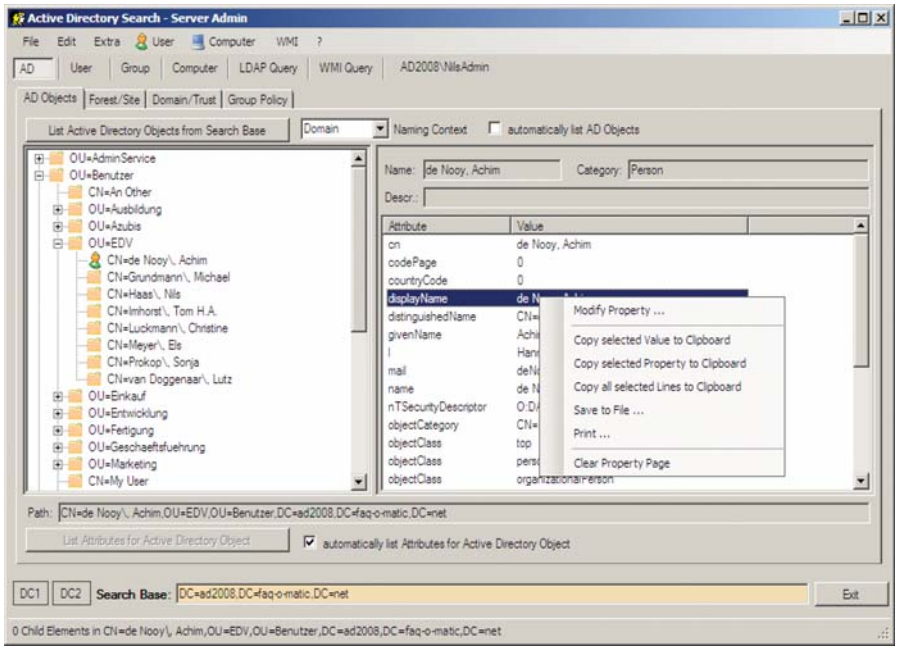


Bild 1: ADsearchAdmin listet im Hauptfenster die Domänenstruktur auf und zeigt alle Details des gewählten Objekts. Viele Werte können Sie dabei direkt bearbeiten.

ten Blick recht komplex ist. Folgendes Kommando findet Benutzer, deren Anmeldename mit "N" beginnt und gibt den Vor- und den Nachnamen aus:

```
AdFind -b "DC=domain,DC=de" -f
  "(sAMAccountName=N*)" givenName sn
```

AdFind enthält eine Reihe von Zusatzfunktionen, die andere Werkzeuge nicht bieten. Mit folgender Zeile gibt es alle gelöschten Objekte zurück:

```
AdFind -default -showdel -f
  isdeleted=TRUE
```

Dieses Kommando zählt dagegen alle Benutzer der Vertriebs-OU, deren Telefonnummer mit "0511" beginnt:

```
AdFind -c -b "OU=Vertrieb,DC=do-
  main,DC=de" -f
  "(&(objectClass=user)(objectCate-
  gory=person)(telephoneNum-
  ber=0511*))"
```

Besonderen Wert entfaltet das Programm allerdings, wenn Sie es mit seinem Pendant AdMod einsetzen. Das zweite Werkzeug manipuliert Werte im Active Directory. Sie können es eigenständig einsetzen, interessant ist aber vor allem das "Piping", mit dem die Daten, die AdFind zurückgibt, als Zielobjekte an AdMod übergeben werden. Der nächste Aufruf ändert den Anmeldenamen für den Benutzer Bernd Müller:

```
AdFind -b "DC=domain,DC=de" -f
  "(sAMAccountName=bernd)" -dsq  |
  admod "sAMAccountName::mueller"
```

Suche mit GUI: ADsearchAdmin

Ein sehr leistungsstarkes grafisches Werkzeug zur Suche und Dokumentation des Active Directory stellt Manfred Paleit auf seiner Seite [3] kostenlos zur Verfügung. Der ADsearchAdmin ermöglicht dabei nicht nur das komfortable Stöbern im AD-Datenbestand, sondern bietet auch eine WMI-Abfragemaschine und erleichtert einige administrative Aufgaben. In der Standardansicht listet ADsearchAdmin die Domänenstruktur von einem beliebigen Startpunkt aus auf. Ein Detailfenster rechts zeigt dann die Attributwerte des selektierten Objekts an und ermöglicht bei schreibbaren Werten das Ändern. Weitere Registerkarten zeigen detaillierte Informationen zum AD-Forest und den Domänencontrollern an.

Zum Suchen nach Benutzern, Computern und Gruppen verfügt ADsearchAdmin über eigene Buttons. Völlige Freiheit bietet dabei der Schalter "LDAP Query", über den Sie beliebige Anfragen an das Verzeichnis stellen können. Dabei hat das Programm gleich einige Beispiele eingebaut und wer eigene komplexe Suchstrings gebaut hat, kann sie als eigene Vorlagen abspeichern. Auch einige weitere Schmankerl sucht man in anderen Tools vergebens, so etwa den "True Last Logon": Da das Datum der letzten

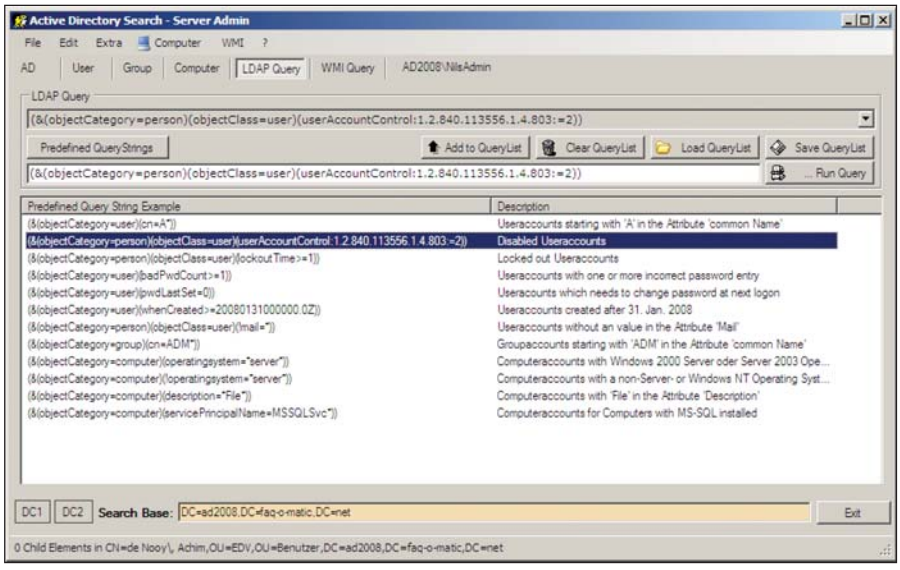


Bild 2: Als kleine Hilfe hat ADsearchAdmin bereits einige nützliche LDAP-Abfragen eingebaut. Eigene LDAP-Strings lassen sich zur späteren Verwendung speichern.

Benutzeranmeldung nicht zwischen den Domänencontrollern repliziert wird, verbindet sich ADsearchAdmin mit allen DCs und liest den Wert "lastLogon" dort aus. Alle gefundenen Daten kann ADsearchAdmin in Dateien speichern oder auch drucken.

Die Zusatzfunktionen verlassen das Feld der AD-Daten und bieten einen WMI-Abfragegenerator oder den Zugriff auf häufig genutzte administrative Funktionen wie das Ereignisprotokoll eines Remote-Servers oder einen direkten RDP-Verbindungsaufbau. Der WMI-Generator kann auf entfernte Rechner zugreifen und alle WMI-Klassen des Standardnamensraums CIMv2 anzeigen. Fragen Sie eine dieser Klassen ab, so zeigt ADsearchAdmin die derzeitigen Werte für das entfernte System an. Über das WMI-Menü besteht zudem ein schneller Zugriff auf alltäglich benötigte Informationen wie Hotfixes oder die gerade angemeldeten Benutzer.

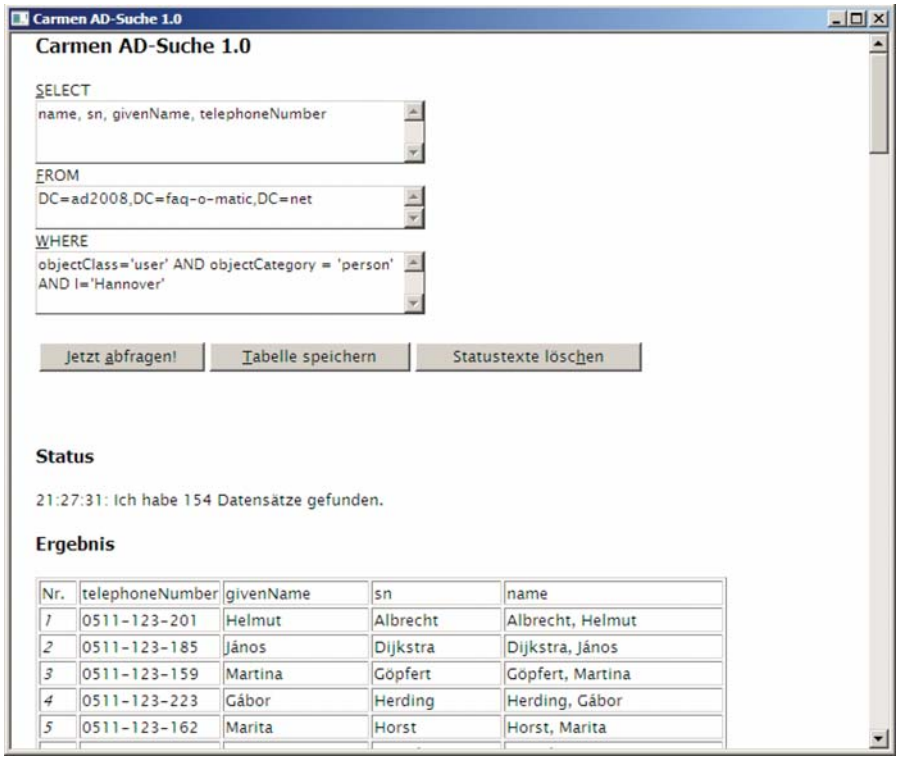


Bild 3: "Carmen" ermöglicht die Suche in Active Directory mit SQL-Kommandos. Das fällt vielen Admins leichter als die krude LDAP-Syntax.

Suchaufträge für das LDAP-Verzeichnis

Suchaufträge erwartet ein LDAP-Verzeichnis in der Form "Attribut = Wert". Die Attribute haben fest definierte Namen, die allerdings je nach Hersteller unterschiedlich ausfallen können. Die wichtigsten Attributnamen für Active Directory finden Sie unter [4] oder Sie fertigen mit den Kenntnissen aus diesem Artikel einen CSVDE-Export an und lesen die Namen der Attribute in der ersten Zeile. In einem Suchfilter lassen sich mehrere Attribute verknüpfen, wobei LDAP erst den Operator (etwa "&" für eine Und-Verknüpfung) und dann die Werte erwartet. Alle Kontakte aus Hannover erfasst etwa dieser Filter:

```
(&(objectClass=contact)(l=Hannover))
```

Jedes Attribut-Wert-Paar steht also in Klammern und auch den ganzen Suchausdruck fassen Sie in Klammern ein – Vorsicht, dass Sie keine Klammer vergessen. Das logische "Oder" markiert das Pipezeichen (|) und für "Nicht" steht das Ausrufezeichen. Alle Benutzer aus Berlin oder Peine, deren Nachname nicht mit "Wester" anfängt, findet also folgender komplexe Filter:

```
(&(objectClass=user)(objectCatego-
  ry=person)(|(l=Hannover)
  (l=Peine))(!(sn=Wester*)))
```

Carmen als SQL-Dolmetscherin

Das LDAP ist eine recht komplexe Abfragesprache. Um Active Directory für Entwickler und versierte Admins leichter zugänglich zu machen, hat Microsoft daher schon mit dem ersten Release in Windows 2000 eine zweite Sprache eingebaut, nämlich SQL. Für die meisten Administratoren dürfte SQL zwar auch nicht gerade zu den bevorzugten Umgangssprachen gehören, doch in vielen Situationen sind auch für Einsteiger SQL-Abfragen deutlich leichter zu verstehen und aufzubauen als LDAP-Queries. Der Haken dabei: Windows enthält kein Programm, das den Verzeichnisdienst mit SQL ansprechen könnte.

Der Aufbau des LDAP

Wie alle modernen und professionellen Verzeichnisdienste beruht das Active Directory auf dem LDAP-Standard. Im Rahmen dieses Workshops möchten wir kurz auf das Protokoll eingehen. Ein wesentlicher Bestandteil von LDAP (Lightweight Directory Access Protocol) ist eine Abfragesprache, die das Suchen und den gezielten Zugriff auf Objekte im Verzeichnis ermöglicht – also etwa Benutzer, Computer oder Drucker. Wer mehr aus Active Directory herausholen will, sollte sich ein paar Grundlagen seiner Datenbanktechnik aneignen. Obwohl LDAP zunächst sperrig wirkt, ist das Wesentliche für den Alltag nicht schwer zu erlernen.

Jedes Objekt wird über einen eindeutigen Pfad innerhalb des Verzeichnisses identifiziert, den man auch "Distinguished Name" nennt (oder kurz DN). Dieser Pfad gibt die Position des Objekts von ganz "unten" bis ganz "oben" an. Die Benutzerin Ute in der Marketingabteilung des IT-Administrator könnte etwa folgenden DN haben: CN=Ute, OU=Marketing, OU=Benutzer, DC=intern, DC=it-administrator, DC=de. Jeden Abschnitt im Pfad leitet ein funktionales Kürzel ein. Active Directory nutzt nur drei verschiedene Kürzel: "CN" steht für "Common Name" und gibt meist den Namen des Objekts an. "OU" heißt "Organizational Unit" und ist für AD-Admins selbsterklärend. "DC" wiederum steht nicht für Domain Controller, sondern für "Domain Component" und gibt die Abschnitte des DNS-Namens der Domäne nacheinander an.

Abhilfe schafft ein kleines Skript-Tool, das der Workshop-Autor vor einigen Jahren zu diesem Zweck geschrieben hat. Die HTA-Anwendung "Carmen" bietet ein grafisches Eingabefeld, um recht einfach SQL-Abfragen an Active Directory einzugeben und die Ergebnisse in übersichtlichen Tabellen zurückzuliefern. Die gefundene Ergebnistabelle lässt sich als HTML-Datei speichern und danach zur weiteren Bearbeitung in Excel öffnen.

Obwohl natürlich auch mit SQL dieselben Feldnamen verwendet werden wie in einer LDAP-Abfrage, sind vor allem die Filterkriterien anders aufgebaut. In SQL führen Sie mehrere Kriterien hintereinander an und verbinden sie mit den Schlüsselwörtern "AND" oder "OR". Der folgende Suchstring gibt etwa alle XP-Rechner mit Service Pack 3 aus dem AD zurück. Dabei tragen Sie die Bestandteile der Abfrage in die passenden Felder für SELECT, FROM und WHERE ein – als Hilfe füllt Carmen das WHERE-Feld automatisch mit dem LDAP-Namen der Domäne aus:

```
SELECT * FROM
  'LDAP://DC=domain,DC=de' WHERE
  objectClass='computer' and
  operatingSystem='Windows XP*'
  and operatingSystemServicePack=
  'Service Pack 3'
```

Im Unterschied zu LDAP erwartet SQL die Kriterien in Hochkommas (Shift + #). In das WHERE-Feld können Sie ganz am Ende auch noch ein Sortierkriterium eintragen, etwa mit "ORDER BY name". Einige nützliche Beispiele führt die Download-Seite von faq-o-matic [5] auf. Dort steht Carmen zum kostenlosen Download bereit.

Grafische Dokumentation mit José und Borg

Zu guter Letzt gehen wir noch auf zwei Skript-Tools ein, mit denen Sie Ihre IT-Umgebung grafisch dokumentieren können. José und Borg [6] ermöglichen es, den aktuellen Stand der Domänenobjekte grafisch festzuhalten. Während José die Domäne selbst dokumentiert und Details zu Benutzern, Computern, Gruppen oder Gruppenrichtlinien in einem HTML-Bericht speichert, kümmert sich Borg um die Replikationsstruktur und gibt Daten zu Standorten und Serververbindungen in einem HTML-Report aus.

José liegt momentan in Version 2.1 vor. Als Neuerung gegenüber älteren Fassungen lässt sich das Tool sowohl manuell als auch skriptgesteuert ausführen. Für Ad-hoc-Berichte eignet sich der grafische Teil *jose.hta*. Er öffnet ein recht komplexes Konfigurationsfenster, in dem Sie über zahlreiche Kästchen die auszugebenden Daten bestimmen können. Ein Klick auf "Jetzt dokumentieren" am unteren Fensterrand startet den Bericht, für den das Werkzeug in großen Umgebungen durchaus eine Weile benötigen kann. Der erzeugte HTML-Report ist statisch und eignet sich beispielsweise als Momentaufnahme oder um Dritten die Struktur des AD zu veranschaulichen.

Durch seine vielen Optionen kann José sehr unterschiedliche Berichte erzeugen und sich etwa auf die Rahmendaten der Domäne und die OU-Struktur beschränken. Sie können aber auch alle Benutzerkonten einer OU mit allen wichtigen Details ausgeben oder einen detaillierten Report über die verknüpften Gruppenrichtlinien aufbauen. Seit Version 2.0 bietet das Werkzeug außerdem eine Kommandozeilenoption, durch die Sie Berichte auch automatisiert oder über eine einfache Batchdatei erzeugen. In diesem Fall erwartet das Programm die Auswahl der zu dokumentierenden Objekte und Attribute in einer Definitionsdatei, die Sie vorab mit der grafischen Oberfläche erstellen. Das folgende Kommando generiert etwa einen Bericht auf Grundlage der Definitionsdatei *OUs_und_GPOs.txt*:

```
cscript JoseExec /d:"
  OUs_und_GPOs.txt"
```

Der kleine Bruder von José ist Borg. Dieses Skript macht etwas Ähnliches, konzentriert sich aber auf eine Aufgabe und kommt daher ohne Konfiguration aus. Wenn Sie es im CMD-Fenster mit *cscript borg.vbs* starten, erzeugt es einen HTML-Bericht über alle Standorte, Domänencontroller und Replikationsverbindungen des Active Directory. Administratoren und Dienstleister verfügen so über zwei kleine, einfache Werkzeuge, mit denen sie die wichtigsten Details des Windows-Verzeichnisdienstes festhalten und später ohne Online-Kontakt zur Domäne auswerten können.

Links

[1] Vergleich von Schema-Versionen
www.faq-o-matic.net/2007/10/21/schema-versionen-vergleichen/

[2] Download des Tools AdFind
www.joeware.net/freetools/

[3] Website von Manfred Paleit mit ADsearchAdmin
www.tools4net.de

[4] Erläuterung von Attribut-Namen im AD
www.faq-o-matic.net/2002/09/21/active-directory-ldap-feldnamen/

[5] Hilfreiche LDAP-SQL-Beispiele zu Carmen
www.faq-o-matic.net/2004/10/20/carmen-mit-sql-das-ad-abfragen/

[6] Grafische Dokumentation mit José und Borg
www.faq-o-matic.net/kategorien/active-directory/

Fazit

Es gibt einige kostenlose Werkzeuge, die Ihnen das Suchen, Auswerten und Dokumentieren von Active Directory erleichtern können. Dabei ist unsere Auswahl keineswegs repräsentativ und schon gar nicht vollständig: Seit das Active Directory vor etwa zehn Jahren in den ersten Beta-Versionen veröffentlicht wurde, hat sich eine riesige Vielfalt an kleinen oder größeren Tools entwickelt. Wenn Sie eine spezielle Anforderung haben, lohnt sich eine Recherche nach dem passenden Werkzeug in jedem Fall. *(dr)*

Nils Kaczenski ist Microsoft-MVP für Directory Services und leitet das Consulting und den Support bei WITcom by Wahl GmbH + Co. KG in Hannover.

Netzwerkrichtlinien mit Windows Server 2008 (3)

Sicherer Zugang

von Thomas Joos

Die "Network Access Protection" ist ein neues Sicherheits-Feature im Windows Server 2008. Über diese Funktion können Unternehmen anhand entsprechender Richtlinien sicherstellen, dass nur solche Clients Zugang zum Firmennetz erhalten, die bestimmten Sicherheitskriterien genügen. Im dritten und abschließenden Teil unserer Workshopserie zeigen wir Ihnen, wie Sie Clients den sicheren Zugang zum Netzwerk ermöglichen.

Auf Basis dieser Verifizierung wird der Client einer Integritätsrichtlinie zugeordnet, also zum konformen oder nicht-konformen Client erklärt. Nachdem Sie die Richtlinie für konforme NAP-Clients erstellt haben, müssen Sie als nächstes eine Netzwerkrichtlinie erstellen, die den Netzwerkzugriff für nicht-konforme Clients steuert. Diese Konfiguration unterscheidet sich etwas von der Netzwerkrichtlinie für nicht-konforme Clients im Bereich NAP über DHCP. Gehen Sie zur Erstellung analog vor und geben Sie der Richtlinie eine passende Bezeichnung. Wählen Sie als Integritätsrichtlinie dieses Mal die Richtlinie "Nicht-NAP-Konform" aus.

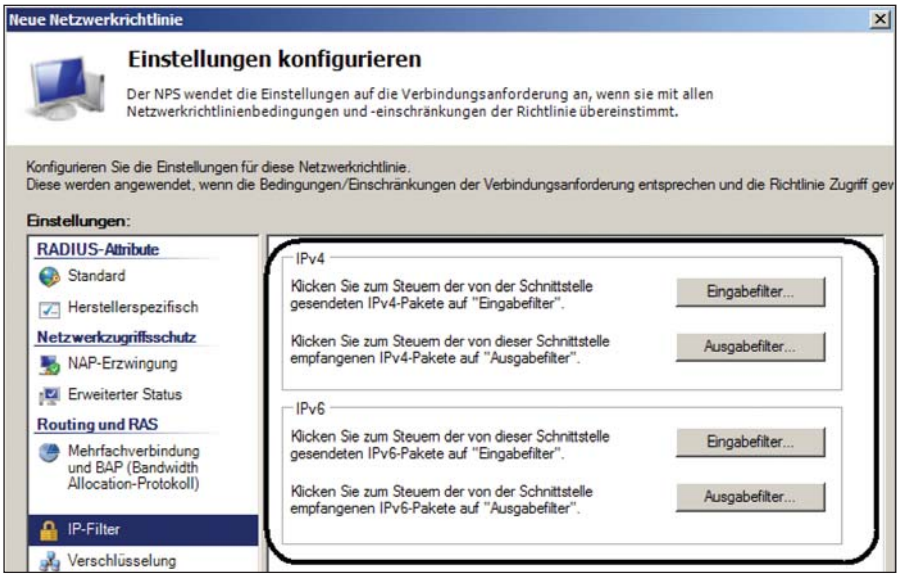


Bild 1: Das Erstellen von IP-Filtern für VPN-Clients zur NAP-Überprüfung ist für IPv4 und IPv6 möglich

Auf der Seite "Zugriffsberechtigung angeben" nutzen Sie die Einstellung "Zugriff gewährt" und klicken zweimal auf "Weiter", um zum Fenster "Authentifizierungsmethoden konfigurieren" und anschließend zur Seite "Einschränkungen konfigurieren" zu gelangen. Ein erneutes "Weiter" und Sie kommen zur Seite "Einstellungen konfigurieren". Dort wählen Sie den Punkt "NAP-Erzwingung" aus und aktivieren die Option "Eingeschränkten Zugriff gewähren". Markieren Sie hier das Kontrollkästchen "Automatische Wartung von Clientcomputern aktivieren" und gehen Sie nun zu "IP-Filter / IPv4 / Eingabefilter / Neu". Aktivieren Sie dort das Kontrollkästchen "Zielnetzwerk" und geben Sie die IP-Adresse des Domänencontrollers mit der Subnetzmaske 255.255.255. 255 an. Dadurch ist sichergestellt, dass sich nicht-konforme NAP-Clients nur mit dem Domänencontroller verbinden können, um sich zu authentifizieren.

Nach Bestätigen der Eingabe mit "OK" aktivieren Sie im Fenster "Eingehende Filter" die Option "Nur die unten aufgeführten Netzwerkpakete zulassen". Dadurch wird sichergestellt, dass der Client sich ausschließlich mit der festgelegten IP-Adresse verbinden darf, allerdings mit allen Protokollen. Klicken Sie nun auf "OK", um das Fenster "Eingehende Filter" zu schließen und im Hauptfenster anschließend im Bereich "IPv4" auf "Ausgabefilter". Gehen Sie hier analog zur Konfiguration des Eingabefilters vor und hinterlegen Sie auch hier die IP-Adresse des Domänencontrollers mit der Subnetzmaske 255.255.255.255. Dadurch ist sichergestellt, dass der Client nicht nur Datenpakete zum Domänencontroller senden kann, sondern auch nur vom Domänencontroller empfängt. Nun schließen Sie die Erstellung der Netzwerkrichtlinien ab. Diese werden nach der Erstellung in der NPS-Konsole angezeigt. Alle anderen Richtlinien sollten als deaktiviert angezeigt werden.

Verbindungsanforderungsrichtlinie für VPN-Clients

Für die Einwahl von VPN-Clients benötigen Sie noch Verbindungsanforderungsrichtlinien (Connection Request Policies, CRPs). Diese konfigurieren Sie über die NPS-Konsole, indem Sie im Bereich "Richtlinien"

auf den Menüpunkt "Verbindungsanforderungsrichtlinien" klicken. Gehen Sie zur Konfiguration einer CRP für die VPN-Einwahl wie folgt vor: Deaktivieren Sie zunächst die Standardrichtlinien und erstellen Sie eine neue Richtlinie, indem Sie mit der rechten Maustaste auf "Verbindungsanforderungsrichtlinien" klicken und "Neu" wählen. Geben Sie der Richtlinie nun einen passenden Namen, zum Beispiel "VPN-Verbindungen" und wählen Sie im Listenfeld zur Option "Typ des Netzwerkzugriffsservers" den Eintrag "Remotezugriffsserver (VPN-Dial up)" aus.

Klicken Sie auf "Weiter" und im Fenster "Bedingungen eingeben" auf "Hinzufügen". Aktivieren Sie dort die Option "Client-IPv4-Adresse" und klicken Sie auf "Hinzufügen". Nun geben Sie die IP-Adresse des RADIUS-Servers ein, an dem sich die Benutzer über das Internet anmelden sollen. Hierbei handelt es sich üblicherweise um den NPS-Server. Nachdem Sie die Eingaben vorgenommen haben, klicken Sie auf "Weiter".

Aktivieren Sie im Fenster "Verbindungsanforderungsweiterleitung angeben" für den Bereich "Authentifizierung" die Option "Anforderungen auf diesem Server authentifizieren" und bestätigen Sie die Eingabe auch hier mit "Weiter". Aktivieren Sie jetzt im Fenster "Authentifizierungsmethoden angeben" das Kontrollkästchen "Netzwerkrichtlinien-Authentifizierungseinstellungen außer Kraft setzen". Durch diese Auswahl wird die Authentifizierung so verwendet, wie Sie diese in der Verbindungsanforderungsrichtlinie festlegen, unabhängig davon, wie die entsprechenden Netzwerkrichtlinien konfiguriert sind. Klicken Sie im Bereich "EAP-Typen" auf "Hinzufügen" und wählen Sie "Microsoft: Geschütztes EAP (PEAP)" aus. PEAP verwendet TLS (Transport Level Security), um einen verschlüsselten Kanal zwischen einem authentifizierten PEAP-Client und einem authentifizierenden PEAP-Server zu erstellen. Klicken Sie anschließend auf "OK" und noch einmal auf "Hinzufügen". Wählen Sie "Microsoft: Gesichertes Kennwort (EAP-MSCHAP v2)" aus, markieren Sie als nächstes die Option "Microsoft: Geschütztes EAP (PEAP)" und klicken Sie auf "Bearbeiten". Stellen Sie sicher, dass das Kontrollkästchen "Quarantäneüberprüfungen aktivieren" eingeschaltet ist. Wählen Sie das Zertifikat aus, das Sie zuvor für den Server ausgestellt haben. Bestätigen Sie schließlich auf den restlichen Fenstern die Standardeinstellungen.

Anschließend folgt die Konfiguration des VPN-Servers auf reguläre Weise, also ohne NAP. Auf diese Schritte gehen wir in diesem Artikel jedoch nicht näher ein. Die nächste Aufgabe besteht nun in der Aktivierung der RAS-Client-NAP-Unterstützung auf dem VPN-Client. Starten Sie dazu auf dem PC die Verwaltungskonsole des NAP-Clients mit dem Befehl *napclcfg.msc*. Klicken Sie auf "Erzwingungsclients" und aktivieren Sie den "Remotezugriffs-Quarantäneerzwigungsclient". Setzen Sie den Starttyp des Dienstes "NAP-Agent (Network Access Protection)" auf "Automatisch" und starten Sie diesen.

IPSec mit NAP einsetzen

Die Verschlüsselung bei IPsec erfolgt mit einem symmetrischen Verfahren, bei dem ein privater Schlüssel ausgetauscht werden muss. Solche Verfahren sind schneller als Public Key-Verfahren. Um den privaten Schlüssel zwischen Sender und Empfänger auszutauschen, verwendet Windows Server 2008 den ISAKMP/Oakley-Dienst, der als IKMP (Internet Key Management Protocol) bekannt ist. ISAKMP, das Internet Security Association and Key Management Protocol, wurde federführend von Cisco definiert und legt fest, wie zwei Knoten in einem Netzwerk Schlüssel austauschen und eine sichere Kommunikationsverbindung aufbauen. Oakley ist das Protokoll, um Verschlüsselungsverfahren und Schlüssel festzulegen. Für den Austausch der privaten Schlüssel können Public Key-Verfahren und Kerberos verwendet werden. Ob eine sichere Kommunikation erfolgen soll, legen Sie unter Windows Server 2008 über Gruppenrichtlinien und die Konfiguration der neuen Windows-Firewall fest. Es wird nicht pro Anwendung, sondern pro System und Verbindung mit bestimmten Rechnern im Netzwerk definiert, ob eine sichere Kommunikation erfolgen soll.

Damit Sie IPSec im Unternehmen einsetzen können, müssen Sie nun auf einem Server die Rolle Active Directory-Zertifikatdienste installieren. Die Installation erfolgt analog wie bereits bei der Verwendung von NAP mit DHCP beschrieben. Unter Windows Server 2003 war die Konfiguration von IPSec noch eine relativ komplexe Angelegenheit. Durch die Integration der IPSec-Verwaltung in die Firewall-Konsole wird diese Konfiguration nun enorm vereinfacht. Die Verwaltungsoberfläche der neuen Firewall können Sie über "Start / Ausführen / wf.msc" starten. Die Firewall für erweiterte Sicherheit ersetzt die Verwaltungskonsolen für IPSec-Richtlinien.

Verwenden Sie unter Windows Server 2008 IPSec-Richtlinien, verhalten sich die Server wie folgt: Ein Server, für den IPSec aktiviert wurde, sendet Pakete über IPSec. Antwortet der empfangende Server ebenfalls mit IPSec, wird der Datenverkehr verschlüsselt. Unterstützt der empfangende Server kein IPSec, wird der Datenverkehr nicht verschlüsselt. Dieser Datenverkehr findet gleichzeitig statt. Unter Windows Server 2003 wurden erst IPSec-Pakete verschickt, dann drei Sekunden gewartet und erst dann die unverschlüsselten Pakete gesendet. So konnten oft starke Performance-Probleme auftreten, die durch das gleichzeitige Versenden der Pakete in 2008 vermieden werden. Durch diese Funktion können Server IPSec-Verkehr unterstützen, aber nicht mehr zwingend voraussetzen, um eine möglichst sichere Verbindung zu erstellen.

Bisher hat IPSec unter Windows nur Internet Key Exchange (IKE) unterstützt. Windows Vista und Windows Server 2008 unterstützen eine neue Funktion, die "Authenticated IP" (AuthIP). Dieses Feature unterstützt weitere Authentifizierungsfunktionen als IKE – zum Beispiel, was die Gültigkeit von Zertifikaten angeht, die Bestandteil der Network Access Protection

(NAP) in Windows Server 2008 sind. Auch die Kerberos- oder NTLMv2-Authentifizierung wird ebenso unterstützt wie die Authentifizierung mit mehreren Konten. IPSec kann dabei so konfiguriert werden, dass sowohl die Computerauthentifizierung als auch die Benutzerauthentifizierung zum Einsatz kommt. Dies erhöht die Sicherheit im Netzwerk deutlich. Unter Windows Server 2008 und Vista kann der Verkehr zwischen Domänenmitgliedern und Domänencontrollern IPSec-verschlüsselt stattfinden, während der Verkehr zwischen Domänenmitgliedern und Nicht-Domänenmitgliedern weiterhin unverschlüsselt erfolgen kann. Diese Funktion war unter Windows Server 2003 und Windows XP nicht möglich.

Sicherheitshalber sollten Sie beim Einrichten einer IPSec-Infrastruktur einigen PCs im Netzwerk die IPSec-Kommunikation gestatten, auch wenn diese nicht NAP-konform sind oder Sie für sie keine NAP-Überprüfung vornehmen wollen. Damit stellen Sie sicher, dass diese Rechner im Notfall nicht vom Netzwerk abgeschnitten sind. Mitglieder dieser speziellen Gruppe können auch dann mit anderen PCs kommunizieren, wenn diese eine Sicherheitsprüfung vorschreiben. Legen Sie dazu am besten eine eigene globale Sicherheitsgruppe in der Domäne an und wählen als Bezeichnung zum Beispiel "NAP-Ausnahmen". In diese

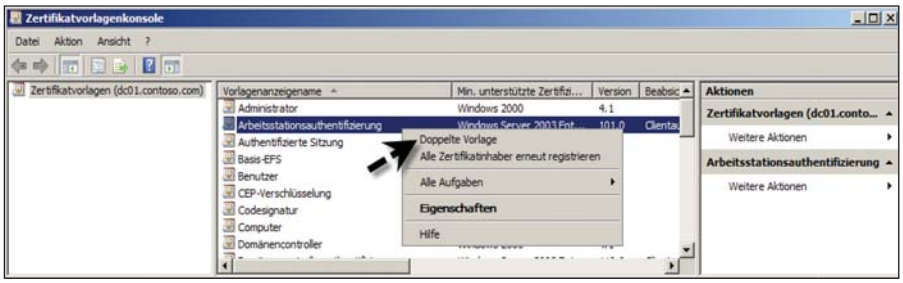


Bild 3: Vorhandene Zertifikatvorlagen lassen sich per Rechtsklick deduplizieren

Gruppe nehmen Sie die Computerkonten auf, denen Sie die NAP-Überprüfung ersparen wollen. Wollen Sie die NAP-Überprüfung für manche Clients auf Basis der erwähnten Gruppe deaktivieren, sollten Sie für diese Clients auch eine eigene Zertifikatsvorlage erstellen. Dies erledigen Sie am besten über die entsprechende Verwaltungskonsole auf dem Zertifikatsserver, die Sie über "Start / Ausführen / certtmpl.msc" erreichen. Klicken Sie mit der rechten Maustaste auf die Vorlage "Arbeitsstationsauthentifizierung" und wählen Sie im Kontextmenü den Eintrag "Doppelte Vorlage" aus.

Zertifikate einrichten

Wählen Sie jetzt aus, für welche Zertifizierungsstelle das Zertifikat kompatibel sein soll. Setzen Sie eine reine Windows Server 2008-CA ein, können Sie an dieser Stelle auch die Minimalvoraussetzung auf Windows Server 2008 nutzen. Anschließend öffnet sich das Konfigurationsfenster für die neue Zertifikatsvorlage. Geben Sie eine passende Bezeichnung für die neue Vorlage ein, zum Beispiel "Systemintegritäts-Authentifizierung". Aktivieren Sie das Kontrollkästchen "Zertifikat in Active Directory veröffentlichen". Wenn ein Antragsteller ein Zertifikat erhält, das auf dieser Vorlage basiert, fügt das System das ausgestellte Zertifikat zu dem Active Directory-Objekt dieses Antragstellers hinzu. Das Kontrollkästchen "Nicht automatisch erneut registrieren, wenn ein identisches Zertifikat bereits in Active Directory vorhanden ist" lassen Sie deaktiviert. Versucht der Antragsteller, sich für ein auf dieser Vorlage basierendes Zertifikat zu registrieren, führen Computer unter XP, Vista oder Windows Server 2003 und 2008 eine Überprüfung durch, um festzustellen, ob bereits ein identisches Zertifikat in Active Directory vorhanden ist. Ist dies der Fall, übermittelt die automatische Registrierung keine erneute Registrierungsanforderung. Das ermöglicht die Erneuerung von Zertifikaten und verhindert

E·BOOK SYSTEMS

Lesen Sie den IT-Administrator als E-Paper

Testen Sie kostenlos und unverbindlich die elektronische IT-Administrator Leseprobe auf **www.it-administrator.de**

Wann immer Sie möchten und wo immer Sie sich gerade befinden – Volltextsuche, Zoomfunktion und alle Verlinkungen inklusive. Klicken Sie sich ab heute mit dem IT-Administrator einfach von Seite zu Seite, von Rubrik zu Rubrik

Infos zu E-Abos, E-Einzelheften und Kombiangeboten finden Sie auf:

www.it-administrator.de

gleichzeitig, dass mehrere identische Zertifikate ausgestellt werden.

Holen Sie nun die Registerkarte "Erweiterungen" in den Vordergrund und klicken Sie auf "Anwendungsrichtlinien / Bearbeiten / Hinzufügen / Neu". Geben Sie im neuen Dialogfeld die Bezeichnung "Systemintegritäts-Authentifizierung" ein und weisen Sie der Richtlinie die Objektkennung "1.3.6.1.4.1.311.47.1.1" zu. Bestätigen Sie die geöffneten Dialogfelder mit "OK", bis nur noch das Dialogfeld "Eigenschaften" der neuen Vorlage geöffnet ist. Wechseln Sie jetzt zur Registerkarte "Sicherheit". In dieser Registerkarte nehmen Sie die erstellte globale Gruppe "NAP-Ausnahmen" auf und aktivieren Sie bei der Option "Automatisch registrieren" das Kontrollkästchen "Zulassen". Klicken Sie auf "OK", um die Eingaben abzuschließen. Nachdem Sie die neue Vorlage für das Zertifikat erstellt haben, müssen Sie in den Zertifikatdiensten noch konfigurieren, dass diese Zertifikatsvorlage für neue Zertifikate verwendet werden darf. Starten Sie hierfür die Verwaltung der Zertifizierungsstelle entweder über die Programmgruppe "Verwaltung" oder über "Start / Ausführen / certsrv.msc". Erweitern Sie den Knoten Ihrer Zertifizierungsstelle und klicken Sie mit der rechten Maustaste auf "Zertifikatvorlagen". Dort gehen Sie auf "Neu / Auszustellende Zertifikatvorlage". Wählen Sie die erstellte Zertifikatvorlage "Systemintegritäts-Authentifizierung" aus und klicken Sie auf "OK". Im Anschluss sollte die Vorlage in der Zertifizierungsstelle angezeigt werden.

Der nächste Schritt besteht darin, die Zertifizierungsstelle so zu konfigurieren, dass diese automatisch ausstellt, wenn ein Domänencomputer ein Zertifikat anfordert. Auf Basis dieser Zertifikate wird später die IPSec-Kommunikation aufgebaut.

Für die automatische Registrierung von Zertifikaten verwenden Sie am besten die Gruppenrichtlinien:

1. Starten Sie dazu die Gruppenrichtlinienverwaltung
2. Öffnen Sie die Bearbeitung der "Default Domain Policy".
3. Navigieren Sie zu "Computerkonfiguration / Windows-Einstellungen / Sicherheitseinstellungen / Richtlinien für öffentliche Schlüssel".
4. Klicken Sie auf der rechten Seite doppelt auf die Richtlinie "Zertifikatdienstteclient-automatische Registrierung".
5. Setzen Sie die Richtlinie auf "Aktiviert".
6. Aktivieren Sie zusätzlich noch die beiden Optionen "Abgelaufene Zertifikate erneuern… " und "Zertifikate die Zertifikatvorlagen verwenden".
7. Bestätigen Sie alle Fenster und schließen Sie den Editor für die Gruppenrichtlinien wieder.

Nehmen Sie anschließend das Computerkonto des NPS in die Gruppe NAP-Ausnahmen auf, damit dieser Server immer uneingeschränkt mit allen PCs und Servern kommunizieren kann. Zusätzlich sollten Sie auf dem NPS eine untergeordnete Zertifikatstelle installieren, die an die IPSec-Umgebung angepasst ist. Fügen Sie auf dem Server dazu neben der Rolle "Netzwerkrichtlinien und -Zugriffsdienste" auch die Rolle "Active Directory-Zertifikatdienste" hinzu. Haben Sie auf dem Server schon die Netzwerkrichtlinien installiert, müssen Sie nachträglich über den Menüpunkt "Rollen" im Server-Manager den Rollendienst "Integritätsregistrierungsinstanz" einrichten. Installieren Sie vor diesem Rollendienst jedoch zunächst die Active Directory Zertifikatdienste auf dem Server.

Als Rollendienst für die "Zertifizierungsdienste" auf dem Server wählen Sie im entsprechenden Fenster nur "Zertifizierungsstelle" aus. Im nächsten Fenster wählen Sie als Setuptyp "Eigenständig" aus und dann "Untergeordnete Zertifizierungsstelle". Bestätigen Sie alle Fenster, bis Sie zum Fenster "Zertifikat von übergeordneter ZS anfordern" gelangen. Aktivieren Sie auf diesem Fenster die Option "Zertifikatanforderung an übergeordnete Zertifizierungsstelle senden" und klicken Sie auf "Durchsuchen". Wählen Sie die bereits installierte Root-CA aus und schließen dann die Installation der CA ab. Fügen Sie nach der Installation der untergeordneten CA den Netzwerkrichtlinien-Rollendienst "Integritätsregistrierungsinstanz" über den Server-Manager hinzu.

Hierfür bestätigen Sie die Auswahl des Rollendienstes und wählen die Option "Später einen Zertifikateserver mit dem HRA-Snap-In auswählen". Im Fenster "Auswählen von Authentifizierungsanforderungen für die Integritätsregistrierungsstelle" aktivieren Sie nun die Option "Nein, anonyme Anforderungen von Integritätszertifikaten zulassen". Wählen Sie im nächsten Fenster "Serverauthentifizierungszertifikat für SSL-Verschlüsselung auswählen" die Option "Zertifikat zur späteren SSL-Verschlüsselung auswählen", damit Sie das Zertifikat nach der Installation der HRA auswählen können. Microsoft empfiehlt zwar beim Einsatz einer HRA SSL zu verwenden, diese Konfiguration ist aber bei der Installation einer HRA nicht zwingend. Bestätigen Sie alle restlichen Fenster und lassen Sie die Installation abschließen.

Der neue Windows Server 2008 bietet nicht nur lang gewünschte Features, sondern stellt auch eine Menge Anforderungen an den Administrator. Das IT-Administrator Sonderheft "Windows Server 2008 – Praktischer Einsatz, Wartung und Optimierung im Unternehmensnetzwerk" mit 180 Seiten Praxis-Know-how hilft Ihnen auf unsere bewährte, praxisnahe Art, den Server optimal in Ihr Netzwerk zu integrieren und dessen Leistungsfähigkeit voll auszuschöpfen.

Als Abonnent können Sie das Sonderheft zum Vorzugspreis von € 29,90 bestellen (Nicht-Abonnenten erhalten das Heft zum Preis von € 34,90. Die Preise verstehen sich jeweils inkl. Versand und 7% MwSt).

Jetzt bestellen:
Sonderheft Windows Server 2008

Nachdem Sie die untergeordnete Zertifizierungsstelle und die Integritätsregistrierungsinstanz installiert haben, müssen Sie diese noch konfigurieren. Starten Sie die Verwaltungskonsole der Zertifikatsdienste über "Start / Verwaltung" oder "Start/ Ausführen / certsrv.msc". Klicken Sie die Zertifizierungsstelle mit der rechten Maustaste an und rufen Sie die Eigenschaften auf. Aktivieren Sie die Registerkarte "Richtlinienmodul" und klicken Sie auf die Schaltfläche "Eigenschaften". Aktivieren Sie anschließend die Option "Der Einstellungen der Zertifikatvorlage folgen, falls zutreffend. Zertifikat ansonsten automatisch ausstellen". Bestätigen Sie die Fenster und wechseln Sie anschließend zur Registerkarte "Sicherheit". Fügen Sie der Liste das Computerkonto des NPS-Servers hinzu und erteilen Sie diesem die Rechte "Zertifikate ausstellen und verwalten und Zertifikate anfordern".

Nach diesen Konfigurationen folgt die Konfiguration der Integritätsregistrierungsinstanz über deren Verwaltungsoberfläche. Erstellen Sie dazu eine neue Management-Konsole mit dem Snap-In "Integritätsregistrierungsstelle". Klicken Sie mit der rechten Maustaste auf "Zertifizierungsstelle" und "Zertifizierungsstelle hinzufügen". Klicken Sie auf "Durchsuchen" und wählen Sie dann die untergeordnete Zertifizierungsstelle aus, nicht die übergeordnete Root-CA. Anschließend klicken Sie nochmals auf den Konsoleneintrag "Zertifizierungsstelle" und überprüfen, ob die Option "Eigenständige Zertifizierungsstelle verwenden" aktiviert ist. Im Anschluss können Sie den Netzwerkrichtlinienserver so konfigurieren, dass der Netzwerkzugriffsschutz verwendet wird. So können Sie auf Basis der Windows-Sicherheitsintegritätsverifizierung sicherstellen, welche Clients eine sichere IPSec-Verbindung aufbauen können. Sie können diese Konfiguration mit dem Assistenten für den Netzwerkzugriffsschutz durchführen.

Starten Sie hierfür die Verwaltung des Netzwerkrichtlinienservers und klicken Sie auf den obersten Eintrag der Konsole und dann in der Mitte der Konsole auf "NAP konfigurieren", um den Assistenten zu starten. Wählen Sie als Netzwerkverbindungsmethode die Option "IPSec mit Integritätsregistrierungsstelle (HRA)" aus. Auf der nächsten Seite des Assistenten legen Sie den Netzwerkzugriffserver fest, auf dem die Integritätsregistrierungsinstanz (HRA) installiert ist. Anschließend können Sie spezielle Gruppen festlegen, die Sie für NAP über IPSec konfigurieren wollen. In den meisten Umgebungen ist dies jedoch nicht nötig und Sie bestätigen dieses Fenster ohne Eingaben. Jetzt legen Sie die NAP-Integritätsrichtlinie fest. Wichtig sind hier die beiden Optionen "Windows-Sicherheitsintegritätsverifizierung" und "Automatische Wartung von Clients aktivieren". Bestätigen Sie die Optionen und schließen Sie den Assistenten.

Client-Konfiguration für das VPN

Der nächste Schritt besteht darin, dass Sie die Windows-Sicherheitsintegritätsverifizierung konfigurieren. Die Vorgänge dabei sind identisch mit der Konfiguration von NAP per VPN oder DHCP. Anschließend werden die Clients im Netzwerk so konfiguriert, dass die Kommunikation über die erstellte Infrastruktur per IPSec und NAP-geschützt stattfinden kann. Wollen Sie IPSec mit NAP im Unternehmen einsetzen, werden nur Arbeitstationen mit Windows Vista oder mit Windows XP SP3 unterstützt. Starten Sie dazu auf dem Vista-PC über "Start / Ausführen / napclcfg.msc" die Verwaltungskonsole des NAP-Clients. Klicken Sie auf den Menüpunkt "Erzwingungsclients" und aktivieren Sie die Option "Abhängige Seite von IPSec".

Für die Verwendung von NAP über IPSec müssen Sie in der NAP-Clientkonfiguration noch den Menüpunkt "Integritätsregistrierungseinstellungen" aufrufen.

Klicken Sie mit der rechten Maustaste auf die Gruppe "Vertrauenswürdige Servergruppen" und wählen "Neu". Geben Sie im nächsten Fenster der Gruppe eine Bezeichnung. Deaktivieren Sie den Punkt "Serververifizierung (https:) ist für alle Server in dieser Gruppe erforderlich", wenn Sie kein SSL verwenden wollen. Fügen Sie nun die URL *http://{NPS-Servername}/domainhra/hcsrvext.dll* als Health Registration Authority (HRA) hinzu. Dieser Server stellt Zertifikate für jene Computer aus, die sich in der Domäne authentifiziert haben. Als nächstes fügen Sie die URL *http://{NPS-Servername}/nondmainhra/hcsrvext.dll* ein. Durch diese Konfiguration ist sichergestellt, dass sich Clients erst authentifizieren müssen, um ein Zertifikat zu erhalten. Gelingt das nicht, wird die zweite URL verwendet, welche ebenfalls einen anonymen Zugriff gestattet. Nach Abschluß der Konfiguration sollten die vertrauten Server und deren URL in der NAP-Client-Verwaltungskonsole angezeigt werden.

Starten Sie jetzt den Client neu und melden Sie sich an. Öffnen Sie anschließend die Verwaltungskonsole für lokale Zertifikate. Fügen Sie dazu in einer Verwaltungskonsole das Snap-In "Zertifikate" hinzu und öffnen Sie den lokalen Zertifikatespeicher. Hier sollte ein Zertifikat angezeigt werden, das durch die Zertifizierungsstelle ausgestellt worden ist. Die aktuelle Logdatei für den NPS finden Sie auf dem Server im Verzeichnis *C:\Windows\System32\LogFiles*. Hier finden Sie viele Infos, was die Arbeit des NPS transparenter macht. Sollten Sie hier Fehler finden, können Sie diesen recht schnell eingrenzen. Auch in den Ereignisanzeigen des NPS-Servers werden viele Ereignisse festgehalten, wenn die NAP-Vorgänge ablaufen. Sie finden diese Fehler im Systemprotokoll auf dem Server. Auf dem Client finden Sie in der Ereignisanzeige über "Anwendungs- und Dienstprotokolle / Microsoft / Windows / Network Access Protection / Operational" zahlreiche Ereignisse, wenn Sie den NAP-Agent-Dienst neu starten. Diese Ereignisse haben die Quelle "Network Access Protection" und "System-HealthState". Wollen Sie IPSec zusam-

men mit NAP einsetzen, sollten Sie sich zunächst die NAP-Einstellungen vornehmen, wie es auf den vorderen Seiten beschrieben wurde.

Solche Richtlinien erstellen Sie am besten über die Einstellungen der erweiterten Firewall in den Gruppenrichtlinien. Sie können dazu die Default Domain Policy verwenden oder für IPSec eine neue Gruppenrichtlinie erstellen. Diese verknüpfen Sie dann mit der OU, in der Sie die Computerkonten der Server und PCs aufnehmen, die per IPSec kommunizieren sollen. Sie finden die notwendigen Einstellungen für IPSec in der "Gruppenrichtlinienverwaltung über Computerkonfiguration / Windows-Einstellungen/ Sicherheitseinstellungen / Windows-Firewall mit erweiterter Sicherheit / LDAP". Rufen Sie über die rechte Maustaste die Eigenschaften von LDAP auf. Anschließend stehen Ihnen verschiedene Registerkarten zur Verfügung, auf denen Sie Voreinstellungen treffen müssen. Hauptsächlich werden hier die Einstellungen für die verschiedenen Netzwerkprofile der PCs vorgenommen.

Sie sollten für alle Netzwerkprofile identische Einstellungen vornehmen. Klicken Sie anschließend auf "Verbindungssicherheitsregeln" und wählen Sie "Neue Regel" aus. Danach können Sie auswählen, welche Art von Regel Sie erstellen wollen. Dazu stehen Ihnen verschiedene Möglichkeiten zur Verfügung. Für die Einrichtung von IPSec-Verbindungen eignet sich am besten die Option "Isolierung", die Sie auch auswählen sollten. Eine Isolierungsregel schränkt Verbindungen auf der Grundlage der von Ihnen definierten Authentifizierungskriterien ein. So können Sie Computer Ihrer Domäne von Computern außerhalb der Domäne isolieren.

Die Authentifizierungsausnahme kann verwendet werden, um Computer unabhängig von anderen Verbindungssicherheitsregeln von der Anforderung auszunehmen, sich selbst zu authentifizieren. Dieser Regeltyp wird gewöhnlich verwendet, um den Zugriff auf Infrastrukturcomputer (Active Directory-Domänencontroller, Zertifizierungsstellen oder DHCP-Server) zu gewährleisten, mit denen der betreffende Computer bereits kommunizieren muss, bevor eine Authentifizierung durchgeführt werden kann. Obwohl die Computer von der Authentifizierung ausgenommen sind, können sie nach wie vor von der Firewall blockiert werden, sofern keine Firewallregel die Verbindung zulässt. Mit dem Regeltyp "Server zu Server" wird die Kommunikation zwischen zwei Computern, zwischen zwei Subnetzen oder zwischen einem bestimmten Computer und einer Gruppe von Computern authentifiziert. Mit einem Tunnel wird die Kommunikation zweier Computer zwischen Tunnelendpunkten abgesichert, etwa bei VPNs oder L2TP-Tunneln (IPsec Layer 2 Tunneling Protocol).

Auf der nächsten Seite des Assistenten legen Sie die Art der Authentifizierung fest. Wählen Sie hier die Option "Authentifizierung ist für eingehende Verbindungen erforderlich und muss für ausgehende Verbindungen angefordert werden" aus. Mit dieser Option bestimmen Sie, dass der gesamte eingehende Datenverkehr authentifiziert oder anderenfalls blockiert wird. Der ausgehende Datenverkehr kann authentifiziert werden, ist aber auch bei fehlerhafter Authentifizierung zugelassen. Mit der Option "Authentifizierung für eingehende und ausgehende Verbindungen anfordern" legen Sie fest, dass der gesamte ein- und ausgehende Datenverkehr authentifiziert wird, lassen die Kommunikation jedoch auch bei fehlerhafter Authentifizierung zu. Sobald die Authentifizierung durchführbar ist, wird der Datenverkehr authentifiziert.

Die Option "Authentifizierung" ist dabei für eingehende und ausgehende Verbindungen erforderlich und legt fest, dass der gesamte ein- und ausgehende Datenverkehr authentifiziert oder anderenfalls blockiert wird. Auf der nächsten Seite stellen Sie ein, auf welche Art die Authentifizierung hergestellt werden soll. Wählen Sie hier "Computerzertifikat" aus. Bei dieser Methode ist ein gültiges Integritätszertifikat zur Authentifizierung erforderlich oder wird angefordert. Die Option "Standard" legt die Authentifizierungsmethode gemäß der Konfiguration auf der Registerkarte "IPSec-Einstellungen" in den Eigenschaften der Windows-Firewall mit erweiterter Sicherheit fest. Bei "Computer und Benutzer" wird sowohl die Computer- als auch die Benutzerauthentifizierung verwendet. Das bedeutet, dass sowohl die Benutzer- als auch die Computerauthentifizierung angefordert wird oder erforderlich sein kann, bevor die Kommunikation fortgesetzt wird.

Kerberos nur in der Domäne

Das Authentifizierungsprotokoll Kerberos Version 5 kann nur verwendet werden, wenn sowohl der Computer als auch die Benutzer Mitglieder einer Domäne sind. Beim Computer ist die Computerauthentifizierung über Kerberos Version 5 erforderlich oder wird angefordert, bei Benutzern die Benutzerauthentifizierung mithilfe der Lösung. Aktivieren Sie die Option "Nur Integritätszertifikate akzeptieren". Bei dieser Methode ist ein gültiges Integritätszertifikat zur Authentifizierung erforderlich oder wird angefordert.

Klicken Sie auf "Durchsuchen" und wählen Sie die erstellte Root-CA aus. Aktivieren Sie auf der nächsten Seite die Regel für alle drei Netzwerkprofile. Schließen Sie die Erstellung der Regel mit der Definition der Bezeichnung ab. Idealerweise testen Sie solche Verbindungsregeln zunächst in einer Testumgebung und beschränken die Gruppenrichtlinie, welche die Verbindungssicherheitsregeln festlegt, nur auf diese OU. Anschließend können Sie die Computerkonten der beteiligten PCs oder Server in diese OU verschieben, um die gesicherte Kommunikation zu verifizieren. *(dr)*

Messaging und Collaboration mit Zarafa

Das Beste aus beiden Welten

von Thomas Drilling

Zahlreiche Groupware-Lösungen auf Basis von Linux buhlen um die Gunst der Unternehmen, die Exchange beispielsweise aus Kostengründen nicht oder nicht mehr nutzen wollen. Während manche Firmen daher auf solche Lösungen umsteigen, schrecken viele von dem Vorhaben zurück, weil es unmöglich scheint, den Anwendern das komfortable und vertraute Outlook abzugewöhnen oder zumindest für gleichwertigen Ersatz zu sorgen. Zarafa geht den umgekehrten Weg und baut Microsofts MAPI-Protokoll transparent in seinen Zarafa Collaboration Server ein, so dass Unternehmen Ihre Outlook-Clients einfach weiter verwenden können. In diesem Workshop setzen wir einen Zarafa-Server auf und verbinden ihn mit Outlook als Client.

Der Zarafa-Server stellt durch die Kompatibilität zu Microsoft Exchange auf Protokoll-Ebene nicht nur funktional betrachtet einen Ersatz für einen Exchange-Server dar. Mit ähnlichen Argumenten vermarkten auch andere Groupware-Hersteller ihre Produkte, doch Zarafa garantiert "migrationsfrei" sowohl die Verfügbarkeit von Exchange-/Outlook-Datenbeständen, Postfächern und Adressbüchern in Echtzeit als auch die Verwendbarkeit von Outlook als Client.

Während andere Groupware-Hersteller unter dem Motto "Bloß weg von Microsoft" vorrangig das Konzept Groupware und Collaboration auf Basis von freier Software in das Zentrum ihrer Vermarkungsstrategien rücken, richtet sich das ursprünglich unter der Bezeichnung "Exchange4Linux" (E4l) entwickelte Zarafa ausdrücklich an Unternehmen und Nutzer von Microsoft-Produkten. Zwar sollen und können auch diese mit Zarafa ihren Exchange-Server in Rente schicken, der zentrale Mail- und Collaboration-Client bleibt aber Outlook auf Basis von MAPI. Zarafa kooperiert aber auch problemlos mit bereits vorhandenen MS Exchange-Servern und spart so zumindest Kosten bei der Erweiterung des firmeneigenen Collaboration-Netzwerkes.

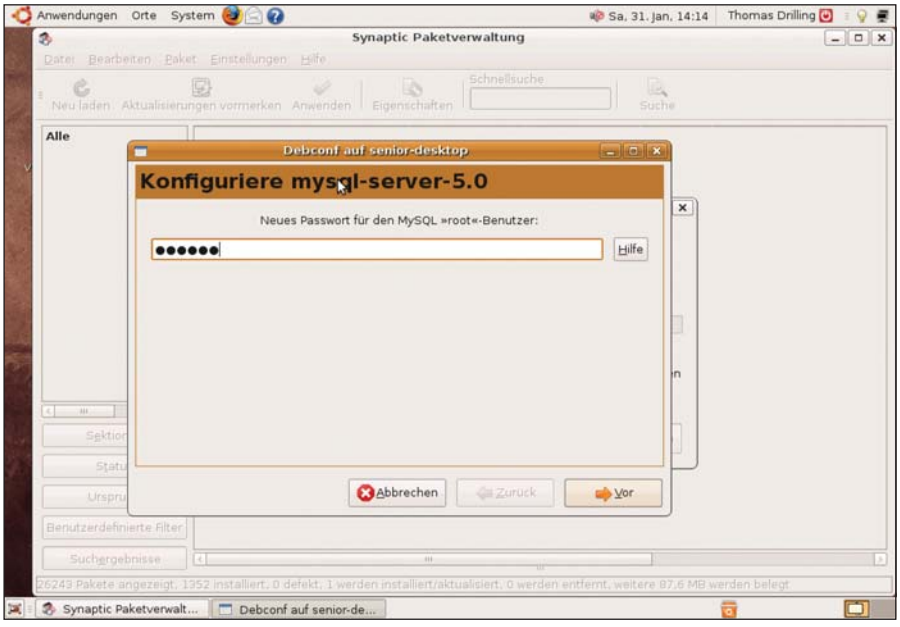


Bild 1: Ubuntu setzt das MySQL Root-Passwort bereits während der Installation

Damit aber noch nicht genug: während das frühere E4l als Server kaum sichtbar in Erscheinung trat (der E4l-Applikationsserver läuft auf der Linux-Maschinedezent im Hintergrund), verfügt das Gemeinschaftsprodukt mit der Bezeichnung "Zarafaserver" seit Ende 2006 über ein äußerst leistungsfähiges, AJAX-basiertes Web-Interface. Der Zarafa-Webclient ist Outlook so weit wie möglich nachempfunden, sodass jeder Anwender problemlos damit arbeiten kann. Mit dem Browser-Client erschließen sich dem Produkt auf Anhieb auch Linux und andere Client-Plattformen, was Zarafa zu einer universell einsetzbaren Groupware-Lösung macht, deren innovativer Kern in der sauberen Implementation des MAPI-Protokolls liegt.

Editionen und Leistungsfähigkeit

Zarafa Germany [1] bietet den Zarafa Server aktuell in der Version 6.20 seit 2006 an. Dabei haben IT-Verantwortliche die Wahl zwischen den vier Versionen "Community", "Standard", "Professional" und

"Enterprise" [2]. Interessant sind auch die Angebote zweier deutscher Firmen [3,4], die sich beide deutlich einfacher und komfortabler in Betrieb nehmen lassen als Zarafa allein.

In Zarafa zeichnen sich die Professional- und die Enterprise-Edition durch das eingebaute webbasierte Monitoring-System aus und letztere bietet sogar Multiserver-Support. Außer der Community-Edition unterstützt Zarafa auch die Authentifizierung gegen ein Active Directory. Daneben bieten alle Versionen neben der MAPI-Unterstützung (die Community-Edition erlaubt allerdings nur drei Outlook-Clients) ein IMAP/POP3- sowie ein iCal-Gateway. Sie können Ihre MAPI/Outlook-Postfächer also auch problemlos mit einem beliebigen IMAP/POP-Client wie Evolution oder Thunderbird abrufen oder den Exchange-Kalender via iCal (iCalendar-Standard, RFC 2445) einbinden. Alle Editionen verfügen über das beschriebene Webinterface und sind mittels Z-Push zu Activesync kompatibel. Neu in den Professional- und Enterprise-Versionen ist der Blackberry-Support (BES-Integration).

Wir zeigen Ihnen im Folgenden die Installation und Inbetriebnahme der Community-Edition [5], die Sie frei herunter laden können. Sie steht in tar.gz-Paketen von knapp 13 MByte für Red Hat, SUSE, Debian und Ubuntu zur Verfügung. Offiziell wird Ubuntu maximal bis zur Version 8.04 unterstützt, allerdings läuft auch die Version 8.10 problemlos.

Vorbereitungen zur Zarafa-Installation

Einzige Voraussetzungen zur erfolgreichen Installation sind MySQL (ab 4.1 oder höher), Apache (ab 2.0) mit PHP-Unterstützung, sowie PHP selbst. Für Apache installieren Sie unter Ubuntu entweder das Paket *apache2-mpm-prefork* oder das Metapaket *apache2*. Den PHP-Support stellen Sie durch die Installation von *libapache2-mod-php5* und *php5-common* sicher. Schließlich installieren Sie den MySQL-Server durch die Auswahl der Pakete *mysql-server-5.0* und *libmysqlclient15off*. Ubuntu konfiguriert das Paket während der Installation und setzt auch gleich das Admin-Passwort für MySQL. Sie haben jedoch die Möglichkeit, die Konfiguration nebst Passwort für MySQL jederzeit später mit folgendem Befehl zu ändern: *sudo dpkg-reconfigure mysql-server-5.0*.

Zarafa fungiert wie Exchange als vollwertiger "MAPI-Provider" und legt seine Datenspeicher komplett in der SQL-Datenbank ab und zwar sowohl die eigentlichen MAPI-Stores als auch (optional) sämtliche Benutzerinformationen. Der Zarafa-Server erzeugt die Datenbank nebst den zugehörigen Tabellen beim ersten Start, wozu der bei der Installation angegebene MySQL-Benutzer über die dazu erforderlichen Rechte zum Anlegen einer neuen Datenbank verfügen muss. Sie müssen allerdings dem Installationsskript nicht zwangsläufig den MySQL Admin-Account übergeben. Entscheidend ist nur, dass der angegebene MySQL-Benutzer Datenbanken anlegen darf. Nach der Erstinitialisierung von Zarafa können Sie dem betreffenden MySQL-Benutzer dieses Recht auch wieder entziehen. Nehmen Sie nach der Installation von Zarafa tief greifende Änderungen am Paketunterbau vor, konfigurieren Sie das Zarafa-Paket unter Debian und Ubuntu mit *sudo dpkg-reconfigure zarafa* neu.

Entpacken Sie das tar.gz-Archiv der Community-Version für die gewünschte Plattform (in unserem Beispiel Ubuntu) in einem beliebigen Verzeichnis. Im Zielverzeichnis finden Sie nach dem Entpacken die passenden Debian-Pakete *zarafa-licensed_6.20-13194_i386.deb* sowie das Installationsskript *install.sh*. Dieses kümmert sich sowohl bei der Deb- als auch bei der RPM-Version um das Auflösen der Abhängigkeiten, das Abfragen der wichtigsten Optionen zur Konfiguration und um das Initialisieren der MySQL-Datenbank.

Starten Sie das Installationsskript mit "-config", überspringt das Skript die eigentliche Installation und fragt lediglich die verfügbaren Konfigurationseinstellungen ab. Sie verschaffen sich auf diese Weise leicht einen Überblick der verfügbaren Optionen. So kann Zarafa die Benutzerauthentifizierung beispielsweise wahlweise gegen ein LDAP-Verzeichnis durchführen oder alternativ die lokale Benutzerdatenbank des Servers beziehungsweise das Datenbankplugin benutzen. Das Installationsskript verwendet per Default –

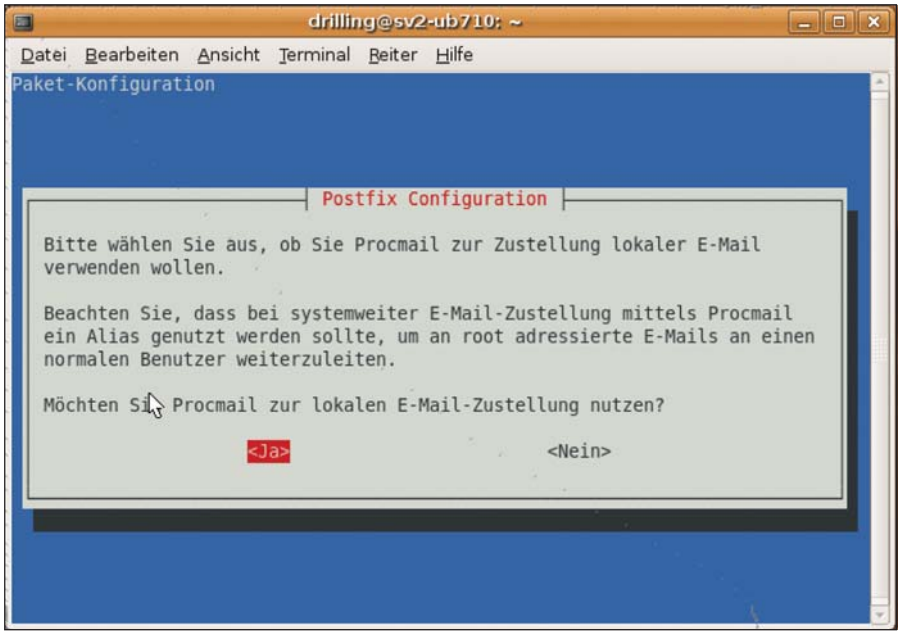


Bild 2: Die Zarafa-Installation verlangt eine fertige oder angepasste MTA-Konfiguration

also beim Aufruf von *Install.sh* oder weiteren Optionen – die Authentifizierung in der MySQL-Datenbank. Zarafa speichert dann sämtliche Benutzerdaten und den kompletten Datenspeicher des Servers (MAPI-Stores) in einer MySQL-Datenbank.

Außerdem muss auf dem Zielsystem ein Mail Transfer Agent (MTA) laufen und entsprechend Ihrer Vorstellungen konfiguriert sein. Bei Ubuntu kommt üblicherweise "Exim" zum Einsatz, den Sie mit *eximconfig* konfigurieren. Installieren Sie alternativ Postfix, passen Sie diesen bei der Erstinstallation des Paketes oder jederzeit später durch Aufruf von *dpkg-reconfigure postfix* dem eigenen MTA-Szenario an. Allerdings verfügt auch das Zarafa-Installationsskript über eine Konfigurationsoption für den SMTP-Server. Dabei ist es empfehlenswert, Postfix so zu konfigurieren, dass sich Procmail um das Einliefern der Mails kümmert.

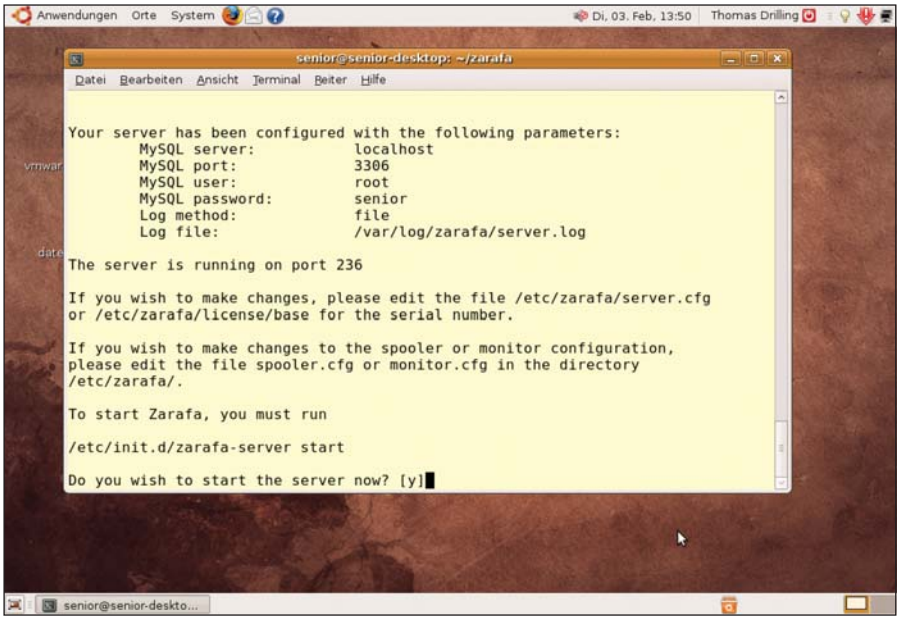


Bild 3: Nach der Installation ist der Zarafa-Server direkt einsatzbereit

Zarafa neu installieren

Sind alle Vorbereitungen abgeschlossen, starten Sie das Zarafa-Installationsskript. Dieses überprüft das Vorhandensein der benötigten Komponenten (etwa MySQL) und installiert dann den Zarafa-Server, wozu es etwaige sonstige Abhängigkeiten automatisch auflöst. Dabei stellt das Skript im weiteren Verlauf eine Reihe von Fragen, wie etwa nach einem gültigen Lizenz-Key. Sie können das Feld im Falle der Community-Edition frei lassen oder sich per Registrierung [6] eine Testlizenz besorgen. Möchten Sie diese später durch einen unbegrenzten Lizenz-Key ersetzen, müssen Sie diesen in der Datei */etc/zarafa/license/base* eintragen.

Das Installationsskript fragt dann nach dem bei der Installation von MySQL angelegten Passwort für den MySQL-Amin-Acccount "root". Die Skripteinstellungen für die von MySQL verwendeten Standardports können Sie in der Regel übernehmen, sofern Sie nicht selbst vorab abweichende Einstellungen konfiguriert haben. Das Skript fragt außerdem über welchen SMTP-Server Zarafa ausgehende Mail verschicken soll, wobei "localhost" der Default-Wert ist, die meisten Admins hier jedoch einen Smarthost eintragen. Bei allen weiteren Einstellungen sollten Sie die Defaultvorgaben des Skriptes bestätigen.

Es empfiehlt sich auf jeden Fall, die Frage "Do you wish to run the Zarafa gateway as well?" mit "Yes" zu beantworten, denn so stellt der Zarafa-Server MAPI-Stores auch als IMAP-Postfächer zur Verfügung, sodass Sie außer mit Outlook mit jedem beliebigen IMAP-Client Mails vom Zarafa-Server abholen können. Für Outlook-Adressbücher und Kalender brauchen Sie aber auf jeden Fall den Zarafa-Outlook-Client. Auch hier können Sie die Defaultvorgaben des Skriptes für die IMAP-/POP-Standardports übernehmen, es sei denn, Sie haben Ihr System vorab abweichend konfiguriert oder betreiben parallel noch einen anderen IMAP-Server.

Zum Schluss listet das Skript noch einmal sämtliche getätigten Einstellungen auf und fragt, ob es den Zarafa-Server starten soll. Dadurch legt Zarafa zunächst den "Public Store" (öffentlicher Ordner) an, um weitere Benutzer-Stores müssen Sie sich mit dem Kommandozeilen-Werkzeug "zarafa-admin" selbst kümmern. Anschließend startet das Installationsskript die Zarafa-Services "zarafa-spooler", "zarafa-monitor" und gegebenenfalls "zarafa-gateway". Sie erhalten weiterhin den Hinweis, dass Sie das Webinterface unter *http://{Zarafa-Server}/webaccess* erreichen, allerdings nur, wenn Sie die PHP-Option "magic_quotes_gpc" in */etc/php5/apache2/php.ini* abschalten. Starten Sie abschließend Apache mit

```
sudo /etc/init.d/apache2 restart
```

neu und Zarafa Webaccess steht bereit.

Manuelle Installation

Neben der Installation von Zarafa mit Hilfe des mitgelieferten Installationsskriptes können Sie die Zarafa-Pakete auch manuell mit *apt-get* oder *Gdebi* installieren. Zur Konfiguration können Sie sich an der kommentierten Beispielkonfiguration */usr/share/zarafa/example.server.cfg* orientieren, die Sie an Ihre Bedürfnisse anpassen und unter */usr/share/zarafa/server.cfg* speichern.

Für die manuelle Zarafa-Installation muss die Datei mindestens den MySQL-Benutzer mit gültigem Passwort enthalten. Die zur Authentifizierung verwendete Option "user-plugin" ist in *server.cfg* mit "db" vorbelegt, sodass Zarafa seine Benutzer in der

MySQL-Datenbank ablegt und gegen diese authentifiziert. Haben Sie die Zarafa Deb- oder RPM-Pakete manuell installiert, müssen Sie die erforderlichen Dienste "zarafa-server", "zarafa-spooler" und "zarafa-monitor" sowie auf Wunsch "zarafa-gateway" und "zarafa-ical" nach der Installation manuell starten. Sie finden sämtliche Startskripte wie üblich unter */etc/init.d*. Den Zarafa-Server starten Sie nun mit

```
sudo /etc/init.d/zarafa-server start
```

Stores und Benutzer

Läuft der Server, können Sie MAPI-Stores und Benutzer anlegen. Wie MS Exchange/Outlook kennt auch Zarafa "öffentliche" und "private" Stores. MAPI-Stores können wie bei Outlook die Objekttypen "Postfach", "Kalender" und "Kontakte" enthalten. Darüber hinaus gibt es genau einen zwingend erforderlichen "Public Store" (Öffentlicher Ordner), den Sie mit dem Kommandozeilenwerkzeug */usr/bin/zarafa-admin* durch den Befehl *zarafa-admin -s* anlegen.

Zum Anlegen privater Stores verwenden Sie den Befehl

```
zarafa-admin -c {Benutzername} -p
  {Passwort} -e {E-Mail-Adresse} -f
  {vollständiger Name} -a \
  {Administrator}
```

Die Optionen sind im Wesentlichen selbsterklärend, der Parameter "Administrator" erwartet entweder "0" oder "1" beziehungsweise "yes" oder "no" in Abhängigkeit davon, ob der Benutzer über administrative Rechte verfügen soll. Das Erstellen und Löschen von Benutzern und Gruppen ist nur beim DB-Plugin möglich; das LDAP-Plugin synchronisiert die Benutzerinformationen mit dem bestehenden LDAP-Verzeichnis. Zum Löschen eines Stores verwenden Sie

```
zarafa-admin -d {Benutzer}
```

Existiert mindestens ein Benutzer, können Sie sich bereits am Zarafa Webaccess anmelden. Allerdings empfängt/versendet Zarafa bis jetzt noch keine E-Mails im angegebenen Store. Sieht Ihr Mailserver-Einsatzszenario den Versand über einen externen Smarthost nicht vor, sondern direkt über den Zarafa-Server, starten Sie den "Zarafa-Spooler" (*/etc/init.d/zarafa-spooler*) mit *zarafa-spooler start*. Der Zarafa-Spooler leitet ausgehende E-Mails per Default an den auf Ihrem Server laufenden MTA weiter. Sieht Ihre MTA-Konfiguration ohnehin den Versand ausgehender Mail über einen Smarthost vor, können Sie Ihren Smarthost auch direkt beim Start des Zarafa-Spoolers als Parameter übergeben:

```
zarafa-spooler start {SMTP-Server
  Ihres Providers}
```

Alternativ hinterlegen Sie Ihren Smarthost in der Zarafa-Spooler-Konfiguration unter */etc/zarafa/spooler.cfg* und lesen die Konfigurationsdatei direkt beim Starten des Zarafa-Spoolers ein:

```
zarafa-spooler -c /etc/zarafa/
  spooler.cfg
```

E-Mailempfang konfigurieren

Bis jetzt verfügen Sie zwar über einen funktionierenden Zarafa-Server nebst Benutzer mit E-Mail-Postfach, Sie müssen aber noch dafür sorgen, dass ankommende E-Mails auch tatsächlich in diesem Postfach landen. Der bei Zarafa zuständige "Mail Deliver Agent" (MDA) "zarafa-

Outlook als Client

Damit Outlook mit Ihrem Zarafa-Server kommuniziert, also als "Fullclient" für dessen MAPI-Stores fungiert, müssen Sie an Ihren Windows-Arbeitsplätzen den mit Zarafa gelieferten Outlook-MAPI-Client installieren. Ohne diesen könnten Sie mit Outlook zwar Mails Ihrer Zarafa-Postfächer via IMAP lesen, Gruppenkalender oder globale Adressbücher bleiben aber außen vor. Sie finden das Windows-Installer-Paket zarafaclient-6.20.1.msi im Archiv-Verzeichnis von Zarafa oder im Download-Bereich der Community-Version [5].

Damit Outlook den MAPI-Client auch verwendet, müssen Sie lediglich – analog zum Vorgehen im Exchange-Server – ein neues Profil anlegen. Erstellen Sie dazu ein neues Mail-Profil über "Systemsteuerung / Benutzerkonten / Mail" und wählen Sie im Dialog "E-Mail-Konten" den Eintrag "Ein neues E-Mail-Konto hinzufügen". Nun wählen Sie unter "Servertyp" die Option "Zusätzliche Servertypen", hier steht jetzt der Servertyp "Zarafa 6 Server" zur Verfügung. Es folgt das Dialogfeld "Zarafa Outlook Sharing", in dem Sie die Verbindungsdaten zu Ihrem Zarafa-Server eintragen und außerdem Ihre Benutzerdaten. Jeder Zarafa-Nutzer muss sein eigenes Outlook-Profil erhalten und seinen MAPI-Client mit den persönlichen Nutzerdaten bestücken . Wählen Sie den Verbindungstyp "Online", wenn der betreffende Windows-Arbeitsplatz permanent mit dem Zarafa-Server verbunden ist. Mit "OK" verbindet sich Outlook erstmals mit dem Server.

Konfigurieren Sie Outlook so, dass das Programm per Default mit diesem Profil startet oder nach dem zu verwendenden Profil fragt, wenn Sie sich abwechselnd mit unterschiedlichen MAPI-Servern verbinden möchten.

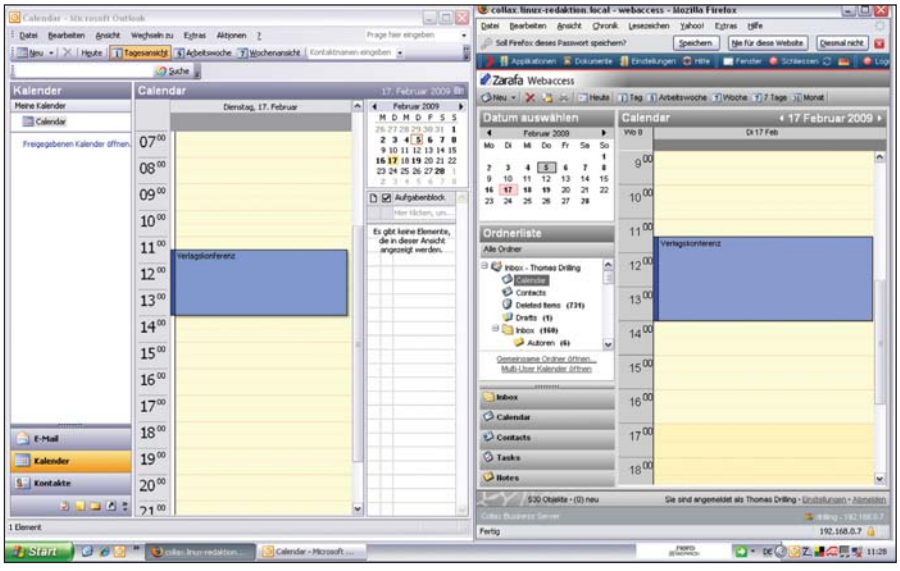


Bild 4: Zwillinge: der Web-Client ist vom echten Outlook kaum zu unterscheiden

Bild 5: Zarafa-Nutzer haben zahlreiche Optionen, um das Webinterface an persönliche Bedürfnisse anzupassen

dagent" liest E-Mail-Nachrichten per Default von der Standardeingabe. Das Übergeben von Mails durch "zarafa-dagent" an den gewünschten Zarafa-Store steuert einer der Parameter "postfix", "procmail" oder "qmail", den Sie an Ihr Mailserver-Szenario anpassen können.

Ist bei Ihnen beispielsweise *procmail* für das Einsortieren eingehender Mail in die lokalen Benutzerfächer zuständig, lautet der passenden Aufruf von "zarafa-dagent" in Ihrer procmail-Konfigurationsdatei */etc/procmailrc*:

```
:0 w
«| /usr/bin/zarafa-dagent {Benutzer}
EXITCODE=$?
```

Wird procmail in Ihrem Mailserverszenario vom fetchmail-Skript aufgerufen, lautet der zugehörige Eintrag in */etc/fetchmailrc*:

```
#"{E-Mail-Adresse des gewünschten
  IMAP-Postfachs}" poll {Adresse des
  IMAP-Servers Ihres Providers} pro-
  tocol imap user "Benutzername beim
  IMAP-Provider" there with password
  "xxxxxxxxxxx" mda "/usr/bin/proc-
  mail -t -a \$EXTENSION"
```

Webinterface nutzen

Neben dem speziell von Zarafa entwickelten Outlook-Client, der im Gegensatz zu ähnlichen Lösungen anderer Anbieter keinen Connector darstellt, sondern Zarafa-Stores in Echtzeit zur Verfügung stellt – was insbesondere bei Gruppenkalendern wichtig ist –, können Sie auch das hervorragende AJAX-Webinterface als Client nutzen. Dies steht nach erfolgreicher Installation unter *http://192.168.0.7/webaccess* zur Verfügung. Oberfläche und Bedienung des Clients lehnen sich bis ins Detail an Outlook an, sodass sich jeder Anwender, insbesondere durch die Bedienung aller Operationen mit der Maus und Drag&Drop, sofort zurechtfindet. Eingehende E-Mails landen bei korrekter Konfiguration Ihres Mailstacks automatisch im Store des jeweiligen Zarafa-Benutzers. Jeder Nutzer kann seinen Web-Client mit einem Klick auf "Einstellungen" problemlos an seinen persönlichen Geschmack anpassen. Das betrifft neben Sprache und Layout auch das E-Mailformat oder die Kalender-Konfiguration.

Was die eigentlichen Arbeitsabläufe angeht, arbeiten Sie sowohl mit dem Webinterface als auch mit Outlook genauso wie bei einem echten Exchange-Server. Beim Adressbuch haben Sie die Wahl zwischen dem globalen Adressbuch und Ihrem persönlichen Kontakte-Ordner. Selbstverständlich lassen sich unter "public folder" weitere öffentliche Ordner für "E-Mail", "Kontakte" oder "Kalender" anlegen.

Fazit

Zarafa ist gerade in der Community- oder Standard-Edition die ideale Groupware-Lösung für Unternehmen, die bereits Exchange einsetzen. So ersetzt oder ergänzt Zarafa Ihren Exchange-Server zu einem Bruchteil der Kosten und Ihre Nutzer müssen sich nicht an einen anderen Client als Outlook gewöhnen. Wer seine Client-Landschaft zusätzlich um weitere Plattformen erweitern möchte, findet im hervorragenden Webinterface dank AJAX beinahe die gleiche Funktionalität im identischen Look.

Auch mobile Mitarbeiter profitieren durch Activesync-Kompatibilität und Z-Push und wenn nötig, erhalten Sie mit einer der kommerziellen Versionen auch Blackberry-Support. Ebenso das webbasierte Monitoring und die Active Directory-Unterstützung der kostenpflichtigen Versionen sind immer noch deutlich günstiger als mit Microsoft-Produkten. Da das Produkt ausgehend von Exchange4Linux bereits eine recht lange Entwicklungsgeschichte aufweist, läuft es stabil und zuverlässig – was unser Langzeittest bestätigt. *(jp)*

Links

[1] Zarafa Germany
www.zarafaserver.de

[2] Leistungsmerkmale Zarafa-Versionen
www.zarafa.com/?q=de/content/versions

[3] Collax GmbH
http://www.collax.com/de/produkte/partner-produkte/zarafa.html

[4] Bitbone AG – bitkit|ZARAFA
www.bitbone.de/bitkit-ZARAFA.53.0.html

[5] Zarafa Community-Edition
www.zarafa.com/download-community

[6] Testlizenz für Community-Edition
www.zarafaserver.de/download/evaluation.html

Tipps & Tricks ohne Gewähr

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.

Microsoft Windows

Auf einem meiner Windows XP-Rechner habe ich versehentlich eine wichtige **Systemdatei gelöscht**. Nun scheint die automatische **Wiederherstellung** von Systemdateien nicht vollständig zu funktionieren. Kann ich diese auch manuell anstoßen?

Zunächst können Sie sich eine Übersicht über die vergangenen Änderungen an Systemdateien anschauen. Diese finden Sie unter "Systemsteuerung / Verwaltung / Computerverwaltung / System / Ereignisanzeige / System". Eventuell haben Sie so die Möglichkeit, die betroffene Datei aus einer anderen Quelle wieder in Ihr System einzuspielen. Sie können die Windows-eigene Wiederherstellung zudem mit *sfc* auslösen. Die Option "/scannow" bewirkt dabei eine sofortige Überprüfung Ihres Rechners. Mit "/scanonce" schaut sich das Tool die Dateien beim nächsten Neustart an. Weitere Informationen erhalten Sie über den Parameter "/?". *(dr)*

Wir nutzen **Windows Server 2008** im abgespeckten **Server Core-Modus**. Hin und wieder kommt es vor, dass wir dort mehrere Dateien in ein **Archiv** zusammenfassen müssen. Aus verschiedenen Gründen kommt die Installation von externen Kommandozeilentools hierfür nicht in Frage. Gibt es einen anderen Weg?

Wie Sie bereits geschrieben haben, bieten sich im Regelfall Kommandozeilenprogramme wie etwa 7-Zip zum Packen und Entpacken von Dateien an. Können Sie diese jedoch nicht installieren, stellen CAB-Files eine Alternative dar. In diesen Cabinet-Dateien können sich mehrere Files befinden, die sich mit dem Server-eigenen Tool *Makecab.exe* zusammenfassen lassen. Ein Extrahieren von Dateien ermöglicht dagegen *Expand.exe*. Um nun eine große Datei in eine komprimierte CAB-Datei zu kopieren, geben Sie den Befehl

```
MAKECAB c:\{Originaldatei}.dat
  {Komprimierte_Datei}.cab /l c:\
```

ein. Sie können am Ende des Kommandos auch ein anderes Verzeichnis als Ziel angeben als den Ursprungsordner. Um nun mehrere Dateien in eine CAB-Datei zusammenzufassen, geben Sie im Verzeichnis mit den zu komprimierenden Dateien die Befehle

```
DIR /B > mycab.ddfMAKECAB /d cabi-
  netnametemplate={Zieldatei}.cab /f
  mycab.ddf
```

nacheinander ein. Damit existiert nun das Verzeichnis *Disk1* mit der erstellten CAB-Datei. Die Originaldateien stellen Sie anschließend mit dem Befehl

```
EXPAND -R {Komprimierte_Datei}.cab
  -F:* c:\{Zielverzeichnis}
```

wieder her. *(dr)*

Beim **Installieren von Geräten** kommt es unter XP immer wieder vor, dass das Betriebssystem vor einem **nicht signierten Treiber** warnt. Da ich häufiger Rechner aufsetze und die Hardware ändere, nerven mich diese Meldungen etwas. Über welchen Weg kann ich sie ausschalten?

Windows erlaubt das Deaktivieren dieser Hinweise über die lokalen Sicherheitseinstellungen. Sie finden diese über "Start / Ausführen / secpol.msc". Gehen Sie darin zum Punkt "Lokale Richtlinien / Sicherheitsoptionen". Dort finden Sie den Eintrag "Geräte: Verhalten bei der Installation von nichtsignierten Treibern". Öffnen Sie diesen Punkt mit einem Doppelklick und ändern Sie ihn auf die Einstellung "Ohne Warnung akzeptieren". Nach einem Bestätigen der Änderung mit "Übernehmen", sollte Windows Sie künftig bei nicht signierten Treibern in Ruhe lassen. *(dr)*

Leider habe ich bei einigen neu aufgesetzten Vista-Rechnern den Überblick darüber verloren, ob diese nun schon aktiviert wurden oder nicht sowie über die dabei verwendeten **Lizenzschlüssel**. Gibt es eine Möglichkeit, den Lizenzstatus schnell und unkompliziert anzuzeigen?

Sie können unter Vista über den einfachen Befehl

```
slmgr.vbs -dli
```

sehen, ob Vista bereits aktiviert wurde und welcher Lizenzkey dabei zum Einsatz kam. Dabei muss unter "Lizenzstatus" der Eintrag "Lizenziert" stehen und im Feld "Teil-Product-Key" der zugehörige Schlüssel. *(dr)*

Linux

Wir nutzen einen Linux-Rechner mit **Samba** in unserem Netzwerk. Dabei möchten wir auch **Nachrichten** von diesem Server **an Windows-PCs im Netzwerk verschicken**, etwa über ein Skript, wenn dieser bestimmte Aufgaben erledigt hat. Wie können wir dies über die Kommandozeile tun?

Es gibt einen einfachen Befehl, um Netzwerkmessages an Windows-Rechner zu senden. Geben Sie das Kommando

```
echo {Ihre Nachricht} | smbclient -M
  {Windows-PC}
```

ein. Natürlich muss der Windows-PC erreichbar sein und nicht etwa durch eine Firewall gegen den Samba-Server geschützt. *(dr)*

Apple

Wenn ich unter Mac OS X **mehrere Fenster geöffnet** habe und zu einer bestimmten Anwendung im **Dock** wechsle, sollen sich die anderen Fenster auf dem Desktop schließen. Dies lässt sich über die **Wahltaste** erreichen. Doch gibt es auch eine Möglichkeit, ohne Wahltaste ein Schließen der Fenster zu bewirken?

Es gibt hierfür einen Befehl, mit dem Sie das Verhalten der Fenster beeinflussen können. Geben Sie im Terminal die Zeile

```
defaults write com.apple.dock
  single-app -bool TRUE
```

ein, dann ist beim Aufrufen von Programmfenstern keine Wahltaste mehrnötig. Doch zunächst müssen Sie erst Ihr Dock neu starten, damit es die Änderung übernimmt:

```
killall Dock
```

Die anderen Fenster verschwinden nun automatisch beim Wechsel der Applikationen. Möchten Sie diese Änderung wieder rückgängig machen, ersetzen Sie einfach das "TRUE" am Ende des ersten Kommandos durch ein "FALSE". *(dr)*

Wie kann ich einen **virtuellen Desktop** in einer **anderen Domäne** einrichten als in der des Setup Wizards von XenDesktop?

Mit dem XenDesktop Setup Wizard lassen sich virtuelle Desktops auch in einer anderen Trusted Domain als in der installierten einrichten. Voraussetzung dafür ist, dass alle anderen XenDesktop-Komponenten in derselben Domain installiert sind wie der Wizard. Für dieses Vorgehen benötigen Sie den XenDesktop Setup Wizard Version 2.1.33267 für Citrix XenDesktop 2.1 und Windows Server 2003 (32- und 64 Bit). Laden Sie den Wizard herunter und installieren Sie ihn. Nun setzen Sie den Wizard als Domain User in derjenigen Domain auf, in der Sie die Desktops einrichten möchten. Nun sind einige Änderungen am Umgebungs-Setup erforderlich, damit die Desktops mit dem Desktop Delivery Controller erfolgreich bereitgestellt und registriert werden. In unserem Beispiel sind nun alle XenDesktop-Komponenten in Domain A installiert, die Desktops sollen in Domain B eingerichtet werden, zu der die User dieser Desktops gehören. Die Domains müssen wechselseitig trusted sein und zum selben Domänenwald im Active Directory gehören. Die Forwarder müssen für den Domain Name Service (DNS)-Server jeder Domain aufeinander eingestellt sein. Führen Sie nun als Domain-Administrator den Konfigurations-Wizard des Provisioning Servers der Domain B aus, damit der Anwender Zugriff auf die Farm hat. Fügen Sie anschließend in der Access Management-Konsole den Domain-Administrator von Domain B hinzu. Er startet als Administrator der Farm das Setup-Tool und nutzt die Administrationsknoten. Nun fügen Sie die Domain User Group von Domain B zur Distributed COM User Group des Desktop Delivery Controllers hinzu uns stellen sicher, dass das Virtual Disk Image für den virtuellen Desktop zur Domain B gehört. *(Citrix/dr)*

Viele weitere Tipps & Tricks sowie konkrete Hilfe bei akuten Problemen bekommen Sie auch im Internet bei unserem exklusiven Foren-Partner administrator.de. Fast 50.000 registrierte Benutzer tauschen dort in über 100 Kategorien ihre Erfahrungen aus und leisten Hilfestellung. So wie der IT-Administrator das praxisnahe Fachmagazin für Administratoren ist administrator.de die Internetplattform für alle System- und Netzwerkadministratoren.
www.administrator.de
ADMINISTRATOR | IT-FORUM

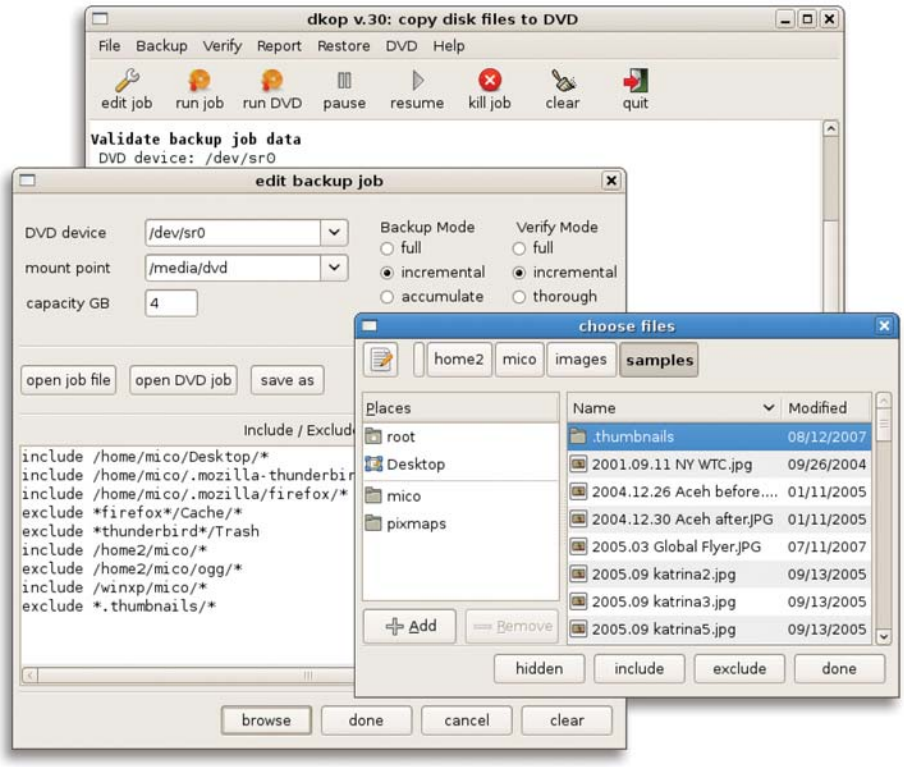
Tools

Um als Administrator **Windows-Systeme** remote zu verwalten – ohne teure KVM- oder Onboard-Fernzugriffs-Lösung – bietet sich das RDP-Protokoll an, das in jedem Windows-Server ab Windows Server 2000 enthalten ist. RDP bietet dabei eine bessere Performance als VNC, hat jedoch den Makel, dass jede **RDP-Verbindung** ein eigenes Fenster benötigt. Dieses oftmals unübersichtliche Vorgehen lässt sich mit dem Tool **Royal TS** vermeiden.

Der zentrale Nutzen des Werkzeugs ist die gemeinsame Verwaltung mehrerer, parallel geöffneter Remote Desktops. Der Wechsel zwischen verschiedenen Sitzungen erfolgt durch einen Mausklick, wobei der jeweils geöffnete Remote Desktop in der Mitte der Konsole als Vollbild erscheint. Allerdings lassen sich einzelne Verbindungen auch so konfigurieren, dass sich diese in einem eigenen Fenster öffnen. Das Tool erlaubt zudem, einzelne Remote-Desktop-Verbindungen über einen Assistenten zu erstellen, der neben den Verbindungsoptionen wie Auflösung, verbundene Laufwerke, IP-Adresse oder Name des Servers auch eine Authentifizierung einschließt. So lässt sich eine RDP-Ver-

bindung per Doppelklick öffnen. Die Verbindungen lassen sich auch gruppieren und auch diese Gruppen können Administratoren in einer so genannten RTS-Datei zusammenfassen. Royal TS lässt sich so konfigurieren, dass eine bestimmte Datei mit den enthaltenen Gruppen automatisch geöffnet wird. *(jp)*
Quelle: http://code4ward.net/main/

Zur Sicherung von Linux-basierten Systemen und Daten auf DVD steht mit **dkopp** eine Lösung bereit, die durchaus professionellen Ansprüchen genügt. Die Steuerung der Backups erfolgt dabei über eine GUI und erlaubt einen hohen Grad an Automatisierung. Die Lösung ermöglicht das volle, inkrementelle oder "akkumulierte" **Backup** einzelner Dateien oder Verzeichnisse.
Das akkumulierte Backup unterscheidet vom inkrementellen, dass es Dateien, die zwischen dem letzten und dem aktuellen Backup auf der Quelle gelöscht wurden, nicht von der DVD entfernt. Das inkrementelle Backup von dkopp erzeugt also immer eine exakte, aktuelle Kopie der Quelle. Ein einmalig angestoßenes Backup können Administratoren dabei über die GUI speichern und den kompletten Vorgang so automatisieren. Darüber hinaus lässt sich das Werkzeug auch per Skript steuern. Die Bedienung ist dabei sehr komfortabel und erlaubt beispielsweise komplette Verzeichnisse in die Sicherung aufzunehmen, dabei aber einzelne Files auszuschließen. Einen hohen Grad an Sicherheit bei der Erstellung und dem Einsatz der DVD als Sicherungsmedium bietet das Tool durch eine umfassende Prüfung des Zielmediums, die neu geschriebene und bereits vorhandene Dateien auf Lesbarkeit prüft. Große Backups lassen sich auf mehrere DVDs schreiben, die im Falle eines Recovery in beliebiger Reihenfolge wieder eingespielt werden können. Als Richtwert lässt sich bei der Sicherung ein Wert von 150 bis 300 MByte pro Minute angeben. *(jp)*
Quelle: http://kornelix.squarespace.com/downloads/



Backups auf DVD lassen sich mit dkopp leicht automatisieren

Das Management von Dateien gehört in einer ESX-Infrastruktur zu den größten Herausforderungen für den Administrator: im Normalfall erfolgt beispielsweise eine Kopie eines ISO-Files in den ESX-Server oder das Backup einer Virtuellen Maschine per FTP. Doch leider bietet ESX 3 diese Möglichkeit nicht an. Zudem würden beim Einsatz von FTP Passwörter im Klartext übertragen, ein unakzeptables Sicherheitsrisiko. Die empfohlene Alternative – SCP –, um eine Datei von einem Windows-Rechner nach ESX oder umgekehrt zu kopieren, bringt jedoch durch die für SSH notwendigen Berechnungen einen enormen Performanceverlust mit sich. Das Tool **FastSCP** schafft Abhilfe.
Das kostenlose Werkzeug erlaubt alle oben angesprochenen Arten von Datei-Transfers in oder aus einem ESX-Server heraus bei deutlich erhöhter Geschwindigkeit. Insbesondere bei großen und sehr großen Dateien ist dies spürbar. FastSCP ermöglicht dabei Dateioperationen zwischen standalone-ESX-Maschinen and ESXi-Hosts (oder zwischen Hosts in verschiedenen vCentern). Die Sicherheit gewährleistet das Tool durch den Einsatz von Einmal-Usernamen und -Passwörtern für den Datentransfer. Zudem ermöglicht das Werkzeug Administratoren, mit mehreren ESX-Servern gleichzeitig in einer Explorer-artigen Oberfläche zu arbeiten. Auch kann sich der IT-Verantwortliche an all diesen ESX-Servern per Single-Sign-On anmelden, muss also beim Wechsel zwischen verschiedenen ESX-Servern keine erneute Anmeldung vollziehen. *(jp)*
Quelle: www.veeam.com/esx-fastscp.html

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

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

Download der Woche

Kompetentes Schnupperabo sucht neugierige Administratoren

Sie wissen, wie man Systeme
und Netzwerke am Laufen hält.
Und das Magazin IT-Administrator weiß,
wie es Sie dabei perfekt unterstützt:

mit praxisnahen Workshops, aktuellen
Produkttests und nützlichen Tipps und Tricks
für den beruflichen Alltag.

Damit Sie sich Zeit,
Nerven und Kosten sparen.

Teamwork in Bestform.
Überzeugen Sie sich selbst!

6 Monate lesen

3 Monate bezahlen

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

Microsoft Exchange-Umgebungen richtig dokumentieren

Volle Akteneinsicht

von Manuela Reiss

Das Projekt zur Einführung von Exchange ist abgeschlossen. Nun fehlt nur noch das Betriebshandbuch, um das neue System dem Betrieb zu übergeben. Als Vorlage dient ein Musterbetriebshandbuch, das seit vielen Jahren die Basis aller firmeninternen Betriebshandbücher bildet. Bei dieser weit verbreiteten Vorgehensweise wird jedoch vergessen, dass ein Betriebshandbuch, das beispielsweise einmal dazu diente, den einzigen Windows 2000-Server der Firma zu beschreiben, für eine komplexe Exchange-Umgebung kaum die richtige Vorlage liefert. Worauf bei der Dokumentation einer Exchange-Umgebung zu achten ist und wie sich diese in die Gesamtdokumentation einordnen sollte, zeigt dieser Beitrag.

Klassische Exchange-Betriebshandbücher zeichnen sich häufig durch folgenden Aufbau aus: Das erste Kapitel enthält eine Beschreibung der Exchange-Server einschließlich der Hardwaredokumentation und der vorhandenen Active Directory-Umgebung beziehungsweise der Exchange-Organisation, der typischerweise die Installationsanleitung folgt. Die anschließenden Kapitel enthalten in der Regel eine Beschreibung der administrativen Aufgaben, bevor möglicherweise noch Backup- und Überwachungstätigkeiten erläutert werden. Den Abschluss bildet häufig ein Kapitel zum Umgang mit Störungen und zur Wiederherstellung von Exchange.

Trennung zwischen Hardware und Anwendungen erforderlich

Problematisch ist hierbei bereits die fehlende Unterscheidung zwischen der Dokumentation der Serverhardware und des Betriebssystems sowie der installierten Exchange-Anwendung. Bei einem einzelnen Server, der dediziert für die Bereitstellung einer Anwendung eingesetzt wird, ist eine Trennung zwischen Server-Hardware und Betriebssystem sowie den installierten Anwendungen nicht zwingend erforderlich. In diesem Fall kann die Beschreibung aller Komponenten durchaus in einem Handbuch erfolgen.

Anders verhält es sich mit auf unterschiedlichen Rechnern gehosten Anwendungen, wie dies typischerweise bei heutigen Exchange-Installationen der Fall ist. Exchange ist optimal dafür ausgelegt, im Verbund mit mehreren Servern zu arbeiten und bereits in mittelgroßen Firmen nehmen in der Regel verschiedene Server unterschiedliche Serverrollen in der Exchange-Organisation wahr. Hierzu zählen etwa:

- Ein oder mehrere Backend-Server (oder auch Einsatz eines Clusters) zur Verwaltung der Datenbanken für die Postfächer und für die öffentlichen Ordner
- ein Connector-Server für die Datenübermittlung an das Internet
- ein Frontend-Server zur Annahme von Anfragen und Verteilung an die Backend-Server
- ein Exchangeserver zur Bereitstellung von OWA-Zugriffen für die Anwender
- ein Faxserver

Zusätzlich werden Administrationskonsolen zur Verwaltung von Exchange benötigt, die auch auf Arbeitsplatzrechnern installiert sein können. Die Auflistung zeigt, dass eine 1-zu-1-Zuordnung zwischen Server und Anwendung in modernen Systemumgebungen kaum noch möglich ist. Hinzu kommt, dass Exchange eng mit dem Active Directory verwoben ist, was Sie bei der Dokumentation ebenfalls berücksichtigen müssen.

Modulares Betriebshandbuch mit getrennten Systemakten

Den genannten Anforderungen begegnen Sie mit einem übergreifenden, modular aufgebauten Betriebshandbuch, das getrennte Beschreibungen für die verschiedenen Systeme umfasst. Als System werden hierbei

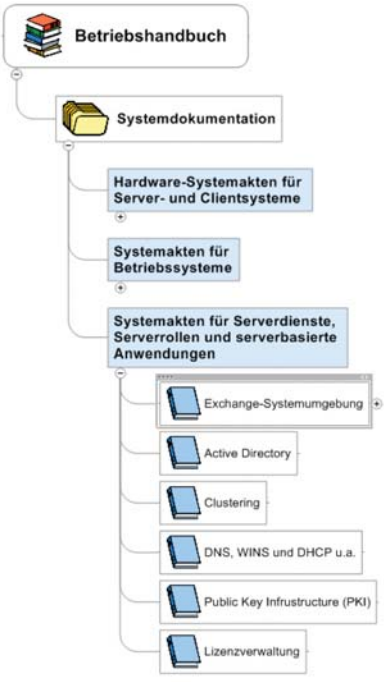


Bild 1: Modular aufgebautes Betriebshandbuch mit dem Fokus auf Exchange

sowohl physische Server (Hardware-Systemakten) als auch Active Directory oder Exchange (Software-Systemakten) betrachtet. Eine sinnvolle Dokumentation für die Exchange-Umgebung sollte demnach einerseits die die Hardware-Systemakten für die Server enthalten (alle serverspezifischen Hardwareinformationen). Das installierte Betriebssystem, installierte Anwendungen und beispielsweise die Rolle, die der Server in Active Directory und der Exchange-Organisation inne hat, werden hier lediglich benannt.

Zusätzlich legen Sie Systemakten für das oder die Betriebssysteme, für Active Directory sowie für die Exchange-Umgebung an, die detailliert die Konfiguration der Systeme beschreiben. Beispielsweise ist in der Hardware-Systemakte für einen Server zu vermerken, dass es sich um einen Frontend-Server für Exchange handelt und auf die entsprechende Systemakte für Exchange zu verweisen, die alle relevanten Informationen zur Exchangekonfiguration enthält. Aber auch die Dokumentationen für alle anderen Anwendungen und Dienste, die unmittelbaren oder mittelbaren Einfluss auf Exchange haben, gliedern Sie in diese Struktur ein. Hierzu zählen beispielsweise der DNS-Dienst, aber auch Systemakten für den Cluster oder die Lizenzverwaltung. Einen möglichen Aufbau eines solchen Betriebshandbuchs zeigt Bild 1.

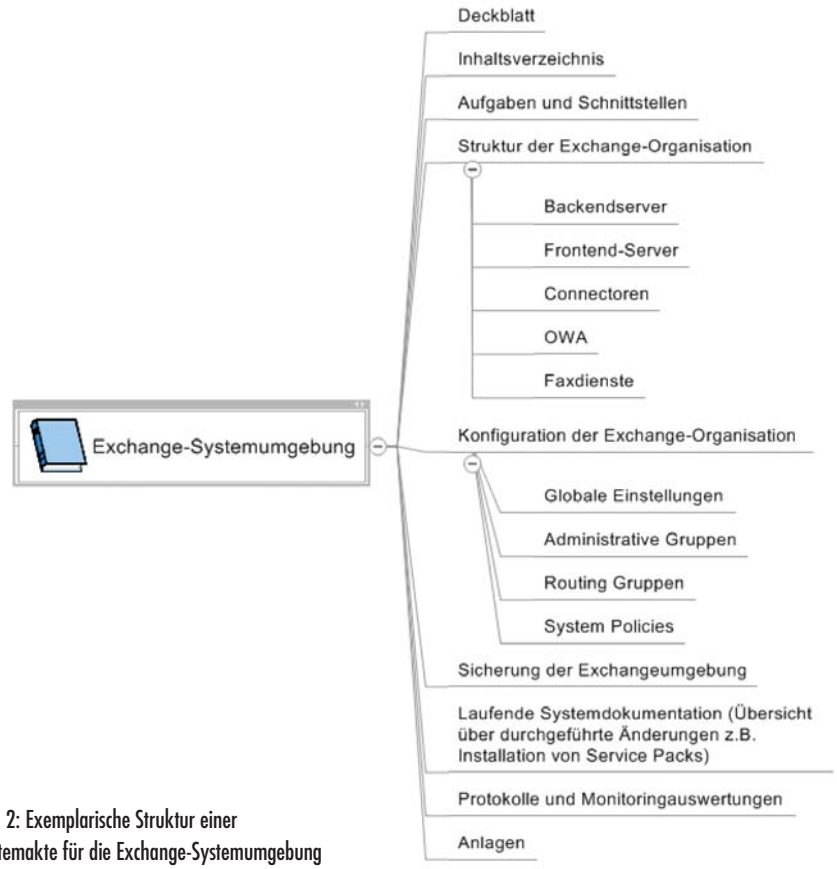


Bild 2: Exemplarische Struktur einer Systemakte für die Exchange-Systemumgebung

Sinnvoll ist es, ein solch modulares Betriebshandbuch nicht allein auf die Exchangesysteme zu beschränken, sondern für den gesamten IT-Betrieb zu verwenden. Entscheidend ist, dass Sie bei dieser Vorgehensweise alle Dokumente zueinander in Beziehung stellen, ohne Informationen redundant erfassen zu müssen.

Der Inhalt der Systemakte für die Exchange-Systeme ist natürlich von der eingesetzten Exchange-Umgebung und auch von der Methode zur Erfassung der Informationen abhängig (manuell oder mittels entsprechender Software) – Bild 2 zeigt exemplarisch die Struktur einer solchen Systemakte.

SEMINARMARKT

Den IT-Administrator Seminarmarkt mit News zu IT-Trainings finden Sie auch online auf:
www.it-administrator.de/seminarmarkt

Mit Wissen zum Erfolg
ADN
Die ADN Akademie bietet bundesweit Seminare und Zertifizierungen als autorisiertes Schulungscenter für:
CITRIX DataCore IGEL Microsoft SONICWALL SWYX
Buchen Sie noch heute!
02327.9912-425
www.adn.de/training

www.SharePoint Camp.de
In 5 Tagen zum SharePoint Profi!
Crashkurs zu SharePoint 2007
20.-24. April '09, Frankfurt
11.-15. Mai '09, Burghausen
bis zu 400,- EUR sparen!
ppedv Events

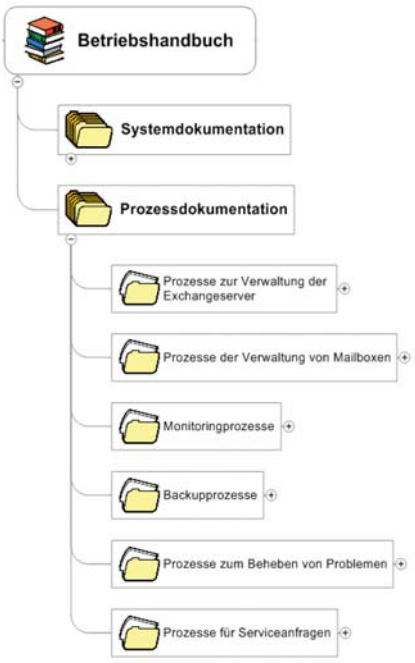


Bild 3: Administrative Anleitungen müssen an den Aufgaben der Mitarbeiter ausgerichtet sein

Systemdokumentation und Arbeitsabläufe trennen

Weiterhin ist eine klare Trennung der Systemakten von Administrationsanleitungen sinnvoll. Schließlich interessiert den für die Einrichtung von Benutzern verantwortlichen Administrator die Konfiguration der Connectoren bei seiner täglichen Arbeit überhaupt nicht. Er benötigt vielmehr rollenspezifische Prozessbeschreibungen und Arbeitsanleitungen beispielsweise für die Wiederherstellung versehentlich gelöschter Postfachinhalte.

Den administrativen Tätigkeiten lassen sich verschiedene Prozessbereiche zuordnen. So gibt es neben den Aufgaben zur Verwaltung von Mailboxen (etwa Einrichtung von Mailboxen oder Pflege öffentlicher Ordner) vor allem auch Tätigkeiten zur Verwaltung der Serversysteme (beispielsweise das Einspielen von Service Packs oder Updates). Weitere Tätigkeiten können Sie beispielsweise in die Bereichen Datensicherung und Monitoring einordnen. Und natürlich benötigen Sie auch Anleitungen zum Umgang mit Problemen und Serviceanfragen.

Es ist daher sinnvoll, auf der obersten Ebene im Betriebshandbuch zwischen der zuvor beschriebenen Systemdokumentation und einer Prozessdokumentation zu unterscheiden. Im Übrigen entspricht eine solche prozessorientierte Strukturierung Organisationsmodellen wie ITIL beziehungsweise Sicherheitsstandards wie dem BSI-Grundschutz, die ebenfalls zunehmend prozessorientiert ausgerichtet sind. Und bei Audits im Rahmen von Zertifizierungen ist die Prüfung der Prozessbeschreibungen ein wesentlicher Bestandteil.

Notfall ist nicht Betrieb

Generell muss Ihr Betriebshandbuch neben der Systemdokumentation alle mit dem IT-Regelbetrieb verbundenen Aufgaben (Was und Wie) einschließlich der erforderlichen Kontroll- und Wartungsarbeiten beschreiben. Nicht Gegenstand eines Betriebshandbuchs aber ist die Dokumentation für den Notfall. Notfälle unterliegen nämlich zwingend anderen Abläufen als der Regelbetrieb und Sie müssen diese daher gesondert dokumentieren. Zudem enthält eine Notfalldokumentation häufig Inhalte, die höheren Geheimhaltungsanforderungen unterliegen als Dokumente für den Regelbetrieb. So ist beispielsweise ein Dokument zur Wiederherstellung von Exchange nach einem Angriff als sicherheitskritisches Dokument zu behandeln, da dessen Inhalte einem potentiellen Angreifer (auch einem internen) wichtige Informationen liefern könnten.

Alle für eine Wiederherstellung im Notfall relevanten Informationen sollten daher in einem gesonderten Notfallhandbuch dokumentiert werden. Die Basis für eine solche Notfalldokumentation bildet wiederum die Systemdokumentation, auf die zu verweisen ist und die auch aus diesem Grund ständig aktuell gehalten werden muss.

Problemfall Installationsanleitungen

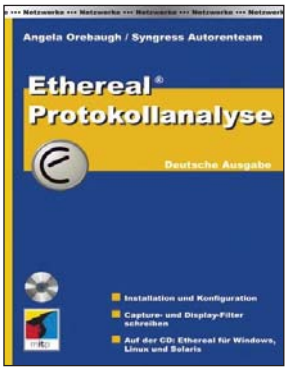
Ein Abgrenzungsproblem ergibt sich häufig bei der Fragestellung, wie mit Installationsanleitungen umzugehen ist. Im betrachteten klassischen Betriebhandbuch für Exchange sind diese Anleitungen meist ein umfassender Bestandteil desselben.

Wie bereits ausgeführt, soll das Betriebshandbuch den ordnungsgemäßen Regelbetrieb unterstützen. Anders aber als beispielsweise Arbeitsplatzrechner, die im Rahmen des IT-Betriebs regelmäßig bereitzustellen sind, ist die Installation von Exchange wohl kaum eine regelmäßige Betriebsaufgabe. Da aber natürlich in einem Notfall eine Neueinrichtung erforderlich werden kann, muss zumindest vonseiten der Notfalldokumentation Zugriff auf die Installationsanleitung möglich sein. Meist ist es daher sinnvoll, dass Sie die Installationsanleitungen den Wiederherstellungsprozessen im Notfallhandbuch beifügen. Hierbei ist jedoch zu beachten, dass vorhandene Installationsanleitungen häufig aus Projekten stammen und dann eine Beschreibung der Erstinstallation liefern. Diese müssen Sie dann an die jeweils aktuellen Erfordernisse anpassen.

Fazit

Häufig erfolgt die Dokumentation der firmeneigenen Exchange-Systemumgebung auf der Basis viele Jahre alter Betriebshandbuchvorlagen. Diese werden aber in der Regel nicht den Anforderungen gerecht, die eine moderne Client-Server-Anwendung wie Exchange fordert. Zu empfehlen ist der Aufbau eines modularen Betriebshandbuchs mit getrennten Systemakten für die Serverhardware, die Exchange-Umgebung und Active Directory. Administrative Aufgaben werden davon getrennt und prozessorientiert dokumentiert. Zusätzlich sollten Sie alle Informationen, die für eine Wiederherstellung im Notfall relevant sind, in einem speziellen Notfallhandbuch dokumentieren. Allerdings genügt es nicht, die Notfallprozesse einmalig zu dokumentieren: Sie müssen diese auch regelmäßig anpassen und üben. *(jp)*

Ethereal Protokollanalyse



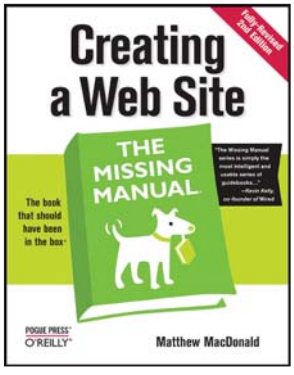
Statt als Taschenbuch oder Hardcover kommt "Ethereal Protokollanalyse" auf elektronischem Weg zum Leser. Der Verlag gibt den Titel nur noch als E-Book heraus. Das ist zwar nicht die angenehmste Art, ein Fachbuch zu lesen, in diesem Fall lohnt es sich dennoch. Gute Grundlagentitel zur Protokollanalyse sind selten, Bücher, die dazu Ethereal als Tool verwenden, noch seltener. Dass das Buch etwas in die Jahre gekommen ist, verrät der Name bereits, denn Ethereal heißt mittlerweile Wireshark. Doch das tut der Nützlichkeit wenig bis keinen Abbruch. Für erfolgreiche Protokollanalyse ist das "Wie" ohnehin wichtiger als das "Womit". Viel Platz wird der Installation eingeräumt. Während bei der Windows-Variante als fertiges Binary ein Doppelklick zur Installation reicht, wird bei Linux der komplette Weg durchgesprochen. Dann geht es an den Einsatz der Software, in deren Zentrum das Aufzeichnen der Datenpakete steht. Es gibt klare Hinweise über die Größe und Funktion des Ringpuffers sowie zu den Aufzeichnungsoptionen.

Im darauf folgenden Kapitel über die Filteranwendung merkt der Leser die Unterschiede zwischen alter und neuer Version am deutlichsten. Es gibt mehr und bessere Graphen aus den abgefangenen Daten und Zusammenhänge können nun erheblich besser visualisiert werden. Die Autorin liefert mehrere Beispielmitschnitte auf der CD mit, um die Analyse selbst am PC nachvollziehen zu können. Danach führt ein eigenes Kapitel in die hohe Kunst der Filterprogrammierung (Capture und Display) mit Befehlen und logischen Operatoren ein. Orebaugh erklärt Technik und Konzept gut, aber knapp. Wer selbst aktiv werden möchte, kommt um weitere Infos und die intensive Beschäftigung mit den Wireshark-Mailinglisten nicht herum. Leider konzentriert sich die Autorin im nächsten Kapitel mit Beispieltraces auf die Analyse von Trojanern und Port-Scanning Techniken. Das ist spannend, für den täglichen Admin-Einsatz wären weniger aufregende Beispiele wie die Analyse von Performanceproblemen sinnvoller gewesen.

Fazit: "Etherreal Protokollanalyse" ist ein sehr gutes Grundlagenbuch zu Wireshark und zur Anwendung von Protokollanalyzern. Kenntnisse zu den Protokollen selbst sollten allerdings vorhanden sein, denn dazu gibt es im Buch wenig bis keine Infos. *Elmar Török*

Autor:	Angela Orebaugh
Verlag:	mitp
Preis:	44,95 Euro
ISBN:	978-38266-1492-7
Bewertung:	★★★★☆

Creating a Web Site



Ein paar HTML-Grundkenntnisse schaden nie, auch im Hinblick auf mögliche Sicherheitschecks des Webservers gegen Attacken von außen. Nun gibt es natürlich zahllose Bücher und Internetangebote wie die Website "selfhtml.de" zum Thema. Warum dann ein englisches Buch von O'Reilly als Lernhilfe? Weil die "Missing Manual"-Bücher so aufgebaut sind, wie sich das Einsteiger in ein Thema wünschen: Die Wissenssprünge zwischen den Kapiteln sind nie so groß, dass plötzlich unüberwindbare Hürden auftauchen, das Lerntempo ist angenehm und durch gut 550 Seiten Stärke bleibt dem Autor trotzdem genug Platz, um auch komplexe Inhalte ausführlich darzustellen.

Das Buch startet mit einer dankenswert kurzen HTML-Einführung und geht dann gleich an die erste Seite Code in XHTML. Die wichtigsten Elemente werden, noch ohne den Einsatz eines richtigen HTML-Editors, erklärt. Danach folgt ein Grundkurs zu Domain-Namen und den unterschiedlichen Wegen, eine Website online zu bekommen. Matthew MacDonald stellt insgesamt drei kostenlose Web-Editoren vor, im weiteren Verlauf arbeitet er größtenteils mit Code View. Ans Eingemachte geht es im Kapitel für den Umgang mit XHTM-Text, Cascading Style Sheets, Graphiken und Links. Der Schreibstil ist O'Reilly-typisch entspannt und locker, es gibt ständig Beispiele für die angesprochenen Elemente. Für die Bedürfnisse eines Admins reichen die ersten 300 Seiten, danach beschreibt der Autor vor allem die Interaktion mit dem Nutzer. Die Möglichkeiten, Google-Ads und Warenkörbe einzubinden sind ebenso dabei wie Kontaktformulare, Foren und Blogs. Ein Grund, warum das Buch trotz seiner Ausführlichkeit kompakt wirkt, ist der Verzicht auf Erklärungen zum Design. Wie die Seite, abgesehen von der groben Navigationsaufteilung, aussieht ist Material für ein anderes Buch – oder einen Designer. Hier geht es nur um die Umsetzung und das ist gut so.

Fazit: Eine optimale Starthilfe für den Admin, der sich in HTML-Programmierung einarbeiten möchte. Mit anderen Titeln mag es schneller gehen, mit "Creating a Web Site" geht es angenehmer und gründlicher. *Elmar Török*

Autor:	Matthew MacDonald
Verlag:	O'Reilly
Preis:	25,99 Euro
ISBN:	978-0-596-52097-7
Bewertung:	★★★★☆

www.debiananwenderhandbuch.de

Umfassender Online-Wälzer zu Debian

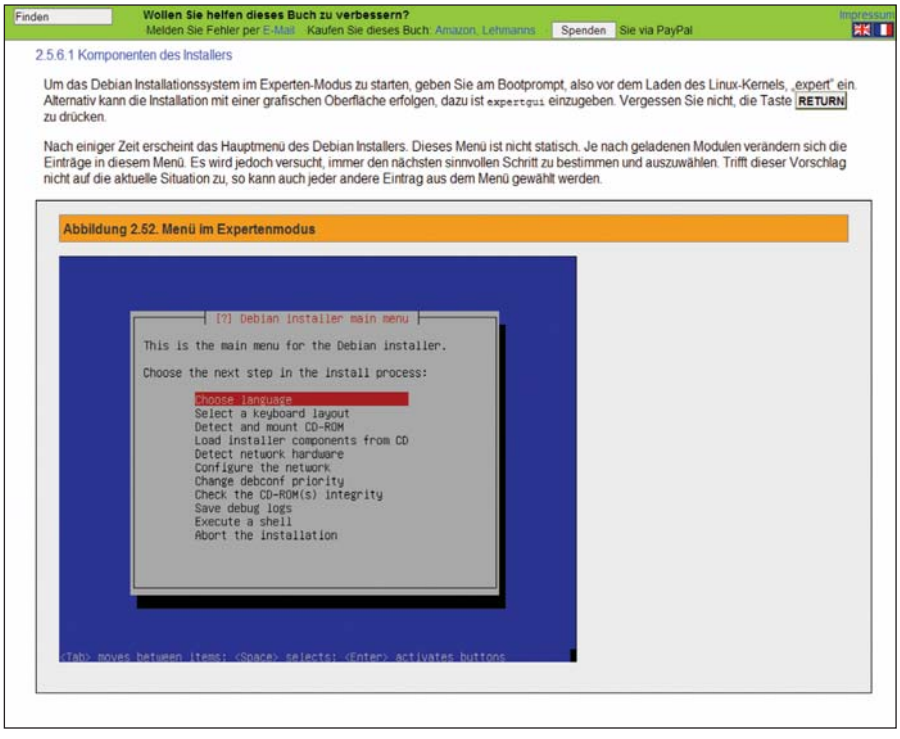
Für immer mehr Unternehmen spielt Linux als Betriebssystem eine Rolle – besonders im Server-Umfeld. Die Distribution Debian genießt dabei einen besonders guten Ruf, den sie nicht zuletzt ihrer hohen Qualität und der Sicherheit zu verdanken hat. Nicht nur für diese Zielgruppe hat Frank Ronneburg sein umfassendes "Debian Anwenderhandbuch" geschrieben.

Besonders den Praxisbezug schreibt er dabei groß und das ist auch gut so. In ganzen 18 Kapiteln erläutert Ronneburg so das Betriebssystem von A bis Z. Die Leser erfahren zunächst etwas über die Geschichte der Distribution, wobei der Autor sogar eine Originalmail von Ian Murdock, dem Debian-Projektgründer, über dessen Beweggründe mit aufführt. Debian steht übrigens für den Vornamen seiner Frau Debra und seinen eigenen, Ian.

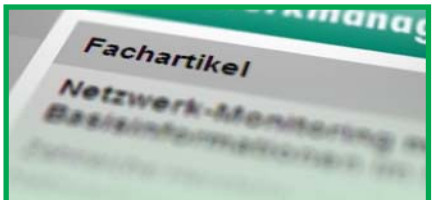
In den nachfolgenden Kapiteln geht es dann ans Eingemachte. Hier beschreibt Ronneburg die Installationsschritte und verdeutlicht die einzelnen Punkte mit Screenshots. So muss der Leser nicht im Dunkeln darüber tappen, ob er nun tatsächlich das gewünschte Ergebnis auf dem eigenen Bildschirm sieht oder nicht – der Praxisbezug lässt grüßen. Auch kommt die Paketverwaltung mit gleich zwei eigenen Kapiteln definitiv nicht zu kurz.

Für IT-Administratoren sicher interessant dürfte auch der Punkt "Server-Dienste" sein: Apache, FTP, DHCP und andere dienstbare Geister stehen ebenso auf dem Programm wie der Zugang zum Netzwerk und dem Internet. Auch die Sicherheit finden die Leser in Kapitel 17 ausführlich erklärt.

Mit dem Debian Anwenderhandbuch steht ein Standardwerk für alle Debian-Nutzer zur Verfügung – und das online und ganz im Linux-like kostenfrei. Selbstverständlich freut sich der Autor über Hinweise zu Neuerungen und Fehlern oder auch die ein oder andere Spende. *(dr)*



Bietet praxisnahes und fundiertes Debian-Know-how: Das Debian Anwenderhandbuch



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 von IT-Administrator können Sie mit den folgenden Links 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:**

Kostenreduktion im Netzwerk

Ein wirtschaftlicher Abschwung kann zur Folge haben, dass Unternehmen Ressourcen einschränken, die Anzahl ihrer IT-Fachkräfte reduzieren und die Beschaffung neuer Anlagen überprüfen. Derartige Einschränkungen bekommen vor allem IT-Administratoren zu spüren. Sie stehen unter dem Druck, funktionsfähige Netzwerke aufzubauen und müssen dabei häufig jeden Cent zweimal umdrehen. Dieser Beitrag beschreibt fünf Möglichkeiten, mit Hilfe des Netzwerks Kosten einzusparen.
www.it-administrator.de/themen/netzwerkmanagement/fachartikel/52173.html

Anwenderbericht: Outsourcing bei der Spam-Bekämpfung

Gerade in mittelständischen Betrieben haben die IT-Verantwortlichen auch ohne die Bedrohung durch Spam schon einen besonders großen Aufgabenbereich. Für den Anwender vor dem PC ist wichtig, dass die elektronische Kommunikation die Arbeit erleichtert und nicht erschwert. Damit die Administratoren ihre Zeit nicht nur mit der Feinjustierung der Spamfilter verbringen, bietet sich die Auslagerung des Spamschutzes an einen Dienstleister an.
www.it-administrator.de/themen/sicherheit/fachartikel/52174.html

Exchange-Server: Erstellen und Verwalten von Raum- und Gerätepostfächern

Unter Exchange Server 2007 sollten Sie Besprechungsräume immer als Raumpostfach anlegen, da diese in Outlook 2007 gesondert dargestellt werden. Auch Gerätepostfächer sollten separat angelegt werden. Der Beitrag zeigt, wie Sie mit Raum- und Gerätepostfächern optimal arbeiten.
www.it-administrator.de/themen/kommunikation/fachartikel/52175.html

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

»Der Film Wargames brachte mich zur IT«

Maurizio Schmidt ist als CTO für die komplexe IT-Landschaft der German Breast Group verantwortlich. Die Organisation ist eine Forschungseinrichtung zur Planung und Durchführung nationaler und internationaler Studien zur Behandlung von Brustkrebs. Die IT-Infrastruktur mit ihren zahlreichen Applikationen bildet dabei einen wichtigen Baustein für die erfolgreiche Arbeit des Institutes.

Welche Ausbildung haben Sie gemacht?

Ich stieg 1999 mit der Zertifizierung zum MCSE in die IT ein. Danach folgten kontinuierlich Weiterbildungsmaßnahmen im Bereich Linux (LPIC1/2) und VMware (VCP) sowie Microsoft (MCITSA) und Checkpoint NG3 (CCSA).

Warum sind Sie IT-Administrator geworden?

Die IT beziehungsweise Technik allgemein interessiert mich seit meiner Jugend nicht zuletzt dank des Films "Wargames". Während meiner Schulzeit jobbte ich dann unter anderem in einem Systemhaus. Privat arbeitete ich an meinem persönlichen Mailboxsystem und war aktiv im FidoNet unterwegs.

Welche IT-Umgebung betreuen Sie?

Ich bin verantwortlich für alle technischen Entwicklungen sowie Ansprechpartner bei technischen Fragen bezüglich Server, Server-Applications, Virtualisierung, Routing, VPN und Netzwerksicherheit. Unsere IT umfasst aktuell knapp 120 Clients und 35 Server-Systeme. Darunter sind Microsoft Exchange 2007, Microsoft Terminal Server, VMware ESX Server, Debian und RedHat Server, Microsoft ISA 2006 sowie verschiedene Datenbank-Server.

Was macht Ihnen an Ihrem Job am meisten Spaß?

Ich finde es befriedigend, Netzwerkstrukturen zu erstellen, die den Mitarbeitern unseres Hauses das Arbeiten erleichtern beziehungsweise die speziellen Prozesse erst möglich machen. Die IT-Administration kennt keine Routine. Ich kann zudem in meinem Aufgabenbereich meinem eigenen Anspruch gerecht werden, das System immer noch besser und ausfallsicherer zu gestalten.

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

Routinearbeiten wie Dokumentation, Reporting und Inventarisierung sind wichtig, gehören aber nicht zu meinen Lieblingsbeschäftigungen.

Geburtstag:	20.09.1978
Familienstand:	feste Beziehung
Hobbys:	Krav Maga, GeoCaching, American Football

Maurizio Schmidt, IT-Administrator

Was tun Sie für Ihre Fort- und Weiterbildung?

Ich profitiere sehr von meinen persönlichen Netzwerken, in denen ich mit anderen Administratoren Erfahrungen austausche. Darüber hinaus informiere ich mich über diverse Blogs und besuche zu meinem Aufgabengebiet passende Schulungsmaßnahmen.

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

Durch eine Unachtsamkeit in einem Login-Skript wurden montagmorgens um exakt 9:30 Uhr knapp 120 Clients ohne jegliche Vorwarnung heruntergefahren. Dies war gleichzeitig ein guter Performance-Test für unsere damals neue VoIP-Anlage, denn als Folge dessen wurde dann doch der ein oder andere Anruf in Richtung IT getätigt. Das war mir recht peinlich.

Was war Ihr größter Erfolg als IT-Administrator?

Vor zwei Jahren haben wir an einem Wochenende die gesamte Client-/Server-Struktur von Linux auf eine Microsoft-Basis umgestellt. Zusätzlich wurde eine VoIP-Telefonanlage implementiert, das gesamte Netzwerk-Backend ausgetauscht (Switches, Verkabelung) und von Exchange 2003 auf Exchange 2007 migriert. Teilweise haben wir auch Server mit VMware virtualisiert und sämtliche Fileserver auf neue Server portiert. Schließlich mussten alle 120 Clients mit neuem Image versehen werden. Am Montagmorgen lief alles tadellos – darauf bin ich wirklich stolz.

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

Mir fällt die Situation ein, in der ein Administrator eine 100.000 Euro teure USV implementierte. Die Server schloss er allerdings ausgerechnet an der Steckerleiste an, die nicht über die USV abgesichert war. Als dann tatsächlich ein Stromausfall eintrat, konnte die USV rein gar nichts retten.

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

Die Herausforderung besteht darin, die Anwenderfreundlichkeit und die Administrierbarkeit von Lösungen zu optimieren. Hier sind die Hersteller gefordert. Ein weiterer Punkt ist die Berücksichtigung interner und externer Einflüsse auf die Sicherheit. Intern müssen wir unseren Qualitätsstandard hochhalten, dabei aber aktuelle Trends und Kosten im Blick behalten.

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 5/09 erscheint am 4. Mai 2009

Schwerpunktthema:

Virtualisierung und Server-based Computing

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

Im **Juni** behandeln wir den Schwerpunkt **Clients – Sicherheit und Virtualisierung**. Dabei zeigen wir Ihnen unter anderem, wie Sie erfolgreich Datenabflüsse unterbinden und mit VirtualPC Ihre Clients sowie Windows und Mac OS virtualisieren.

Als Schwerpunkt im **Juli** folgt dann das Thema **Datei- und Datenbankadministration**.

***Im Test:* icomasoft PowerScripter für Virtual Infrastructure**

***Im Test:* ESX-Backuptool Vizioncore vRanger Pro**

***Workshop:* Hochleistungsnetze mit Infiniband**

***Workshop:* Roaming Profiles für Terminal Services einrichten**

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

IMPRESSUM

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

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

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

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

Autoren dieser Ausgabe
Petra Adamik, Thomas Drilling, Thomas Hümmler, Thomas Joos, Nils Kaczenski, Sandro Lucifora, Chris Meidinger, Manuela Reiss, Elmar Török

Autoren ITANet-Newsletter
Bernhard Bischoff, Hans-Martin Dietrich, Dr. Kürsad Gögen, Andreas Roscher

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

Es gilt die Anzeigenpreisliste Nr. 6 vom 01.01.2009

LAC/2008

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

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

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

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

Erscheinungsweise
monatlich

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

(Studentenabonnements nur gegen Vorlage einer gültigen Immatrikulationsbescheinigung)

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

Internet
www.it-administrator.de

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
80802 München

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

(zugleich Anschrift aller Verantwortlichen)

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

Eingetragen im Handelsregister des Amtsgerichts München unter HRB 151585.

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

ISSN
1614-2888

Urheberrecht
Alle in IT-Administrator erschienenen Beiträge sind urheberrechtlich geschützt. Alle Rechte, einschließlich Übersetzung, Zweitverwertung, Lizenzierung vorbehalten. Reproduktionen und Verbreitung, gleich welcher Art, ob auf digitalen oder analogen Medien, nur mit schriftlicher Genehmigung des Verlags. Aus der Veröffentlichung kann nicht geschlossen werden, dass die beschriebenen Lösungen oder verwendeten Bezeichnungen frei von gewerblichen Schutzrechten sind.

Haftung
Für den Fall, dass in IT-Administrator unzutreffende Informationen oder in veröffentlichten Programmen, Zeichnungen, Plänen oder Diagrammen Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlags oder seiner Mitarbeiter in Betracht. Für unverlangt eingesandte Manuskripte, Produkte oder sonstige Waren übernimmt der Verlag keine Haftung.

Manuskripteinsendungen
Die Redaktion nimmt gerne Manuskripte an. Diese müssen frei von Rechten Dritter sein. Mit der Einsendung gibt der Verfasser die Zustimmung zur Verwertung durch die Heinemann Verlag GmbH. Sollten die Manuskripte Dritten ebenfalls zur Verwertung angeboten worden sein, so ist dies anzugeben. Die Redaktion behält sich vor, die Manuskripte nach eigenem Ermessen zu bearbeiten. Honorare nach Vereinbarung.

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

Diese Ausgabe enthält ein Advertorial der Firma Computer Associates als Einhefter zwischen Seite 34 und 35, zwei Teilbeilagen der Firma ProSoft und den ITANet-Einhefter vom Verlag exklusiv für Abonnenten zwischen Seite 50 und 51.

Liefertermin:
Mitte Oktober 2009

Bestellen Sie jetzt

das IT-Administrator

Sonderheft II/2009!

180 Seiten Praxis-Know-how
rund um das Thema

Virtualisierung

zum "Frühbucher"-Sonderpreis* von

nur € 19,90!

** Der Sonderpreis gilt nur bei Bestellungen bis 30.05.2009.*
Danach erhalten IT-Administrator Abonnenten es zum Vorzugspreis von € 29,90
und Nichtabonnenten zum Preis von € 34,90.

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

iadministrator
Das Magazin für professionelle System- und Netzwerkadministration

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

☐ **Ja**, ich bestelle das IT-Administrator Sonderheft II/2009 zum **"Frühbucher"-Sonderpreis** von nur **€ 19,90** inkl. Versand und 7% MwSt. **Nur bei Bestellung bis 30.05.2009**

☐ **Ja**, ich bin IT-Administrator Abonnent mit der Abonummer (falls zur Hand) _____
und bestelle das IT-Administrator Sonderheft II/2009 zum **Abonnenten-Vorzugspreis** von nur **€ 29,90** inkl. Versand und 7% MwSt.

☐ **Ja**, ich bestelle das IT-Administrator Sonderheft II/2009 zum Preis von **€ 34,90** 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 0409

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

DriveLock 5.5

Intelligente Kontrolle mobiler Geräte

» KEINE CHANCE DEM DATENKLAU

DEN DATENLECKS AUF DER SPUR: DLP MIT DRIVELOCK

DriveLock ist das optimale Werkzeug gegen absichtlichen oder zufälligen Datenklau in Unternehmen. Neben dem Sperren von Ports und Schnittstellen wie beispielsweise USB, Firewire oder Bluetooth, können mit **DriveLock** auch Daten auf externen Datenträgern wie USB-Sticks oder CD-ROMs verschlüsselt werden. Damit sind diese Daten auch im Falle eines Verlierens der Datenträger nicht lesbar.

- » **MAXIMALE SICHERHEIT bei maximaler Flexibilität: Komplett oder selektiv**
- » **FULL DISK ENCRYPTION mit Pre-Boot-Authentifizierung und Rapid Recovery fürs schnelle Weiterarbeiten**
- » **VERSCHLÜSSELUNG MOBILER DATENTRÄGER und aller WINDOWS MOBILE GERÄTE**
- » **Intuitives Arbeiten und Auswerten mit dem SECURITY REPORTING CENTER (SRC)**
- » **Kinderleichte Vorbereitung der individuellen Konfiguration im Netzwerk durch den DEVICE SCANNER**
- » **Die Unterscheidung zwischen erlaubten und unerlaubten Programmen mit dem APPLICATION LAUNCH FILTER**

Referenzen / Informationen / Testversion

» **WWW.DRIVELOCK.DE**

DriveLock wird beständig aktualisiert und weiterentwickelt. Damit ist es ein perfektes Praxistool, geprüft und getestet von Fachblättern und erfolgreich eingesetzt bei vielen kleinen wie großen Unternehmen in Europa, Nordamerika und Asien.

CenterTools

IT-ADMINISTRATOR.DE

ITANet Schirmherrschaft:

REALTECH

ITANet

Newsletter für Mitglieder der System- und Netzwerk-User-Group

Transparenz

Der Schwerpunkt der folgenden 16 Sonderseiten zeigt auf, dass Transparenz im Netzwerk die IT-Sicherheit erhöhen und den reibungslosen Ablauf unternehmensinterner Prozesse gewährleisten kann. Dabei ist das Wissen um den Zustand der von der IT zu verantwortenden Geräte – Server, Clients et cetera – nur die Basis, die sich mit großen Managementlösungen realisieren lässt oder im "Eigenbau". Der Mehrwert, den die IT realisiert, liegt in der Verknüpfung dieser Zustandsinformationen mit den Unternehmensabläufen.

Transparenz und Mehrwert liegen auch uns in der Redaktion sehr am Herzen. Die folgenden Sonderseiten, die nur in den Ausgaben der Abonnenten enthalten sind, wie auch unsere kostenlosen Workshops stellen aus unserer Sicht einen Mehrwert dar, der "passt": mit unseren halbjährlichen Sonderseiten – dem ITANet-Newsletter – werfen wir eine Blick über den Tellerrand der alltäglichen Administrationspraxis. Ganz transparent von unserer Seite: Newsletter und auch Workshops ließen sich ohne unsere Partner und unseren Schirmherren nicht realisieren.

Und gerade das Feedback auf unsere Workshops freut uns ungemein: Fand sich beim ersten Workshop vor einem guten Jahr in Köln nur eine Gruppe von einem guten Dutzend Interessierter zusammen, verzeichneten wir bei unserem letzten Workshop zu MS Exchange über 50 Anmeldungen!

Schauen Sie doch auch mal vorbei, Ihr

John Pardey
Chefredakteur IT-Administrator

IT-Transparenz durch Key Performance Indikatoren

IT-Infrastrukturen im Wandel

von Dr. Kürsad Gögen

Die IT entwickelt sich rasant zum zentralen Transportmedium für Kommunikation und nimmt einen immer höher werdenden Stellenwert als globale Ressource ein. In den letzten Jahren werden immer stärkere Bestrebungen unternommen, um IT-Infrastrukturen zu vereinheitlichen und die in ihr laufenden sowie durch sie ermöglichten Datenströme und Prozesse zu homogenisieren. Dennoch ist ein gegenteiliges Resultat zu beobachten: Angetrieben durch die Konvergenz von Fremdtechnologien in die klassische Datentechnik entstehen immer komplexere, aber auch komplizierte IT-Infrastrukturen. Wie Sie mit Key Performance Indikatoren den Überblick behalten, zeigt dieser Beitrag.

Lebenswichtige gesellschaftliche Adern sind aus technischer und auch wirtschaftlicher Sicht bereits heute auf Gedeih und Verderb von der IT abhängig. Hierzu gehören sowohl öffentliche Organisationen als auch Unternehmen, die heute bereits ab dem Mittelstand ihre Geschäftsprozesse verstärkt auf der IT aufbauen.

Ein Prozess wie etwa das Nachbestellen einer Ware in Abhängigkeit vom Lagerbestand war früher möglicherweise an eine Person gekoppelt, die durch etwas Arithmetik und mithilfe eines Telefons diesen unregelmäßigen zyklischen Vorgang optimal aufrechterhalten konnte. Heute stehen hinter solchen "einfachen" Prozessen ganze Applikationswelten. Die Wechselwirkungskette, die früher hieß: "Bestand im Lager zählen" und wenn die Anzahl einen kritischen Wert unterschreitet "Ware nachbestellen", ist heute bei weitem nicht so durchsichtig.

Die kausalen Zusammenhänge, angefangen bei technischen Sensoren, Applikationsfarmen, Datenbanken und Hardware bis hin zu nicht technischen Bewertungen, sind selbst bei so einfachen Teilprozessen auf einen Blick kaum noch zu erfassen. Die Frage "Was muss ich machen, damit dieser Prozess besser läuft?" konnte im alten Bild heißen, eine "fähige" Person mit dieser Aufgabe zu beauftragen. Heute muss man, um die gleiche Frage zu beantworten, aus dem Blickwinkel eines Geschäftsprozesses nach sehr abstrakten Stellschrauben in einer komplexen Wirkungskette suchen, die wiederum signifikanten Einfluss auf andere Teilprozesse haben können. Bereits die Identifikation solcher Key Performance Indikatoren (KPI) stellt hohe Anforderungen an die Fachabteilungen, die abteilungsübergreifend kommunizieren müssen.

In diesem Zusammenhang ist der Begriff der Transparenz mindestens genau so essentiell wie zum Beispiel aus dem Blickwinkel der IT-Sicherheit. Der Begriff Transparenz steht für "durchsichtig" oder auch "deutlich erkennbar" und wird im Alltag in verschiedensten Gebrauchskontexten wie beispielsweise "Der gläserne Mensch" manchmal negativ oder "Kostentransparenz" eher positiv ausgelegt. Bei der Anwendung auf komplexe Abläufe bedeutet dies, die kausale Auswirkung der Änderung des Zustandes eines Teilsystems auf das Ganze zu verstehen.

Auf dem Weg zu mehr Transparenz

Was aber sind KPIs? Gibt es Standard KPIs, die eine Allgemeingültigkeit genießen? In der Tat kann das Auffinden eines KPI ein komplexer Vorgang sein, weil in diesem Zusammenhang Gültigkeitsbereiche und Blickwinkel eine starke Rolle spielen. Ein prominentes Beispiel unserer Tage verdeutlicht dies sehr plastisch: Aufgrund der schwindenden Rohstoffreserven ist in der letzen Zeit immer stärker der Druck auf die Autoindustrie gewachsen, schadstoffarme Autos herzustellen. Die Größe "CO2-Ausstoß pro gefahrenen Kilometer" ist zu einem KPI im Prozess der Kauf-Entscheidung geworden.

Unter anderem auf diesem KPI baut die Argumentationskette für die "Abwrack-Prämie" auf, die einen doppelten Nutzen verspricht: Auf der einen Seite den lahmenden Autoabsatz anzukurbeln, auf der anderen Seite die Ökologie durch reduzierten CO2-Ausstoß zu entlasten. Eine umfassendere Sicht auf die Problematik zeigt jedoch, dass die ökologische Bilanz ganz anders aussieht, werden die bei der Herstellung der Automobile anfallende CO2-Menge mit berücksichtigt. Hiernach wäre es sinnvoller, alte Autos bis zu ihrem "natürlichen" Ende fahren zu lassen und danach erst durch neue zu ersetzen. Dies bedeutet, dass der KPI "CO2-Ausstoß pro gefahrenen Kilometer" unter diesem Blickwinkel um "CO2-Ausstoß (Herstellung)" ergänzt und auf die Laufzeit angewendet werden müsste. In der Regel wird ein ganzes Bündel von Messkri-

terien benötigt, um eine belastbare Aussage über die Qualität eines komplexen Prozesses zu erhalten.

Eine formale Definition für einen KPI könnte lauten: Ein Key Performance Indikator ist ein messbares Kriterium, das entweder allein oder im Zusammenspiel mit anderen Key Performance Indikatoren eine gesicherte, auf einen definierten Zeitraum bezogene Aussage über die Qualität eines komplexen Systems oder Prozesses erlaubt. Daraus lässt sich auch sehr anschaulich ableiten, dass es für komplexe IT-Infrastrukturen kaum generelle Sets von KPIs geben kann, die eine Allgemeingültigkeit besitzen.

Die verschiedenen KPIs in ihren wechselseitigen Abgrenzungen müssen jedes Mal aus den vorliegenden Geschäftsprozessen und deren Geschäftszielen abgeleitet werden. Anschließend liefern diese KPIs eine Transparenz der Geschäftsprozesse, jedoch erfordert wiederum ihre Identifikation und Überwachung bereits eine hohe Transparenz der zugrunde liegenden IT-Infrastruktur.

Transparente IT-Infrastrukturdaten

Heutige IT-Infrastrukturen sind geprägt von Begriffen wie Konvergenz, Security oder SOA und so weiter. Unter dem Strich bedeutet dies technologisch, dass wir uns mit hoch integrierten und dynamischen Netzwerkstrukturen auseinandersetzen müssen. Der antreibende Faktor bei diesem Prozess ist Kostenreduktion, die Folgen sind die Verschleierung kausaler Zusammenhänge wie zum Beispiel die Tatsache, dass der Ausfall eines Druckers dazu führen kann, dass eine Wertschöpfungskette mehrere Stunden unterbrochen wird.

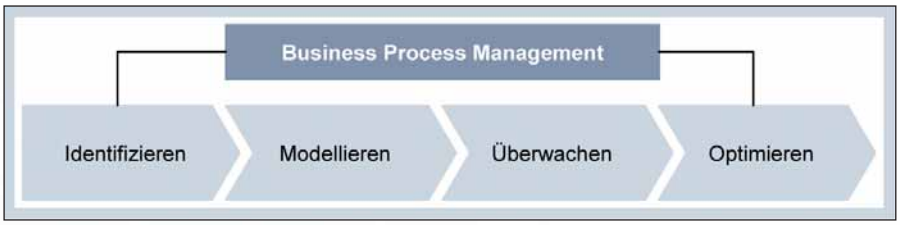
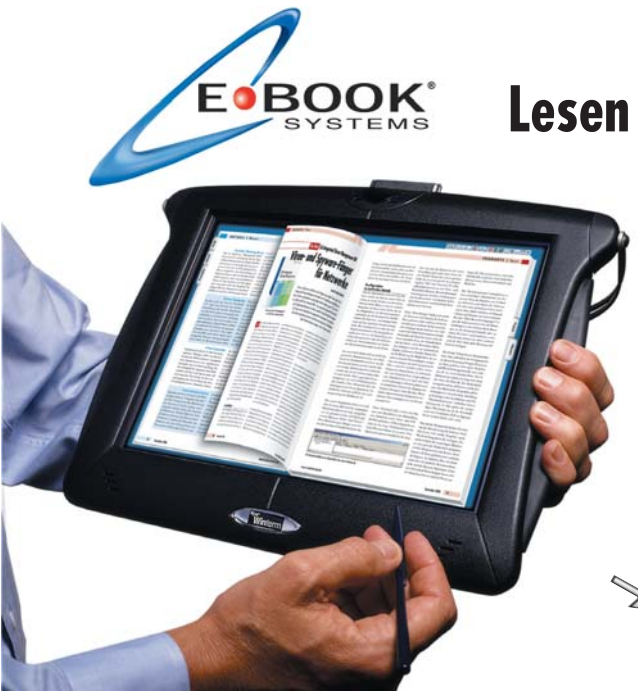


Bild 1: Im ersten Schritt sind Geschäftsprozesse losgelöst von der Technik zu beschreiben

Um diese funktionalen Zusammenhänge "sehen" zu können, ist neben einer umfassenden und stets aktuellen Datenhaltung des Ist-Zustandes eine Vergleichbarkeit von Daten gleicher Kategorie unbedingte Voraussetzung. Falls etwa ein Sensor die Temperatur in Fahrenheit und ein anderer die Temperatur in Grad Celsius angibt, so sind diese Zahlenwerte erst dann miteinander vergleichbar, wenn sie nach einem Normalisierungsprozess in derselben Einheit notiert sind. Dies klingt simpel, ist in der Praxis aber häufig eine Quelle für Störfälle. Der wohl publizistisch größte Zwischenfall dieser Art war 1999 der Absturz der Marssonde Climate. Auslöser für den Verlust von damals 125 Millionen Dollar war ein Navigationsfehler. Aus den Telemetriedaten wurde im Nachhinein ermittelt, dass der marsnächste Punkt zum Zeitpunkt des Verlustes nicht bei 150 km, sondern bei nur 57 km lag. In dieser Höhe ist die Marsatmosphäre jedoch bereits so dicht, dass die Sonde durch die Reibungskräfte und die Hitze zerstört wurde.

Die Ursache dieses Navigationsfehlers war schnell klar: Während die NASA Impulse im international gebräuchlichen SI-System mit der Einheit "Newton mal Sekunde" berechnete, wurde die Navigationssoftware des MCO vom Hersteller Lockheed Martin für das imperiale System mit der Impulseinheit "Pfund mal Sekunde" ausgelegt, also um den Faktor 4,45 größer.

Neben Vollständigkeit und Normalisierung ist die Automatisierung der Datenerhebung, das heißt die Aktualität des Ist-Zustandes, eine weitere Bedingung, um eine hinreichende Transparenz der IT-In-



E-BOOK SYSTEMS

Lesen Sie den IT-Administrator als E-Paper

Testen Sie kostenlos und unverbindlich die elektronische IT-Administrator Leseprobe auf **www.it-administrator.de**

Wann immer Sie möchten und wo immer Sie sich gerade befinden – Volltextsuche, Zoomfunktion und alle Verlinkungen inklusive. Klicken Sie sich ab heute mit dem IT-Administrator einfach von Seite zu Seite, von Rubrik zu Rubrik.

Infos zu E-Abos, E-Einzelheften und Kombiangeboten finden Sie auf:

www.it-administrator.de/magazin/epaper/

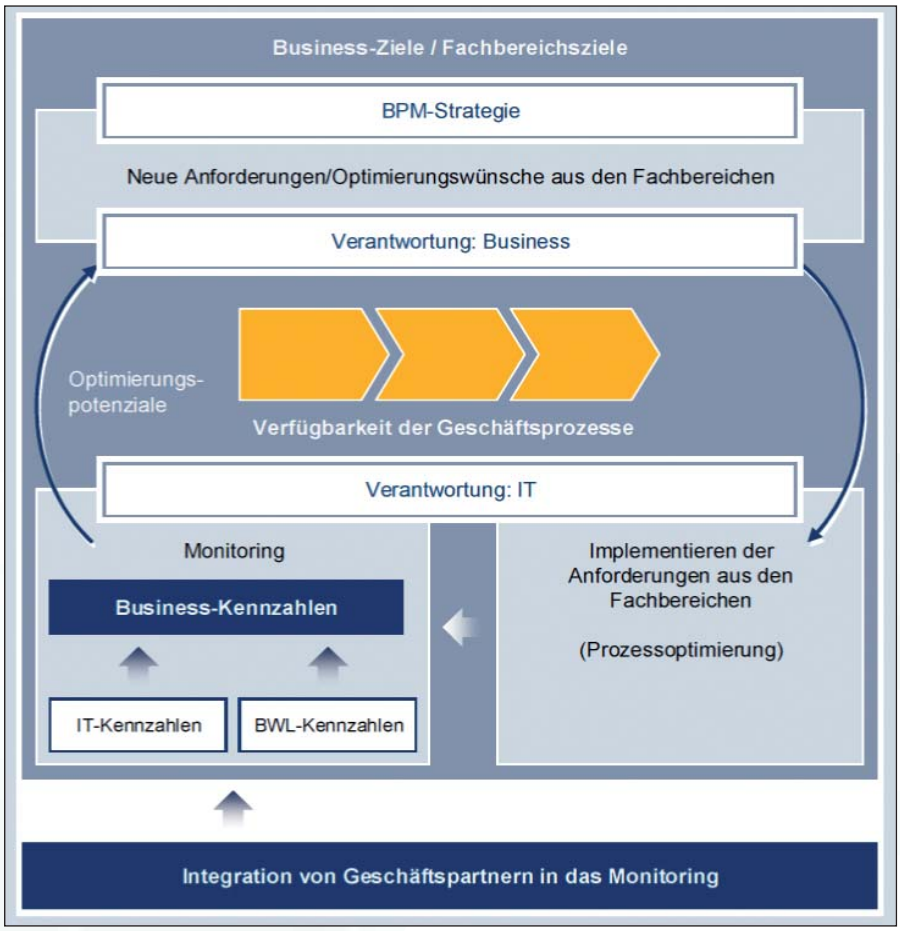


Bild 2: Zusammenspiel von IT und Geschäftsleitung im BPM

frastruktur zu gewährleisten. Unter diesen Umständen ist die IT bereit, im Dialog mit den Fachabteilungen wichtige KPIs zu überwachen.

Die Einführung der Geschäftsprozessüberwachung

Das Umsetzen einer transparenten und damit proaktiven Überwachung von Geschäftsprozessen erfolgt in Schritten:

1. Die Beschreibung der Geschäftsprozesse unter dem Blickwinkel des Geschäftziels: Die Beschreibung von geschäftskritischen Prozessen muss in erster Näherung aus einem Top-Down Blickwinkel erfolgen. In dieser Phase sollte die Beschreibung völlig losgelöst von Technik erfolgen, damit nicht im Vorhinein die Sicht auf das reine Geschäftsziel durch technische Bedenken beschränkt wird. Dabei sind die Prozesse unter Berücksichtigung einer Weiterentwicklung zu bewerten.
2. Das Zusammenführen technischer und nicht technischer Geschäftskriterien: Ist Schritt 1 vollzogen, kann als nächstes der Austausch über die Umsetzung zwischen den Abteilungen erfolgen. Insbesondere muss zu diesem Zeitpunkt die technische Machbarkeit geprüft werden.
3. Die Definition neuer Rollen und Qualifikationen: Essentiell für die anschließende Umsetzung sind die Kommunikation, die Akzeptanz und damit die Identifikation betroffener Personen mit den Prozessen. Es zeigt sich, dass dies am einfachsten durch die Definition neuer Rollen und Qualifikationen innerhalb einer Organisation umsetzbar wird. Bekannte Rollen sind in diesem Zusammenhang Chief Process Officer, Enterprise Architect oder Business Process Expert.
4. Die Identifikation und Ermittlung der KPIs: Eine wichtige praxisbezogene Regel ist die Verbindlichkeit einmal definierter KPIs. Häufig veränderte Rahmenbedingungen und die Hinzunahme weiterer Indikatoren innerhalb kurzer Zeit verhindern verlässliche Aussagen über die Prozess-Performance. Daher sollte eine gründliche Recherche nach den besten KPIs nicht unter Zeitdruck stattfinden. Einmal vereinbarte Messkriterien sind nach einer zu definierenden Einschwingphase von allen Beteiligten strikt einzuhalten.
5. Die proaktive Überwachung der KPIs: Dies setzt eine Software voraus, welche erlaubt, die beschriebenen Geschäftsprozesse zu übernehmen und zu modellieren.

Die Software muss grundsätzlich in der Lage sein, alle für einen Prozess erforderlichen Elemente (dies können IT-Elemente, aber auch nicht IT-Elemente, wie beispielsweise Anzahl der Bestellungen oder Vertragslaufzeiten sein) abzubilden und mit einem Status zu versehen. Ein hoher Grad an Automatisierung muss dabei den Ist-Zustand des Status mit größtmöglicher Aktualität garantieren. Anschließend wird der Status solcher Geschäftsprozesse überwacht und bei Statusänderung entsprechend den definierten Workflows reagiert. Als Software-Unterstützung kann hierzu das "theGuard! Service Management Center" von REALTECH eingesetzt werden. Neben der Möglichkeit, beschriebene Geschäftsprozesse abzubilden, zeichnet sich diese Monitoring-Lösung dadurch aus, über Business-Connectors relevante Information etwa aus externen ERP-Systemen zu integrieren und mit der Status-Information zur darunter liegenden IT-Infrastruktur zu korrelieren und konsolidiert zu bewerten. Beliebige KPIs lassen sich auf diese Weise erfassen und in ihrer Auswirkung auf Geschäftsprozesse überwachen. Alle Informationen liegen im "theGuard! Service Management Center" in normalisierter und aufgrund hohen Automatisierungsgrades in stets aktueller Form vor. *(jp)*

Dr. Kürsad Gögen ist Product Manager IT Service Management bei der REALTECH GmbH.

Einheitliche Softwareverteilung bei der GEWOFAG

Das Ende der Extrawürste

von Andreas Roscher

Ob Server, Desktop oder mobiler Client – was die zentrale Verteilung von Software betrifft, bekommen alle Rechner bei der GEWOFAG trotz verschiedenster Betriebssysteme die gleiche Behandlung. Dies trifft besonders auf die zentrale Verteilung von Anwendungen zu. Alles, was nicht zum Betriebssystem gehört, wird in Softwarepakete verpackt. Der folgende Anwenderbericht zeigt, mit welchen Mitteln das Unternehmen die einheitliche Softwareverteilung umsetzt und welche Klippen dabei zu umschiffen sind.

Die Administratoren der GEWOFAG verwalten insgesamt rund 450 Computer. Davon sind 130 Rechner in Außenstellen zu managen, außerdem befinden sich circa 60 Notebooks im mobilen Einsatz. 20 Server bilden aktuell das Rückgrat der Bereitstellung von Services. Schon vor sieben Jahren gab es bei der GEWOFAG die Anforderung, Windows- und Linux-Systeme gleichermaßen zu managen. Inzwischen ist sogar Solaris Sparc hinzugekommen. Linux wird zum Beispiel für Firewalls genutzt, Windows Server liefern für das Microsoft-Betriebssystem die Updates. Die Sparc-Server liefern die Samba-Freigaben.

Die GEWOFAG betreut knapp 30.000 Wohneinheiten in München

Hier zeigte sich die Problemlage vieler heterogener Systeme: Es musste im wahrsten Sinne des Wortes zu oft zu viel Handarbeit an den einzelnen Computern geleistet werden. Mittel der Wahl war die Duplizierung und Verteilung von kompletten Platten-Images. So konnten aber keine Softwarepakete gezielt entfernt oder hinzugefügt werden. Außerdem war auch die verschlüsselte Verteilung von Software auf die Computer nicht möglich.

Hauptkriterien bei der Suche nach einer geeigneten Lösung waren also die Möglichkeit der Verschlüsselung, die Verteilung einzelner Softwarepakete sowie die Unterstützung heterogener Systeme. Fündig wurden die IT-Verantwortlichen der GEWOFAG bei der Software "Open Management Architecture" (OMA).

Als einziges Produkt verwendet OMA durchgängig eine verschlüsselte Verteilung aller Daten auf der Basis des SSH-Protokolls und unterstützt Linux, Windows und Solaris. Es lassen sich alle Systeme vom Netz booten. Die Unterstützung aller anderen Systeme wie etwa Mac OS X erlaubt der GEWOFAG auf jede Form zukünftiger Anforderungen zu reagieren.

Für die Außenstellen der Firma wurde entweder ein mobiles OMA-Server-Notebook verwendet oder es wurde per USB-Platte betankt. Seit der durchgängigen 2 MBit-Anbindung der Filialen behandeln die IT-Verantwortlichen die Computer in den Außenstellen genauso wie die Systeme am Hauptsitz.

Betriebssystem ausrollen

Am Anfang aller zu erfüllenden Softwarewünsche für einen Computer steht immer die Verteilung des Betriebssystems. Da heterogene Systeme in der Praxis recht häufig vorkommen, muss das Ausrollen sowohl für Windows als auch Linux funktionieren.

Windows verteilen

Windows wird mit einem aktuellen Service Pack und einem zusätzlichen Stand an Patches verteilt. Um den Aufwand eines unbeaufsichtigten Setups von Windows zu vermeiden, wird pro Hardware-Plattform eine manuelle Installation von Windows XP ausgeführt und als Partitionsimage abgelegt. Das Vorgehen ist dokumentiert und endet nach einer Installation von Windows mit folgenden Aktionen:

- Alle Treiber installieren
- oma2win Prozedur ausführen
- Automatische Updates ausschalten
- Energiesparen der Netzkarte abschalten
- Nicht zertifizierte Treiber zulassen

Um das Datenvolumen an Partitions-Images nicht ins Unermessliche wachsen zu lassen, lassen sich die Unterschiede zwischen den Windows-Installationen der verschiedenen Hardware-Plattformen als Differenz auf den OMA-Servern ablegen. So gibt es für die Desktops der Firma etwa nur ein einziges Windows XP-Image und N-1 Differenzen, wobei N die Anzahl der unterschiedlichen PC-Typen ist. Für das Verteilen der Windows-Partitionsimages reicht das flotte Booten in die Linux basierte OMA-Konsole.

Linux verteilen

Linux wird mit einem aktuellen Stand als Workstation-Installation erfasst. Auch hier findet kein unbeaufsichtigtes Setup statt. Nach einer manuellen Installation ist nur eine Aktion erforderlich, nämlich das Ausführen der "oma2linux"-Prozedur. Das Abziehen der Installation erfolgt im Gegensatz zu Windows als Archivimage. Es werden faktisch nur die Dateien und Verzeichnisse abgeholt. Damit können die Typen der Dateisysteme und die Partitionierungen jederzeit ohne Anpassung des Archivimages verändert werden. Ein und dasselbe Archivimage kann auf reiserfs-, ext3- oder lvm2- Partitionen zum Einsatz kommen. Die notwendigen Korrekturen etwa an der Datei */etc/fstab* lassen sich in der OMA-Verwaltung separat hinterlegen. Die gewünschten Formatierungen regelt der dem Archivimage zugewiesene Image-Typ. Die Verwendung des passenden Kernels und der richtigen Initial-Ramdisk wird von den Distributionen entkoppelt und erfolgt unter Regie von OMA über eine auf dem Computer platzierte Management-Partition. So lässt sich ein einmal gezogenes Linux-Archivimage unverändert über Jahre hinweg einsetzen.

Ist die Zeit reif, kommt es mit einem neuen Archivimage zu einem Wechsel auf ein neues Linux (beispielsweise von Debian 3.1 auf Debian 4.0). Eine Einschränkung auf bestimmte Distributionen oder gar Releases gibt es generell nicht. Die Hardwaredifferenzen fallen unter Linux wesentlich spärlicher aus als unter Windows. Um die Grafik und den Plattencontroller einzufangen, reichen bei richtiger Konfiguration von Linux zwei Dateien pro Hardwaresorte aus, nämlich */etc/X11/xorg.conf* und */etc/fstab*.

OS individualisieren

Die neutralen Images von Linux und Windows müssen beim Verteilen individualisiert werden. Dem Windows-System muss eine eindeutige SID gegeben werden. An Stelle der IP-Adresse 0.0.0.0, die in den Images für jede Netzwerkkarte eingestellt wurde, muss die vorgesehene Konfiguration aufgebaut werden. Hier gilt es zu berücksichtigen, ob die Adressen fest zugeteilt werden oder ob auf DHCP zurückgegriffen wird. Auch sollte klar sein, ob eine Workgroup gebraucht wird oder eine Domäne besucht werden muss. Das regelt sich in der OMA-Verwaltung über die einmalige Zuteilung einer Generierungsmethode zum Imagenamen.

Für das Einstellen von Serversystemen können bis zu neun Netzwerkkarten exakt adressiert werden. Ein gut eingestelltes und mit allen Hardwaretreibern versorgtes Betriebssystem ist aber nur das Mittel zum Zweck. Final geht es um die Bereitstellung von Services in Form von Softwarepaketen. Ein Service sind zum Beispiel die automatischen Updates bei Windows oder die Bereitstellung des aktuellen SAP-Clients.

Prinzipien der Paketierung

Softwarepakete bestehen aus Dateien und Prozeduren. Die Dateiformate sind so unterschiedlich wie nur denkbar. Formate wie MSI, DEB und RPM sind nur die Spitze des Eisberges, in dem die Daten der Softwareprodukte vom Hersteller eingefroren werden. Passend zum Format ist die richtige Prozedur mit den richtigen Schaltern aufzurufen, damit die Software unbeaufsichtigt installiert werden kann. Neben der Anwendung eines plattformübergreifenden Scan-Verfahrens für Software bietet OMA die Integration jedes beliebigen Paketformates in ein OMA-Softwarepaket an. So kann vorzugsweise immer mit dem Paketformat des Herstellers gearbeitet werden.

Alle Paketdaten solcher Softwareprodukte werden in OMA in komprimierten cpio-Archiven versteckt. Die .msi-Dateien eines Lotus Notes-Clients liegen etwa in einer einzigen Datei *cpiogzip* von 230 MByte Größe und die Sourcen eines VMware-Servers für Linux in einer einzigen 280 MByte umfassenden Datei. Die passenden Prozeduren zu den Softwarepaketen befinden sich dagegen unkomprimiert auf dem OMA-Server und können jederzeit angepasst werden. Bei einer Komplettbespielung eines Computers gelangen die Daten und die Prozeduren bereits auf den Computer, bevor Linux oder Windows das erste Mal bootet. Die Fähigkeit von OMA, die Software offline zu verteilen, verkürzt den Prozess der Bespielung deutlich. Die Schale, die OMA um Softwarepakete legt, erlaubt auch den Austausch von Pakten. So können Pakete direkt übernommen werden.

Windows Pakete schnüren

Eine MSI-Datei in einem Softwarepaket auf dem OMA-Server abzulegen, ist die geringste Übung. Der Schwerpunkt liegt in den passenden Prozeduren, damit die

Installation so abläuft und so endet, wie Firmenvorgaben zum Einsatz einer Software das vorsehen.

Nicht zu vergessen sind die Konfigurationseinstellungen von Windows. Eine Installation von Windows kennt nicht die besonderen Sicherheitsanforderungen einer Firma. Mit einem Softwarepaket, das nur aus einer Prozedur besteht, werden final die Dienste abgeschaltet, die nicht gebraucht werden. Ändern sich die Anforderungen, lassen sich die Dienste auch jederzeit wieder anschalten.

Auch Linux mag Päckchen

Da die Linux Archivimages immer nur eine Linux-Workstation-Installation repräsentieren, muss auch hier etwas getan werden, um bei der Bespielung beispielsweise einen Webserver zu erzeugen. Die notwendigen Pakete sind in einer Softwaregruppe zusammengefasst. In der Realität sind die Paketnamen in OMA in voller Länge präsent und enthalten schon im Namen die Information über den exakten Versionsstand.

Auch bei Linux gilt der Grundsatz der Verteilung der Software vor dem Booten und der Installation der Software beim ersten Start. Dabei wird versucht, die Installation autark zu halten, damit der Computer in jedem Fall in den gewünschten Zustand kommt, ohne auf Verbindungen zum Internet oder Intranet angewiesen zu sein. Im Härtefall oder auch um die manchmal lästigen Prüfungen von Abhängigkeiten zu umgehen, kann eine Linux-Software auch aus den Sourcen heraus installiert werden.

Wahl zwischen Online- und Offline-Betankung

Ob Desktop, Server oder Notebook – die Betankung mit Software läuft im Prinzip stets auf die gleiche Art ab. Einfacher ist es, wenn die einzelnen Stationen Bestandteile eines Netzwerkes sind. Doch auch mobile Geräte lassen sich mit Hilfe eines USB-Sticks problemlos mit den nötigen Anwendungen versorgen.

Desktops und Server betanken

Rechner, die fest mit dem Netz der Firma verbunden sind, werden immer über das Netz bespielt. Das für eine Komplettbespielung notwendige Booten vom Netz wird vom OMA-Server geregelt und muss dort explizit eingeschaltet werden. Ob der Aktion noch ein Aufwecken per Wake-OnLan vorausgeht, ist Entscheidung des Operators. Im ungünstigsten Fall muss irgendwer den Computer einschalten. Ob das Betanken gleich startet, wenn der Computer sich meldet oder das Bespielen besser genau zu dem Zeitpunkt erfolgt, zu dem das Netz massive parallele Bespielungen auch verkraftet, ist nur eine organisatorisch zu treffende Entscheidung.

Notebooks notfalls offline versorgen

Die Erstbetankung eines Notebooks erfolgt wie die Betankung von Desktops und Servern. Eventuelle Schäden an den gelieferten Geräten werden sofort erkannt und die Geräte können gegebenenfalls reklamiert werden. Die Erstbetankung passiert in einem eigenen Teilnetz über eine feste IP-Adresse. Im bespielten Betriebssystem wird über die OMA-Generierung der DHCP-Client aktiviert und das Notebook kann dann in allen Netzen der Firma verwendet werden, in denen IP-Adressen dynamisch vergeben werden. Neben der Konfiguration der internen Karte des Notebooks wird auch der Von-Überall-Zugriff per WebnWalk-USB-Stick bei der Bespielung eingerichtet und für den Fall der Fälle bekommt jedes Notebook eine lokale Kennung, die identisch mit der Domänenkennung des Anwenders ist.

Am Ende der Erstbespielung erfolgt eine automatische Aufnahme des Notebooks in die Domäne. Über ein nachfolgendes, einmaliges Logon der zugewiesenen Benutzerkennung auf der Domäne wird das Herunterladen des vorhandenen Benutzerprofils erzwungen. So erfolgt der Wechsel eines bestehenden Anwenders von einem Desktop zu einem Notebook ohne Identitätsverluste beziehungsweise das Domänenprofil eines Notebook-Besitzers ist nach der Betankung nach dem ersten Domänen-Login wieder vorhanden. Die Beispieldaten des Notebooks lassen sich über OMA auf einem Installationsstick ablegen. Mit Hilfe der Managementpartition kann eine auf dem USB-Stick hinterlegte Bespielung auch ohne Firmenkontakt durch den Anwender selbst ausgeführt werden.

Nachverteilen bei Bedarf

Alle Systeme haben nach einer Bespielung einen von OMA bereitgestellten und konfigurierten SSH-Serverdienst. Unter Verwendung einer Public/Private-Key-Autorisierung lassen sich Softwarepakete bei laufendem Windows beziehungsweise Linux verschlüsselt nachverteilen. Wieder müssen Daten und Prozeduren verteilt werden. An welcher IP-Adresse ein Client gerade erreichbar ist, weiß immer das DNS, das durch OMA beziehungsweise dem dynamischen DHCP aktuell gehalten wird. Für die Online-Verteilung von Open Office auf Windows ist die Prozedur recht einfach.

Fazit

Mit der durchgängigen Verwendung von Softwarepaketen, die die Administratoren zu jeder Zeit schnell und sicher verschlüsselt verteilen können, hat die GEWOFAG das Dilemma ewiger Imageanpassungen hinter sich gelassen. Kommt eine neue Software zum Einsatz, wird nur ein neues Paket gepackt und per SSH auf die Systeme nachverteilt. Die Pakete kommen in die entsprechenden Softwaregruppen und sind damit fester Bestandteil der erneuten Bespielung eines Computers. Dabei gibt es beim Aufbau der Softwarepakete keinen prinzipiellen Unterschied zwischen Pakten für Linux, Windows oder Solaris. Software wird bei der erneuten Inbetriebnahme schon vor dem ersten Booten übertragen und beim ersten Start laufen bei Bedarf nur noch die Installationsaufrufe ab. Mit einer auf einem USB-Stick basierenden Verteilung klappt dies auch für mobile Clients, die keinen Netzkontakt haben. Durch die Verwendung eines Verbundes mehrerer OMA-Server sind zudem Ausfallsicherheit und Lastverteilung stets gegeben. *(ln)*

Firmenporträt: Pan Dacom Networking

Managed Services geben Sicherheit auch in Krisenzeiten

Hat die Finanz- und Wirtschaftskrise ihren Höhepunkt bereits erreicht oder stehen Unternehmen womöglich bald vor noch größeren Herausforderungen? So unterschiedlich die Prognosen ausfallen, stimmen die Experten in einem zentralen Punkt doch überein: Niemals war es für Unternehmen wichtiger, erfolgskritische Geschäftsprozesse gegen Störungen abzusichern, um damit die Handlungsfähigkeit auch im Katastrophenfall zu erhalten.

Das Spektrum der potenziellen Bedrohungen ist weit gefächert und reicht von äußeren Einflüssen über Sturmschäden, Verwüstung durch Feuer und Wasser bis hin zu Einbruch, Angriffen aus dem Internet, Diebstahl und Sabotage. Vor diesen Gefahren können auch Sicherheitsexperten keinen absoluten Schutz garantieren. Wohl aber lassen sich die Risiken wirksam begrenzen, so dass im Ernstfall das Unternehmen steuerbar bleibt und keinen Schaden nimmt.

Entscheidende Komponente eines wirksamen Business Continuity Managements ist das Business Process Management, wobei die Optimierung von Geschäftsprozessen im Fokus steht, was fast immer eine präzise Abstimmung mit der Unternehmens-IT voraussetzt. Denn kaum ein Geschäftsprozess ist heute ohne die Unterstützung durch vernetzte IT-Strukturen und Services mehr denkbar. Dies verdeutlicht den hohen Stellenwert, welcher der Absicherung von IT-Prozessen im Rahmen des Business Continuity Managements zukommt.

ITSCM und Managed Services als Dienstleistung

Weder ein kleineres Unternehmen noch ein Großkonzern kann der Menge an Sicherungsaufgaben verantwortlich nachkommen, ohne dafür große personelle Ressourcen zu binden. Unter dem Begriff "IT Service Continuity Management" (ITSCM) bieten deshalb die Netzwerkexperten der Pan Dacom Networking AG genau diese Kompetenz als Dienstleistung. Ob Mittelstand oder Industrie, die Anforderungen sind weitestgehend gleich: Die Herausforderung besteht darin, eine immer komplexere Infrastruktur samt ihrer Komponenten zu beherrschen, um damit die Verfügbarkeit der Geschäftsprozesse national wie auch international verlässlich sicherzustellen.

Die Pan Dacom Networking AG

Der Lösungsansatz der Pan Dacom gründet auf dem ausgewiesenen technologischen Know-how ihrer Experten und der in Zusammenarbeit mit dem Unternehmen entworfenen IT-Konzeption und ITIL-konformen Services. Hierbei sind sämtliche Kompetenzen der Pan Dacom als Solution-Partner in ihrem Zusammenspiel gefordert, betrifft dies doch gleichermaßen die Anbindung an ein WAN (Access & Transmission) wie auch Fragen der Sicherheit (Security) und der Verfügbarkeit von Daten und Applikationen (Storage) bis hin zu IP Communication (Netzwerk) und den Managed Services. Denn bei Bedarf übernimmt die Pan Dacom auch das Management der implementierten Lösung. Schließlich bedeutet eine hohe Verfügbarkeit der IT auch eine optimale Sicherheit.

Topthemen Security und Storage

Die Zusammenarbeit mit einem Unternehmen beginnt mit einer Analyse des Ist-Zustandes. In gemeinsamen Workshops werden das gewünschte Leistungsspektrum und die Verantwortungsbereiche von Kunde und Pan Dacom definiert. Hochspezialisierte Anforderungen in den Bereichen Security und Storage bilden traditionell einen Schwerpunkt der an Pan Dacom delegierten Services und Leistungen.

Basierend auf den Anforderungen wird ein für das Unternehmen individuell zugeschnittenes Servicekonzept erarbeitet, welches detailliert die erforderlichen Migrationsschritte beschreibt. Die Migrations- und Transitionsphase von Ist- zum Soll-Zustand wird durch das qualitätssichernde Projektmanagement der Pan Dacom auf PRINCE2-Standard begleitet.

Unterstützend kommen die Realtech-Produkte "theGuard! ServiceDesk" als Trouble Ticket-System und "theGuard! NetworkManager" als Monitoring-Tool zum Einsatz. Ausschlaggebend für den Einsatz der gewählten Realtech-Lösung ist vor allem deren modulare Struktur und dynamische Anpassbarkeit der vorhandenen Elemente sowie die reibungslose Integration weiterer Module wie zum Beispiel das BPM-Modul.

Garantierte Sicherheit 24x365

Zentrale Service-Instanz im Soll-Szenario der Managed Services ist das Network Operation Center (NOC) mit seinem Service Desk. Betrieb und Überwachung der Komponenten erfolgen dabei zentral aus der Unternehmenszentrale der Pan Dacom Networking AG in Dreieich und dies rund um die Uhr im 24x365-Modus. Das Pan Dacom NOC ist somit Drehscheibe und Plattform für sämtliche Serviceanforderungen.

Sobald sich eine Störung andeutet, greifen exakt definierte Service Level, die im Service Center hinterlegt sind. Die Mitarbeiter vom Service Desk der Pan Dacom nehmen je nach Anforderung proaktiv Kontakt mit dem eigenen Expertenteam, dem zuständigen Hersteller und Logistiker sowie ggfs. zusätzlichen Dienstleistern auf, um eine schnelle Problemlösung sicherzustellen. Durch Operational Level Agreements (OLA), in denen interne Annahme-, Antwort- und Weiterleitungszeiten definiert sind, können Probleme umgehend erkannt, an die richtige Supportinstanz weitergeleitet und behoben werden. Die Definition dedizierter Service Levels garantiert optimale Reaktions- und Lösungszeiten und stellt das vom Unternehmen geforderte Maß an Gesamtverfügbarkeit der IT-Infrastruktur und der darüberliegenden Prozesse sicher.

Nutzen für das Unternehmen und die IT

Mit der Bereitstellung von Managed Services durch die Pan Dacom Networking AG erhält ein Unternehmen die notwendige Unterstützung für die Absicherung geschäftskritischer Prozesse. Durch die gezielte Steuerung der Übergabe der Verantwortlichkeiten werden revisionssichere Betriebsabläufe nach ITIL und eine optimierte Transparenz geschaffen.

Mit dem zentralen Network Operation Center (NOC) und Service Desk der Pan Dacom verfügt auch ein weltweit aufgestelltes Unternehmen über einen global gültigen "Single Point of Contact". Dies vereinfacht und optimiert die Serviceabwicklung im Unternehmen und unterstützt dessen IT-Strategie. Das Unternehmen profitiert von einem qualifizierten Support, der durch unternehmenseigene Ressourcen (Personal und Skill) wirtschaftlich kaum zu leisten wäre. Somit wird das Betriebsteam genau in jenen Bereichen entlastet, in denen Expertise nicht ausreichend vorhanden ist, diese aber zwingend benötigt wird.

Die Zusammenarbeit der Netzwerkexperten der Pan Dacom Networking AG mit dem unternehmenseigenen Betriebsteam sorgt im Rahmen der vereinbarten Services für eine Entlastung des IT-Teams. Damit sind die Mitarbeiter wieder in der Lage, neue IT-Konzepte zu entwickeln und somit die Unternehmensstrategien aktiv zu unterstützen.

Bernhard Bischoff zeichnet bei der Pan Dacom Networking AG verantwortlich als Business Development Manager für den Bereich Service und berät Unternehmenskunden in ihrer BCM-Strategie, erfolgskritische Geschäftsprozesse gegen Störungen effektiv abzusichern.

NEU Abo-Upgrade – werden Sie IT-Administrator-Jahresabonnent mit Jahres-CD/DVD

Für nur € 9,84 Upgrade-Zuschlag auf Ihr Jahresabo bekommen Sie jedes Jahr im Dezember die IT-Administrator Jahres-CD/DVD mit den 12 Heftausgaben von Januar bis Dezember im PDF-Format automatisch zugesendet.

Bestellen Sie jederzeit und ab sofort online auf:

www.it-administrator.de/upgrade

Schutz der E-Mail-Kommunikation am Max-Planck-Institut

Ungehinderte Kommunikation für internationale Forschung

von Frank Rickert

Quelle: Pixelio.de

Das Max-Planck-Institut für ausländisches und internationales Sozialrecht (MPI) beobachtet und analysiert die sozialrechtlichen und sozialpolitischen Entwicklungen in verschiedenen europäischen und außereuropäischen Ländern und beherbergt die Max Planck Digital Library. Fundiertes Wissen über die jeweils vorherrschenden gesellschaftlichen, kulturellen und wirtschaftlichen Hintergründe ist für die Beurteilung des Sozialrechts unerlässlich. Das Institut verfügt deshalb über ein großes Netz von akademischen Kontakten und Forschungsprojekten in den jeweiligen Ländern, mit denen es vor allem per E-Mail in Verbindung bleibt. Die ständige Sicherstellung der E-Mail-Kommunikation ist deshalb eine zentrale Voraussetzung für die Arbeit des Instituts und der Schutz der E-Mail-Infrastruktur vor Spam, Malware und Überlastung ein kritischer Faktor.

Seit 2006 verzeichnen die Verantwortlichen des MPI eine stetig steigende Belastung ihrer E-Mail-Server. Obwohl das Institut "nur" 150 Mitarbeiter zählt, trifft täglich eine sechsstellige Anzahl von E-Mails auf den Servern ein. Rund 90 Prozent davon sind unerwünschte Werbung. Insbesondere nach Urlaubszeiten oder Wochenenden war der IMAP-Server des Instituts der Vielzahl von Schreib-/Leseanfragen durch die auf den Arbeitsplatzrechnern installierten, lokalen Spam-Filter nicht mehr gewachsen. Als Mailclient kommt Thunderbird zum Einsatz, mit dem entsprechenden programmeigenen Spam-Filter. Als MTA kommt exim auf zwei Servern zum Einsatz.

Hinzu kam eine False-Positive-Rate von 0,05 Prozent. Das bedeutet, dass pro 2.000 E-Mails eine fälschlich als Spam klassifiziert wird und dadurch verloren gehen kann – angesichts des täglichen E-Mail-Volumens ein untolerierbar hoher Wert.

Spam reduzieren, Vertraulichkeit wahren

Nach einer kurzen Suche stießen die Verantwortlichen am MPI auf einen Fachartikel, der den Spam-Filter und E-Mail-Kategorisierungsdienst "eXpurgate" der Firma "eleven" vorstellte. Die Lösung überzeugte durch ihren neuartigen Ansatz zur Spam-Erkennung: den Bulkcheck. Dieser reduziert die zu prüfenden E-Mails auf Kontrollsummen, die dann in einer zentralen Datenbank gespeichert und mit denen anderer E-Mails verglichen werden. Treten gleiche oder ähnliche Kontrollsummen in großer Zahl auf, wird die betreffende E-Mail als Spam kategorisiert. Das so genannte "Massen-E-Mailkriterium" arbeitet unabhängig vom Inhalt der E-Mail und sichert damit die Vertraulichkeit des elektronischen Briefwechsels. Die Kontroll-

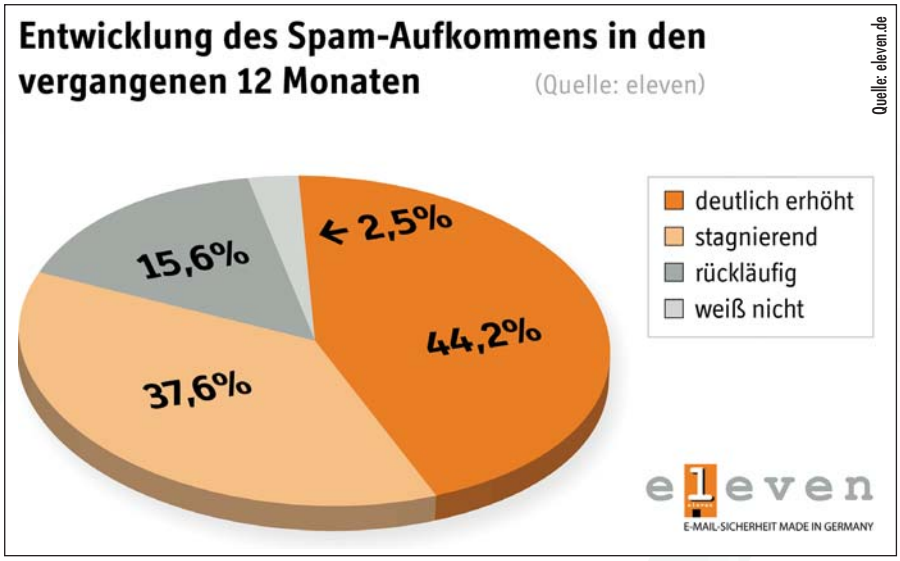


Bild 1: Wie auch die Mehrheit von 300 IT-Verantwortlichen deutscher Unternehmen in dieser Umfrage kämpft das MPI gegen die steigende Spamflut

summen sind nur wenige Bytes groß und verursachen nur eine sehr geringe Netzwerkbelastung.

Wichtigste Anforderung war daher, Spam bereits beim Empfang durch den E-Mail-Server abzulehnen und dabei Fehlsortierungen zu verringern oder am besten ganz zu vermeiden. Die so genannten False Positives sind legitime E-Mails, die durch fehlerhafte oder zu "starke" Einstellungen des Spam-Filters aussortiert werden, dadurch verloren gehen oder in aufwändigen Suchen durch die Mitarbeiter aus dem Spam-Ordner "gefischt" werden müssen. Dies war ein massives Problem, dass man am MPI zukünftig sicher gelöst haben wollte, da mit dem Spam-Wachstum auch die Zahl der False Positives immer weiter anstieg.

Schluß mit False Positives

Hier sahen die Verantwortlichen einen der wichtigsten Vorteile der avisierten Lösung: Aufgrund des Massen-E-Mail-Kriteriums sind Fehlsortierungen individueller E-Mails praktisch ausgeschlossen. Die False-Positive-Rate liegt daher bei von anderen Lösungen unerreichten 0,00001 Prozent, das heißt auf 10 Millionen E-Mails kommt eine Fehlsortierung. Nicht zuletzt sollte die neue Anti-Spam-Lösung zukunftssicher sein, das heißt auch auf neue Spam-Formate reagieren können. Auch dieses Kriterium war bei eXpurgate durch die content-unabhängige Erkennungsmethode gegeben.

Ein zusätzliches Plus bei eXpurgate ist die Wartungsfreiheit der Lösung. Die eXpurgate-Datenbank wird von eleven gepflegt. Im vom MPI gewählten Inhouse-Modell von eXpurgate besteht eine ständige Verbindung zu dieser Datenbank, um die reibungslose und schnelle Klassifizierung der Mails zu gewährleisten. Ein großer Vorteil dieser Lösung ist, dass die E-Mails das Unternehmensnetzwerk nicht verlassen. Es werden nur die Kontrollsummen ausgetauscht, die keinerlei Rückschlüsse auf den Inhalt der E-Mails zulassen. Für vielen Unternehmen und öffentliche Einrichtungen ist dies ein entscheidender Punkt, da er optimalen Datenschutz gewährleistet.

Fazit

Die Implementierung in das Netzwerk des MPI verlief problemlos. Nachdem die Lösung auf den institutseigenen Rechnern installiert war, konnte die Spam-Filterung buchstäblich auf Knopfdruck beginnen. "Der Einsatz von eXpurgate verläuft sehr gut. Unser IMAP-Server wurde spürbar entlastet und unsere Erwartungen wurden somit voll erfüllt", so Dr. Andreas Wohlschläger, Leiter der wissenschaftlichen EDV.

Die schnellen Ergebnisse überzeugten auch die Mitarbeiter. Keine False Positives mehr und keine Konfiguration oder Trainingsphasen durch die Anwender. Eine regelmäßige Wartung oder Administration ist nicht notwendig, lediglich die bei jeder Software üblichen Updates müssen installiert werden. Die Wissenschaftler am Max-Planck-Institut für ausländisches und internationales Sozialrecht können sich damit jetzt wieder voll und ganz auf die Forschung konzentrieren. *(jp)*

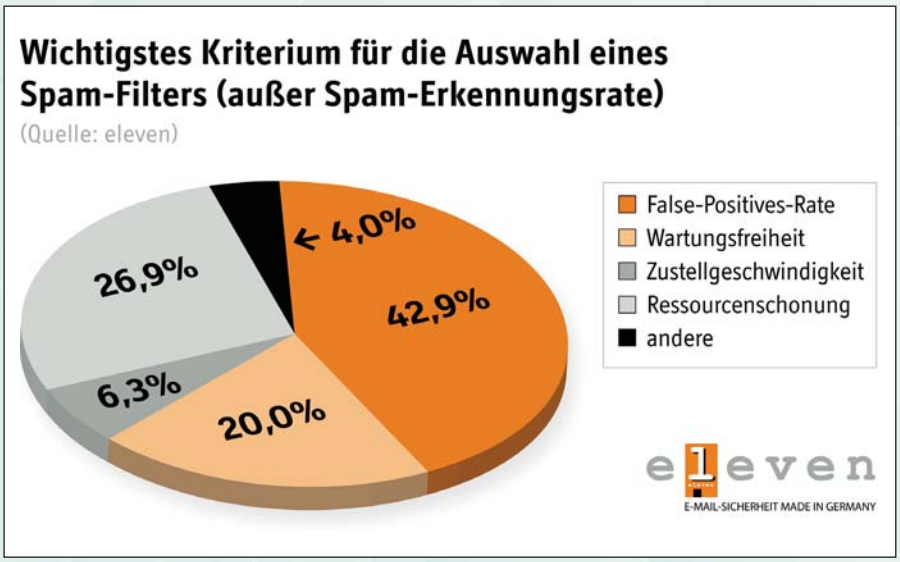


Bild 2: Die wichtigsten Kriterien bei der Auswahl einer Anti-Spam-Lösung

Netzwerkmanagement als zentraler Baustein in der Serviceorganisation

Durchblick schaffen

von Gerrit Behrens

Das Hannoveraner Unternehmen Fleischhauer setzt das Produkt "theGuard! Netzwerkmanagement" als zentralen Baustein in der Serviceorganisation eines international agierenden Kunden ein. Die Lösung bewältigt ein flächendeckendes Netzwerkmanagement mit mehreren tausend aktiven Komponenten und leistet relevante Sicherheitsfunktionen.

Dabei wird Sicherheit auch im Sinne des IT-Grundschutzwertes "Verfügbarkeit" verstanden. Die IT-Leistung ist Teil des Geschäfts, ein Ausfall bedeutet, dass Unternehmensleistung nur erheblich eingeschränkt erbracht werden kann. Der IT-Grundschutzwert "Verfügbarkeit" beschreibt laut Bundesamt für Sicherheit in der Informationstechnik (BSI) "die Verfügbarkeit von Dienstleistungen und Funktionen von IT-Systemen zu jedem von dem Nutzer geforderten Zeitpunkt".

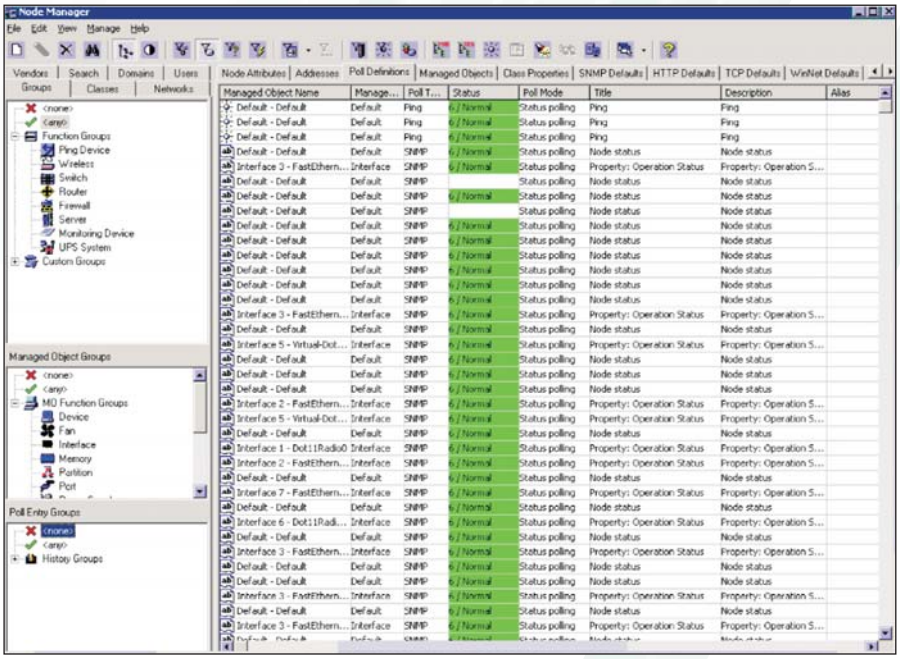


Bild 1: Mit Hilfe von theGuard! werden Probleme erkannt und validiert

Zielvorstellung des Kunden

Für den Kunden steht die Verfügbarkeit seiner Geschäftsprozesse im Vordergrund sowie die transparente Nachweisführung über die eigene Service-Level-Erfüllung. Die interne IT-Abteilung stellt den IT-Betrieb (Applikationen, Netze, Server, Clients) der gesamten Unternehmensgruppe entgeltlich zur Verfügung und hat dafür die Einhaltung der getroffenen Service Level Agreements (SLAs) über Verfügbarkeiten und Antwortzeiten zu dokumentieren.

Auch hierfür wird theGuard! genutzt, indem etwa Zugriffszeiten auf Websites wie Google gemessen werden und bestimmte Laufzeiten nicht überschritten werden dürfen. Das Programm misst als Referenzwert das Requestecho sowohl über den Unternehmensproxy-Cluster als auch via direktem Webconnect. Fehlerhafte Proxy-Dienste werden durch große Delays erkennbar. Des Weiteren wird die Visibilität des gesamten Datennetzwerkverbundes in einem monatlichen Report zusammengefasst und per Mail den Verantwortlichen automatisch zugestellt.

Netzwerksicherheit durch Transparenz

Durch den Einsatz der selbstorganisierenden Online-Datenbank über den Aufbau des Datennetzwerkverbunds (theGuard! Inventory Management) wird die unerlässliche Infrastrukturdokumentation durch Automatisierung erheblich vereinfacht, ständig aktualisiert und Kosten reduziert. Die Configuration Management Database (CMDB) der Lösung schafft

Kundenprofil

Die Unternehmensgruppe des Endnutzers ist mit fast 10.000 Mitarbeitern einer der Globalplayer im Bereich der technischen Dienstleister. Sie ist auf drei Kontinenten in mehr als 70 Ländern vertreten. Ihre Marktposition verdankt die Gruppe der technischen Kompetenz und ihrem breiten Beratungs-, Service- und Prüfspektrum.

Transparenz über den weit verzweigten Netzaufbau. Sie erlaubt die Ansicht des weltweiten Weitverkehrsnetzes des Unternehmens bis hin zum Zoom auf jeden einzelnen Link respektive auf jede einzelne Komponente. So lassen sich proaktiv Störungen und Verbindungsprobleme diagnostizieren und kurzfristig an Fleischhauer als externen Serviceprovider melden und beheben.

Die offenen Schnittstellen von theGuard! bieten vielfältige Möglichkeiten, individuelle Erweiterungen zu programmieren oder Softwarelösungen von Drittanbietern anzubinden. Für die übersichtliche Darstellung und Zusammenfassung jeglicher Stati und Änderungen, die für die Netzverfügbarkeit relevant sind (Transparenz), wurde von Fleischhauer ein Monitoring-Tool als Extension entwickelt und in theGuard! integriert.

Mehr Sicherheit durch Ticket-System

Fällt eine Komponente oder ein Link aus, sendet theGuard! einen Trap mit einer ID an das Fleischhauer Ticket-System (FTS), welches zunächst anhand der generischen ID die Zuordnung zu dem jeweils zuständigen Servicehelpdesk herstellt. Handelt es sich um eine Fremdkomponente, die nicht durch die Servicevereinbarung abgedeckt wird, wird das Ticket automatisch aussortiert und fällt in den Zuständigkeitsbereich eines anderen verantwortlichen Serviceproviders.

Je nach Relevanz der ausgefallenen Strecke oder Komponente definiert die begleitende ID die Eskalation im FTS. Mit dem Logging-Modul von theGuard! agiert eine Art Dolmetscher, der die generierten Traps (Status- oder Fehlermeldungen) mit der internen Datenbank abgleicht und als Klartextinfo per E-Mail weiterleitet (zum Beispiel: Trap 5412 = Lüfter ausgefallen).

Es arbeiten regelmäßig bis zu dreißig User in theGuard!, um proaktiv Servicelevel zu validieren, einzuhalten und zu übertreffen. Nachdem der eingehende Trap vom Serviceleitstand daraufhin überprüft wurde, ob das Problem weiterhin existent ist, erhält das Ticket eine Freigabe für den 2nd Level Support. Dieser leitet das Troubleshooting ein, in dem er beispielsweise die Parameter/Logfiles ausliest und geeignete Maßnahmen ergreift. Unterschiedliches Rechtemanagement ermöglicht es, dem 1st- und 2nd Level Support abgestufte Zugänge zum System zu gewähren. Die Serviceorganisation kann dadurch mit Personen mit unterschiedlichen Skills aufgebaut werden. Wenn für die Lösung eines Tickets mehr Qualifikation erforderlich ist, muss das Ticket weitereskaliert werden. Fehlnutzungen und damit eingehende Störungen durch qualifikationsüberschreitende Systemrechte werden auf diese Weise verhindert.

Das Netzwerkmanagement-System wird kundenseitig sukzessive erweitert und nahezu jede Technik, die die Möglichkeit bietet, ihren Betriebszustand anzugeben, integriert, wie beispielsweise aktive Komponenten, USV-Anlagen, Telekommunikationsanlagen, Server, Videokonferenz-Systeme, Klimalagen, Temperaturüberwachungen oder Wasserstand im Doppelboden.

Einsatz und Nutzen für den Kunden

Der Kunde setzt bei dem Produkt theGuard! Netzwerkmanagement die Module Reporting, Provisioning, diverse produktspezifische Module, das tG! SMC Reporting BaseKit mit dem Reporting Package NM-Basic sowie Administrator- und Web-Client-Lizenzen ein. Den positiven Nutzen hat er in der eindeutigen Interpretation und Bearbeitung von Fehlermeldungen und Warnhinweisen aus dem IT-Verbund sowie in der Tatsache, dass zielgerichtet (keine umständliche Suche mit Versuch und Irrtum) gearbeitet werden kann. *(jp)*

Links

IT-Grundschutz-Leitfaden
www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf

iladministrator
Das Magazin für professionelle System- und Netzwerkadministration

Worüber Administratoren morgen reden

Sichern Sie sich den E-Mail-Newsletter des IT-Administrators und erhalten Sie Woche für Woche die

- neuesten TIPPS & TRICKS
- praktischsten TOOLS
- interessantesten WEBSITES
- unterhaltsamsten GOODIES

sowie einmal im Monat die Vorschau auf die kommende Ausgabe des IT-Administrators!

Jetzt einfach und kostenlos bestellen unter:

www.it-administrator.de/newsletter

Überwachung von IT-Infrastrukturen

Sicherheit durch Transparenz

von Hans-Martin Dietrich

Ein noch so genau beschriebener und in allen relevanten Anteilen erfasster Geschäftsprozess benötigt im Kernpunkt eine Prozessüberwachung, die die vielfältigen Abhängigkeiten auch über verschiedene Ebenen hinweg in Beziehung setzt und entsprechend der spezifischen Bedeutung bewertet. Dazu dient ganz zentral die Methodik der Key Performance Indikatoren, durch deren geeignete Definition, kontinuierliche Erfassung und konsolidierte Bewertung der Grundstein für eine transparente und in ihrer kausalen Verknüpfung überwachbaren Systemlandschaft gelegt ist. In der Zusammenführung von technischer Sicht und Geschäftssicht liegt der Vorteil dieser Methodik.

Zu einem umfassenden Sicherheitskonzept gehören natürlich auch die klassischen Maßnahmen, wie etwa die korrekte Konfiguration von aktiven Netz-Komponenten sowie von Firewalls, aber auch der Patchstand und die Version des verwendeten Virenscanners auf Arbeitsplatzsystemen. Allerdings ist in diesem Bereich eine oft nur mangelhafte Erfassung des aktuellen Zustandes der Netzwerkumgebung die Ursache für massive sicherheitskritische Zwischenfälle.

Somit kommt der aktuellen und automatisierten Erfassung dieser Parameter eine zentrale Bedeutung zu. Typische Schnittstellen für die Informationserhebung sind neben SNMP weitere CIM-Protokolle wie WMI und WBEM. Nur eine IT-Landschaft, in der Sicherheitslücken frühzeitig identifiziert und erforderliche Maßnahmen umgehend eingeleitet werden können, ist als tendenziell sicher einzustufen.

Gerade die typisch sicherheitsrelevante Information muss in reproduzierbarer und transparenter Weise in Beziehung zu den übrigen Daten der Systemlandschaft gesetzt werden. Auf diese Weise allein kann seriös beurteilt werden, welche Relevanz eine scheinbar unwesentliche Information für die Sicherheit eines Netzwerkes und der darin realisierten Geschäftsprozesse hat. Nur durch Sichtbarmachen kann Sicherheit geschaffen werden.

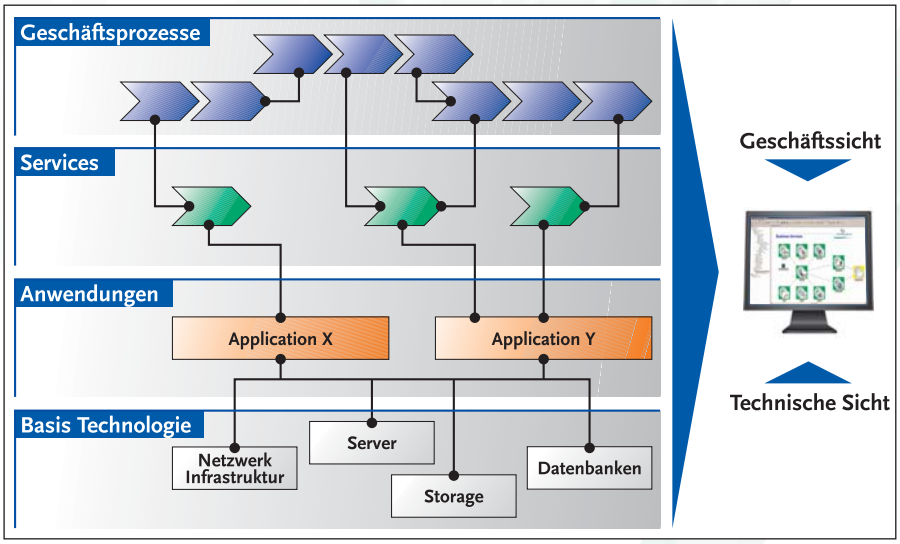


Bild 1: Die Geschäftssicht auf Prozesse im Unternehmen ist ebenso wichtig wie die technische Sicht

End-to-End-Monitoring

Ein immer stärker in den Vordergrund tretender Aspekt ist dabei aber auch die Einbeziehung des Menschen als Teil von Geschäftsprozessen. Denn an den Endpunkten von Prozessabläufen befinden sich Menschen, die von außen betrachtet einen natürlichen Teil dieser Prozesse bilden.

Sie sind es, die den Prozess "spüren" und ihn damit ebenfalls bewerten. Und das bedeutet: Akzeptieren die Benutzer die Umstände, unter denen sie einen Prozess bedienen, so wird der Prozess auch in der Regel einen höheren Wirkungsgrad gewinnen. Paradebeispiel hierfür sind Antwortzeiten von Applikationen innerhalb von Prozessschritten. Hier unterliegen Bewertungen der Prozess-Performance oft sehr ungenauen, weil aus der jeweiligen "gefühlten" – subjektiven – Beurteilung des Anwenders heraus getroffenen Wertungen. Ein darauf basierender KPI kann deshalb auch nur wenig relevante Beiträge zur Bewertung eines Geschäftsprozesses liefern.

Hier setzt das systematische End-to-End-Monitoring an:

1. Datenvolumina und Performance beschreibende Kommunikationsparameter lassen sich im Bereich der passiven Messungen an Netzwerkkomponenten (vornehmlich Router) erfassen. Hier

laufen die Informationen auf, wer mit wem wann was und über welche Protokolle kommuniziert hat (in der Praxis wird hier auf typische Technologien wie Netflow, NBAR oder vergleichbare zurückgegriffen). Zur Auswertung ist natürlich ein durchaus komplexes Mapping auf die interessierenden Geschäftsprozesse erforderlich (Ableitung der relevanten KPI).

2. Im Bereich des aktiven End-to-End-Monitorings wird im ersten Schritt das Antwortzeit-Verhalten beim Anwender als KPI erfasst und in der Gesamtbewertung des Geschäftsprozesses berücksichtigt. Zentraler Punkt dieser Methodik, die charakteristische End User-Szenarien zyklisch ablaufen lässt und ermittelte Transaktionszeiten erfasst, ist, dass der End User in seinem Verhalten durch einen Roboter simuliert wird. Auf diese Weise wird zum Beispiel das Antwortzeit-Verhalten eines Applikations-Servers aus der Position des End Users erfasst. Dabei fließen allerdings unterschiedlichste Parameter in das Messergebnis ein. So kann beispielsweise der Kommunikationspfad vom End-User über einen beliebigen von den redundanten Pfaden innerhalb einer WAN-Strecke verlaufen. Innerhalb des redundanten Rechenzentrums (Site 1 / Site 2) kann der Zugriff auf den Applikationsserver über Citrix, Webportal oder im Falle eines Fat Client beim End User direkt auf dem Applikationsserver erfolgen. Hier muss sorgfältig geplant werden, welche Parameter für die Bewertung eines Geschäftsprozesses zusätzliche Relevanz liefern. Neben applikationsbezogenen Messtransaktionen sind auch aussagekräftige Standardtransaktionen auf anderen Protokoll-Ebenen (FTP-Transfer, URL-Verfügbarkeit) – wiederum von Roboter-Maschinen ausgeführt – in der Praxis geläufig.

3. Ein zweiter Schritt im Bereich des aktiven End-to-End-Monitoring umfasst die gezielte Messung von anteiligen Transaktionszeiten auf Kommunikationsabschnitten, zum Beispiel am Anfang und am Ende einer WAN-Verbindungsstrecke (Ermittlung von Differenzwerten). Dazu werden weitere Messroboter platziert (etwa am Eingangs-Router des Rechenzentrums oder sogar innerhalb desselben). Dadurch lassen sich die KPIs weiter spezialisieren, wodurch ihre Relevanz für die Beurteilung des Geschäftsprozesses und der darunter liegenden IT Infrastruktur zunimmt. Dadurch ist es möglich, auftretende Probleme etwa auf einer WAN-Strecke frühzeitig als für den Endanwender relevant zu identifizieren und erforderliche Maßnahmen umso gezielter einzuleiten.

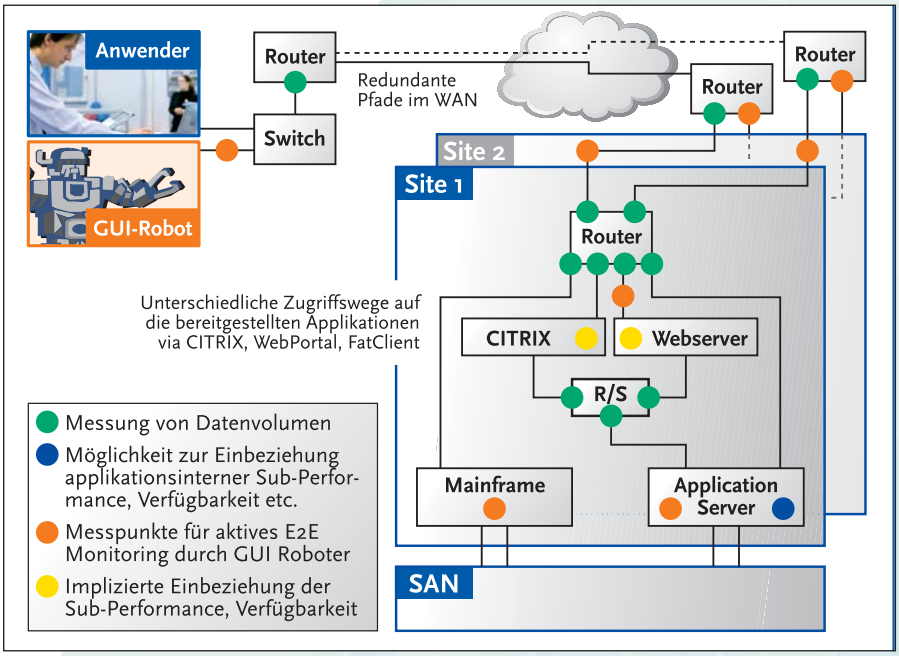


Bild 2: Mögliches Szenario für ein End-to-End-Monitoring

Für die Umsetzung eines solchen End-to-End-Monitoring-Konzeptes ist eine verteilte Roboter-Messumgebung erforderlich, deren Messwerte statistisch aufbereitet und stabilisiert als KPIs verwendet werden. Die Einbindung in die Geschäftsprozess-Überwachung setzt eine leistungsfähige Software voraus, die die ermittelten KPI-Werte aus der End-to-End-Messung mit den übrigen Parametern zusammenführt und konsolidiert bewertet. Dadurch wird auch die Applikationsebene der Systemlandschaft transparent gemacht und in ihrer Relevanz für die Verfügbarkeit und Performance von Geschäftsprozessen mithilfe von KPIs berücksichtigt.

Das "theGuard! Service Management Center"von REALTECH bietet eine integrierte Lösung, die sowohl im Bereich End-to-End Monitoring wie auch in der Überwachung der Security innerhalb einer Systemlandschaft eingesetzt wird. Über vielfältige Schnittstellen (inklusive SNMP und WMI) wird die zentrale Datenbank automatisiert stets aktuell gehalten. Auf Basis der darin enthaltenen normalisierten und darum vergleichbaren Parameter wird ein Baselining zur individuellen Überwachung von beispielsweise Security-Patches ermöglicht. Darüber hinaus bietet die Korrelation dieser Information in der Gesamtsicht der Prozessstruktur sowie die transparente Verknüpfung mit End-to-End-Transaktionszeiten eine umfassende Monitoring Lösung. *(jp)*

Hans-Martin Dietrich ist Product Manager IT Service Management bei der REALTECH GmbH.

Was brauchen Sie mehr ?

Als IT-Verantwortlicher sind Sie gefordert, Ihrem Management aussagekräftige Reports zur Verfügbarkeit von unternehmensweiten Geschäftsprozessen zu liefern. Gleichzeitig müssen Ihre Administratoren die technischen Zusammenhänge von Geschäftsprozessen und einwirkenden Objekten ganzheitlich erfassen können.

Die dafür notwendigen Business-Views stellt Ihnen das theGuard! Service Management Center zur Verfügung. Die Software analysiert verschiedenste Daten Ihrer IT-Landschaft, verknüpft diese mit Informationen aus ERP-Systemen und generiert aussagekräftige Kennzahlen für Ihre Geschäftsprozesse. Automatische Analysemechanismen stellen bei Abweichungen sicher, dass zeitnah und zielgerichtet reagiert werden kann.

Erfahren Sie mehr unter: www.realtech.de/bpm

REALTECH AG
Tel. +49.6227.837.651
bpm@realtech.de
www.realtech.de/bpm

REALTECH